Indirect Data Embedding In Digital Image Using Identifier Channel (IDEIC)

Karshan Kandoriya[#], H. M. Diwanji[*]

[#]*Department of computer Engineering, LDCE, Ahmedabad*

[*]*Assistant Professor, computer Engineering Dept. LDCE, Ahmedabad*

Abstract: The proposed new method, “Indirect Data Embedding using Identifier Channel”, use the colour (RGB) image. In this method two files are require two embed the secret information. The first file is secret message and second file is cover image. In the proposed method, Data is not directly embedded in the cover image. Secret message is first of all translated to binary stream of binary bit (digit) zero and one. Then consecutive occurrence of binary digit is counted. The count of consecutive occurrence is embedded in the digital image hence Indirect Data Embedding. The counter is of 3-bit. There we can count max occurrence to 7. One channel is use as a digit identifier. Here identifier used for identifying the binary digit (0/1), count of consecutive occurrence of that digit will be embedded in remaining two channels. Remaining two channels named channel-I and channel-II are used to hide the count of consecutive occurrence of binary digit. 1-LSB of channel II is used to hide 1-MSB of the counter. 2-LSBs of channel I are used to hide 2-LSB of the counter. Proposed algorithms (IDEIC) provides two layer of security. Proposed algorithm provides indirect data hiding. Thus ultimate benefit is indirect data hiding and implicit end marker. And visual quality is improved in IDEIC.

Keywords: - Indirect data Embedding, Data hidings, Cover Image, Stego Image and Visual Quality.

I. Introduction

The purpose of this paper is to improve visual quality of stego image. Today, watermarking and data hiding are current topic for research. Both has different goal. This Section covered introduction of only data hiding. Data hiding has goal of providing safety and security for safe data transmission and even some time for data storage. Data hiding is the new concept, using embedding algorithms secret data get hidden in some original digital image called redundant or cover file. There can be many more types of files (viz. audio, video etc) as a redundant/cover file. Data hiding can be done three domains in digital image processing. In spatial domain, data directly embedded in pixels at LSB positions, simple is example is LSB [1]. Second is compression domain [2]. Spatial domain has more embedding capacity than compression domain and frequency domain. Second is frequency domain. In frequency domain Fourier Transform of digital image is used to hide data. It can be discrete sine or discrete cosine transform of digital image. After embedding data inverse Fourier Transform is carried out. In frequency domain data embedding capacity is less than spatial domain. Frequency domain is more robust compared to spatial domain.

Cryptography is another mean for encrypting and transmitting data through an internet in secure manner, but data hiding has extra advantages over cryptography, mainly for eavesdropping unauthorized person. As encrypted data can be embedded in digital image thus data hiding is works as an additional layer of security. Data hiding provides security, ownership and authorization of document. Ownership verification and authentication is major task for military people, research institute and scientist [3]. Information security and image authentication has become very important to protect digital image document from unauthorized access [4]. Thus improving the visual quality is important. Also Electronic medical records are very sensitive in need more security [5] and also it need more embedding capacity Algorithm as this data are large in size. There is also good capacity algorithm, A Data Hiding Scheme for Digital Image Using Pixel Value Differencing [6].

In the proposed method, Data is not directly embedded in the cover image. Secret message is first of all translated to binary stream of binary bit (digit) zero and one. Then consecutive occurrence of binary digit is counted. The count of consecutive occurrence is embedded in the digital image hence Indirect Data Embedding. The counter is of 3-bit. There we can count max occurrence to 7. One channel is use as a digit identifier. Here identifier used for identifying the binary digit (0/1), count of consecutive occurrence of that digit will be embedded in remaining two channels. Remaining two channels named channel-I and channel-II are used to hide the count of consecutive occurrence of binary digit. 1-LSB of channel II is used to hide 1-MSB of the counter. 2-LSBs of channel I are used to hide 2-LSB of the counter. Proposed algorithms (IDEIC) provides two layer of security. Proposed algorithm provides indirect data hiding. Thus ultimate benefit is indirect data hiding and implicit end marker. And visual quality is improved in IDEIC.

Data Hiding Concept

In any data hiding system, embedding concept has four elements. Inputs are secrete data which is to be hide, cover image which is redundant file hides data and stego key which defines the pattern for embedding data. Embedding algorithm which is use to decide the depth of eavesdropping from unauthorised person. And output image called stego image.

Further, this paper is divided in four sections. I. Introduction. II. Existing data hiding scheme. III. Proposed Method. IV. Analysis and Comparisons. IV. Conclusion.

II. Existing data hiding scheme

Segmenting and Hiding Data Randomly Based on Index Channel (SHDRIC)

In this scheme three channel of colour image is wisely used to hide the secret data. Khalaf and Suiaiman have done this work [4]. In this scheme data is segmented to two parts odd and even. Then one of three channels is used as index channel for hiding the secret data. Single pixel i.e. 24 bits are used to hide four bit of secret data. Now let's see how data is randomized. If number of 1's in index channel are odd then 4 bit from odd segment of secret data are embedded in other two channels, 2 bit in both channel. And if numbers of 1's in index channel are even then 4-bit from even data segment are embedded. Index channel in this scheme is not fix, sequentially all channels use as index channel. Same is illustrated in Table 1.

Table 1 Index Channel and Embedding in SHDRIC

No of 1's in index channel	Channel I	Channel II
Even	2 bit from even segment	2 bit from even segment
Odd	2 bit from odd segment	2 bit from odd segment

The same can be explain by simple example, here depending on number of 1's in index channel, 2-LSB bit from which segment are embedded is shown.

Index channel	channel-I	channel-II	
(1):11011011	101011**11**	110110**10**	Even
(2):11011001	101101**10**	110101**00**	Odd
(3):11010101	101110**00**	110111**01**	Odd

III. Proposed Algorithm

The proposed new method, "Indirect Data Embedding using Identifier Channel", use the color (RGB) image. The method proposed to hide the secrete data in digital color image by using concept of three separate channels. This scheme somewhat based on SHDRIC, just the idea of wise use of three channel is extracted from SHDRIC by Emad T. Khalf and Norrozila [7]. In this method two files are require two embed the secret information. The first file is secret message (information to be hiding) a message file may be plain-text, cipher-text or other image file, or anything that can be embedded in bit stream. The second file is redundant image file. This is extra innocent looking image that hide the secret information. This redundant image file is also called as cover image.

For understanding the embedding in image, basic of digital image is given. All images are store in computer as an array of points also called pixels. Gray scale images are of 8-bit i.e. pixel value are in range of 0 to 255. Color image are build of three monochromes Red (R), Green (G) and Blue (B). It is 24-bit image each monochrome is of 8-bit. For simplicity, color pixel require 24-bit, range is from 0 to 2^{24}-1(1677216). And is monochrome range, 0<= R, G, B<=255.

In the proposed method, Data is not directly embedded in the cover image. Secret message is first of all translated to binary stream of binary bit (digit) zero and one. Then consecutive occurrence of binary digit is counted. The count of consecutive occurrence is embedded in the digital image hence Indirect Data Embedding. The counter is of 3-bit. There we can count max occurrence to 7.

One channel is use as a digit identifier. Here identifier used for identifying the binary digit (0/1), count of consecutive occurrence of that digit will be embedded in remaining two channels. Remaining two channels named channel-I and channel-II are used to hide the count of consecutive occurrence of binary digit. 2-LSB of channel I are used to hide the 2-LSB of counter. 1-LSB of channel II is used to hide the 1-MSB of counter.

Insertion Algorithm

Now detailed explanation of insertion algorithm is provided. We scan the data stream and identify the digit for which are going to store count. After finding digit we replace the 1-LSB from identifier channel by that digit. Now this will be used for extracting data. Then count of consecutive occurrence of that digit is calculated. This counter is of 3-bit; counter will be stopped in two cases, case 1: if there is no consecutive digit or counter reach to its max count 7. We will hide this count in channel I and channel II. Two LSB of channel I will be replaced by 2-LSB of counter. 1- LSB of channel II will be replaced by MSB of counter. This process of continue till the end of secret data stream. No explicit information of secret data file is required unlike embedded image in SHDRIC also carry that information. Here implicit end is considered as counter embedded is Zero. Step-wise illustration of insertion algorithm is given as follows.

Inputs: Cover image of size m × n and secret message to be embedded
Outputs: Embedded image of size m × n
Method: Indirect insertion of secret data stream

Step 1: Convert secret data in to binary data stream
Step 2: Set counter of consecutive occurrence to zero
Step 3: Scan the next digit in the data stream and replace 1-LSB of the identifier channel with it.
Step 4: Count the consecutive occurrence of next found digit, counter will be increase each time until no more consecutive occurrence or counter reach to its max count 7.
Step 5: Replace two LSB of channel I with 2-LSB of count and replace one LSB of channel II with MSB of count.
Step 6: Repeat step 2 to 5 until complete secret data stream get embedded
Step 7: Replace two LSB of channel I with 00 and replace 1-LSB of channel II with 0 will be used as an end marker for extraction.

Extraction Algorithm

In this section let’s explain extraction algorithm in detail. We will extract 2 LSB from channel 1 and 1-LSB from channel II, concate it to get counter and calculate counter then construct bit stream using LSB of identifier channel and counter. We will repeat extraction steps 2 to 5 as shown below until end marker. From the bit stream constructed we will construct secret message. Step wise illustration is given as follows.

Inputs: embedded image of m*n size
Outputs: secrete message
Method: extract bit of channels
Step 1: Take null stream s
Step 2: Set counter to 0
Step 3: Extract 2 LSB from channel I and 1-LSB from channel II and concate it to get counter value
Step 4: Get digit from LSB of identifier channel
Step 5: Concate digit in stream s counter times
Step 6: Repeat step from 2 to 5 until filled counter is 0(i.e. end marker occur in embedded image)
Step 7: Construct secret message from bit stream

Now let’s explain new method by taking one example. In this example, data is taken as bit air plane 11100111111100010011111001010. Now let’s take some random five adjacent pixels and illustrate insertion as follows.

Identifier channel	channel I	Channel II
1101010**1**	001001**11**	1001011**0**
1101001**0**	001001**10**	1010111**0**
1110101**1**	010010**11**	1011011**1**
1101010**0**	010101**10**	1100001**0**
1011011**1**	100011**01**	1011001**0**

Here one can easily understand that in first pixel counter was 0011 i.e. 2- LSB in channel I and 1-MSB in channel II. And digit is 1 is in identifier’s LSB. Thus indirect data hidden is 111. Similarly in second pixel indirect data hidden is 00. And so on.

IV. Analysis and Comparisons

This Section provides the details of IDEIC algorithm Analysis and comparisons. This algorithm is implemented using Matlab. Here secret message is plain text file. Cover image used is lenna.png (color). Image size is 168×299 pixels. . Visual Quality is analysed. Original cover Image and stego Image are produced as a part of analysis to see Image perception. Also I have taken all (R, G and B) monochromes in account for visual perception all original and stego are produced to see the effectiveness. Also histogram of all are provided and found similar. All resulted figures are as follows:

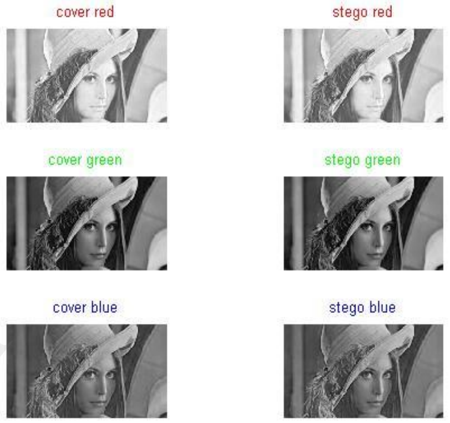

Fig. 1 Visual Quality of Monochromes

Figure 1 shows all monochromes of cover image as well as monochromes of stego image. It can be easily found that there is no visual different with respective monochromes.
Figure 2 shows histogram of all monochromes. Horizontal represent pixel level and vertical axis shows no. of pixel of that level. One can see that there is no visual different in histograms of respective monochromes.

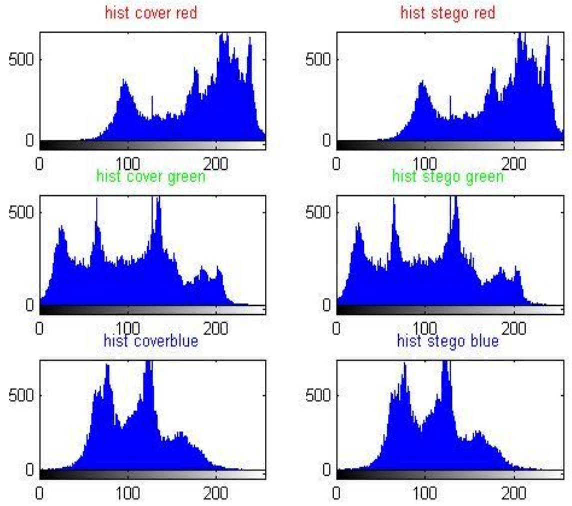

Fig. 2 Histograms of Monochromes

After embedding data, using both SHDRIC and IDEIC, bar is generated on stego image’s color components red, blue and green components on 50×299 Image block. And no of pixel changed with different level as higher level change degrades the image quality. One can see in fig 3 in existing more pixels are changed with level 2 and 3 while in proposed method more pixels are changed with level 1. Figure 3 illustrate it completely.

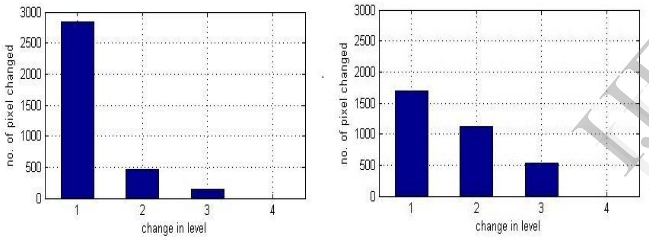

Fig. 3.1 Change in level in Red Channel a. by Proposed, b. by Existing

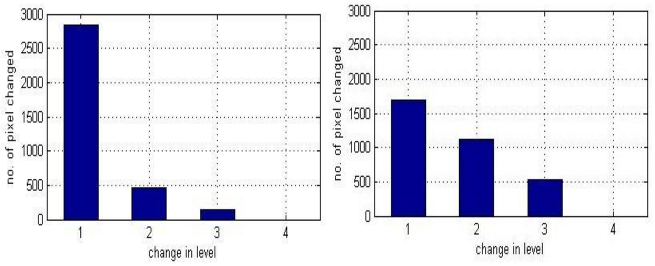

Fig 3.2 Change in level in Green Channel a. by Proposed, b. by Existing

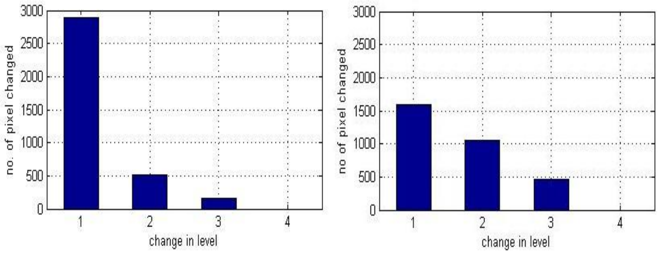

Fig 3.3 Change in level in Blue Channel a. by Proposed, b. by Existing

Comparison of SHDRIC and IDEIC

Here in this section, comparisons of SHDRIC and IDEIC is provided. Here in the both algorithms only 4-bit are replaced. Both algorithm has different method of hiding, in SHDRIC method of hiding is direct that is segmented data are get hidden as it was. In case of proposed scheme data hidden indirectly that is counter. In proposed algorithm stego image carries only secret information as there is implicit end marker. Both have two layer of security. Table 2 shows some parameter for comparison.

Table 2 Comparison of SHDRIC and IDEIC

	SHDRIC (existing)	IDEIC (proposed)
No. of Bit replaced per 24-bit	4	4
Method of hiding	Direct	Indirect
Information carries	Data and size of data	Only data
End marker	Explicit	Implicit
Advantage	Data Segmentation provides two layer of security	Data indirection provide two layer of security
Disadvantages	One channel used for index	One channel use for identifier

IV. Conclusions

Today, security of EMRS is very important and worthy. After theoretical analysis and comparisons it is derived that DHPVD has highest and good data embedding capacity and visual quality of original image is maintained. Thus DHPVD is good candidate for data hiding scheme for EMRs. If secret message is encrypted then information can be transmitted more securely on internet.

Acknowledgments

Karshan kandoriya wish to acknowledge and thanks H. M. Diwanji, for her guidance and help for doing this work. He also acknowledges Prof. Asst. Prof. D. A. Parikh, Head of computer department, and to all staff of computer department for full support for completion of this work. H.M. Diwanji wishes to acknowledge her family and staff of computer department.

References

[1] Chi-Kwong Chan and L.M. cheng "Hiding data in image by Simple LSB Substitution" The Journal of The Pattern Recognition Society, Aug. 2003, pp 470-474.

[2] E. Delp and O. Mitchell "Image Compression Using Block Truncation Coding" IEEE Transaction on Communication, vol. 27, no.9, pp. 1335-1342, 1979.

[3] J.K. Mandal and A. Khamrui "A Data Hiding Scheme for Digital Image Using Pixel Value Differencing" International Symposium on Electronic System Design 2011 pages 347-351.

[4] C. Rechberger, V.Rijman and N. Skelvos "The NIST Cryptographic Workshop on Hash Functions" IEEE Security and Privacy, vol. 4, pp. 54-56, Austria, Jan-Feb 2006.

[5] Karshan Kandoriya and H.M Diwanji "Analysis of Different Data Hiding Schemes for Electronic Medical Records System" in NCIET-2013, SRPEC, pp 325-328. (ISBN 978-81-925650-0-2).

[6] J.K. Mandal and A. Khamrui "A Data Hiding Scheme for Digital Image Using Pixel Value Differencing" International Symposium on Electronic System Design 2011 pp 347-351.

[7] Emad T. Khalf and Norrozila Sulaiman "Segmenting and Hiding Data Randomly Based on Index Channel" IJCSI International Journal of Computer Science Issue, Vol. 8, Issue 3, No. 1, May 2011, pp 522-529.