ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Data Embedding Using Adaptive Pixel Pair Matching

A.Pratap Reddy
Department of ECE,
JNTU Ananatapur,
MRRITS Udayagiri, Ap, India.

G. Sumathi
Department of ECE,
JNTU Ananatapur,
MRRITS Udayagiri, Ap, India.

D.Anusha
Department of ECE,
JNTU Ananatapur,
MRRITS Udayagiri, Ap, India.

P.Sainath Reddy
Department of ECE,
JNTU Ananatapur,
MRRITS Udayagiri, Ap, India.

P.Kishor
Department of ECE,
JNTU Ananatapur,
MRRITS Udayagiri, Ap, India.

ABSTRACT:

This paper proposes a new data-hiding method based on pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit Exploiting modification direction (EMD) and diamond encoding (DE) are two data-hiding methods proposed recently based on PPM. The maximum capacity of EMD is 1.161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighbourhood allowing sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, Experimental results reveal that the proposed method not only provides better performance than those of OPAP and DE, but also is secure under the detection of some well known steganalysis techniques.

Index Terms:

Adaptive pixel pair matching (APPM), exploiting modification direction (EMD), least significant bit (LSB), optimal pixel adjustment process (OPAP), pixel pair matching (PPM).

INTRODUCTION:

This paper proposes a new data-hiding method based on pixel pair matching (PPM). The basic idea of PPM is to use the values of pixel pair as a reference coordinate, and search a coordinate in the neighborhood set of this pixel pair according to a given message digit. The pixel pair is then replaced by the searched coordinate to conceal the digit Exploiting modification direction (EMD) and diamond encoding (DE) are two data-hiding methods proposed recently based on PPM. The maximum capacity of EMD is 1.161 bpp and DE extends the payload of EMD by embedding digits in a larger notational system. The proposed method offers lower distortion than DE by providing more compact neighborhood allowing sets and allowing embedded digits in any notational system. Compared with the optimal pixel adjustment process (OPAP) method, the proposed method always has lower distortion for various payloads. Experimental results reveal that the proposed method not only provides better performance than those of OPAP and DE, but also is secure under the detection of some well known steganalysis techniques.

Embedding Procedure:

Suppose the cover image is of size M x M , is the message bits to be concealed and the size of S is | S | . First we calculate the minimum such that all the message bits can be embedded. Then, message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

Input:

Cover image I of size M x M, secret bit stream S, and key kr .

Output:

Stego image I′, CB and kr .

1. Find the minimum B satisfying [M x M/2] ≥ | SB |, and convert S into a list of digits with a B-ary notational system SB .

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2. Solve the discrete optimization problem to find CB and B (x ,y)

3. In the region defined by B (0 ,0), record the coordinate (x^i, y^i) such that f(x^i y^i) = i, 0 ≤ i ≤ B-1 .
4. Construct a nonrepeat random embedding sequence Q using a key kr .

5. To embed a message digit SB , two pixels (x,y) in the cover image are selected according to the embedding sequence Q , and calculate the modulus distance [14] d = (SB-f(x,y)) mod B between SB and f(x,y) , then replace (x,y) with (x + x^d, y+ y^d)

6. Repeat Step 5 until all the message digits are embedded.

Extraction Procedure:

To extract the embedded message digits, pixel pairs are scanned in the same order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs.

Input:
Stego image I,CB ,(x,y) , and kr .

Output:
Secret bit stream S .

1.Construct the embedding sequence Q using the key kr .

2.Select two pixels (x',y') according to the embedding sequence Q .

3.Calculate f(x',y'), the result is the embedded digit.

4.Repeat Steps 2 and 3 until all the message digits are extracted.

Finally, the message bits can be obtained by converting the extracted message digits into a binary bit stream. Continue from the previous example. Let the scanned pixel pair be (x',y') = (9,12) . The embedded digit in a 16-ary notational system can be extracted by calculating f(9,12)= (9 + 6 x 12) mod 16 = 116 .

STEGANOGRAPHY: INTRODUCTION:

The fast developments in resource sharing through net-work essentially require security. Secured communication is possible by using different techniques such as water-marking, cryptography, Steganography etc. Digital watermark is a perceptually transparent system which is inserted in digital data using an embedding algorithm and key. Digital water marking is mainly used in copy right protection.

Cryptography is the class of information security and associated with scrambling text into cipher text. The various techniques of Cryptography includes such as microdots, merging words with images, and other ways to hide information in storage or transit. Steganography is a technique of hiding confidential information in the cover media. In image steganography the cover media used is an image and confidential may be an image or text. Image is preferred compare to other media be-cause it has more redundant information. The most commonly used cover media are text, audio files, video, images etc. The important aspects of steganography are Security, Capacity and Imperceptibility.

Different types of steganography: Steganography can be split into two types :

a) Fragile: This steganography involves embedding information into a file which is destroyed if the file is modified.

b) Robust: Robust marking aims to embed information into a file which cannot easily be destro

Steganography in Digital Mediums:

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security.

Image Steganography:

Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Network Steganography:

When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields [24].

Video Steganography:

Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (e.g., 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

Quality analysis and experimental results:

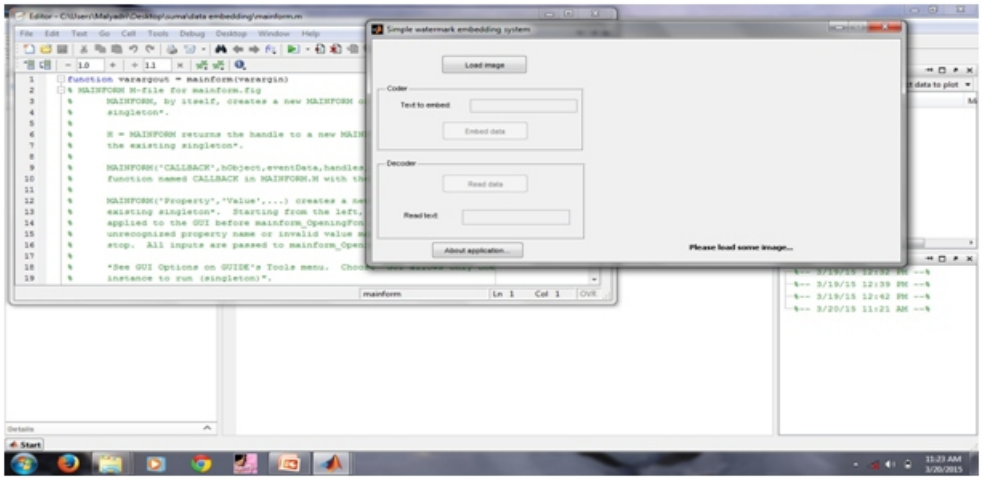
Image distortion occurs when data are embedded because pixel values are modified. We use MSE to measure the image quality.

$$MSE = 1/(M*M) \sum_{i=0}^{M} \sum_{j=0}^{M} (Pi,j - Pi,j)2$$

Where M x M denotes the image size, Pi,j and Pi,j denote the pixel values of the original image and the stego image, respectively .MSE represents the mean square error between the cover image and stego image. A smaller MSE indicates that the stego image has better image quality.

Fig: a.Cover Image b. Stego Image

Step by step process of this project is explained in the form screen shots

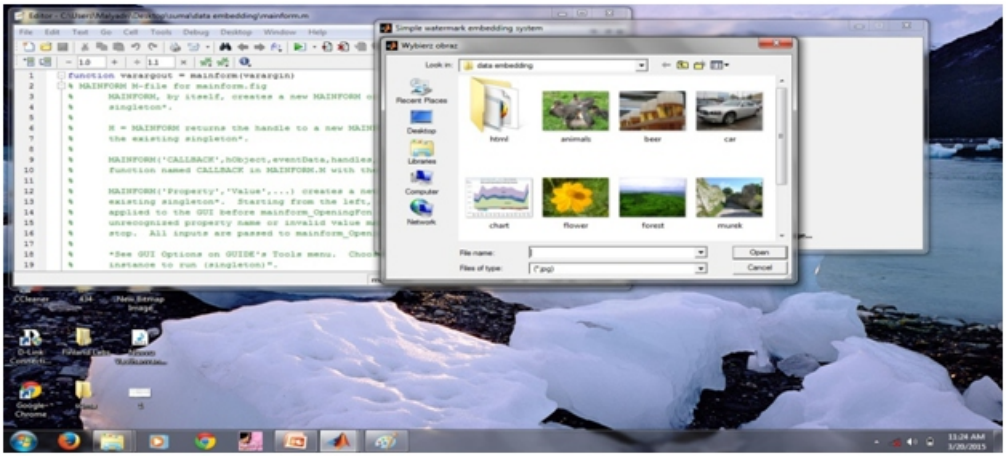


This is the first step in the process of running our project, immediately after running the program, a separate window and dialog will, this dialog box is in above fig foe the reference purpose

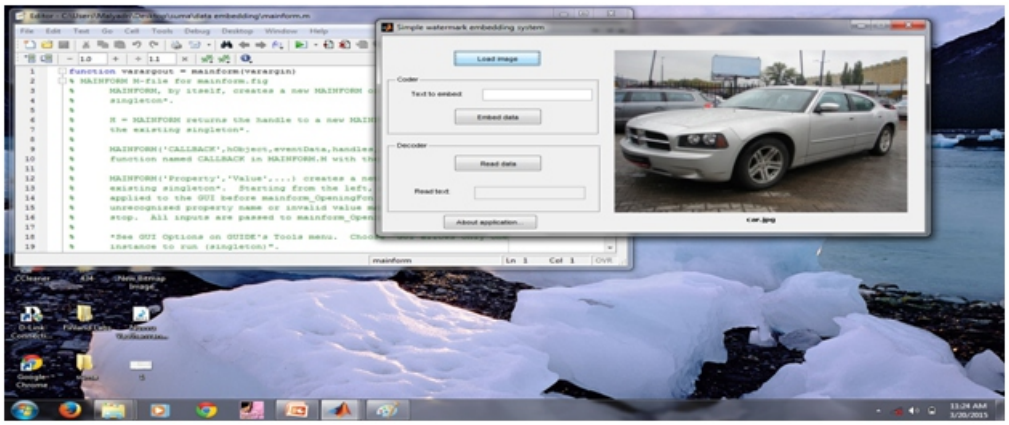
selection:

In the dialog box we have to click load image then we have to select the path from where we have to take image, after the completion of path selection then we have to select image from fixed folder. Then image is selected this is basic process for the experiment

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



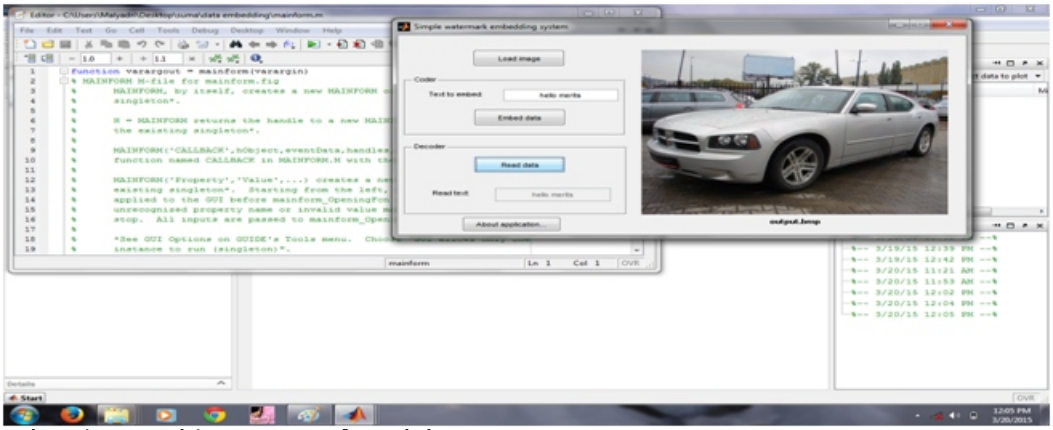
Sending secret data:



After selecting the image, the image will be displayed dialog box, to the left side of that box there will coder and decoder. In the coder first we have to enter the data which we want sent,

After the completion of process entering the data then press embedded data. Stegonography process occur for hiding the data in the picture it requires same pixel.

Read data:



The embedded in the picture, this process of read data will occur at receiver side. After receiving picture, we have to decode the data present in it. For this process in dialog box in the part decoder part we have to press read data. Then we can see the data present in the picture.

ADVANTAGES:

- It is used in a way of hiding, not the information but the password to reach that information
- Basically used in intelligent services.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

• Can be applied differently in digital image, audio & video file

• It can be done faster with the varying no of software's using different algorithms

DISADVANTAGES:

• HUGE data = huge file size, so some one can suspect about it

• During sending and receving information is maintained by the algorithms, and if the algorithms are known then its all over

• The confidentially of information is maintained by the algorithms are known then its all over

• The software can be misused if it goes in wrongs hands i.e., people with wrong intentions

APPLICATIONS:

• Confidential communication and secret data storing

Steganography provides us with:

• Potential capability to hide the existence of confidential data

• Hardness of detecting the hidden (i.e., embedded) data

• Strengthening of the secrecy of the encrypted data

• Protection of data alteration

• Access control system for digital content distribution

• Media Database systems

• Usage in modern printers

• Alleged use by terrorists

• Alleged use by intelligence services

CONCLUSION:

This paper proposed a simple and efficient data embedding method based on PPM. Two pixels are scanned as an embedding unit and a specially designed neighborhood set is employed to embed message digits with a smallest notational system. APPM allows users to select digits in any notational system for data embedding, and thus achieves a better image quality. The proposed method not only resolves the low-payload problem in EMD, but also offers smaller MSE compared with OPAP and DE. Moreover, because APPM produces no artifacts in stego images and the steganalysis results are similar to those of the cover images, it offers a secure communication under adjustable embedding capacity

FUTURE SCOPE:

This paper proposed a simple and efficient data embedding method named as Secured APPM based on APPM. In that two pixels are used as an embedding unit and a specially designed compact neighborhood set is used to embed secret message digits in to a smallest possible notational system by allowing users to select digits in any notational system for the data embedding. The proposed method not only resolves the low-payload problem in EMD, but also offers smaller MSE than OPAP, DE and APPM. It also provides a better image quality because Secured APPM does not produce any artifacts in stego images.

The steganalysis results of stego images are similar to those of the cover images, which offer a secure communication under adjustable embedding capacity. It also contains additional features such as digital watermark and encryption of secret messages for the provision of more security. The secured APPM technique is also able to hide all different types of data provided to it in languages like English, Marathi, and Hindi etc. As well as this technique is secure under the detection of some well-known steganalysis techniques. All these various features made a Secured APPM technique a straightforward, economical embedding method for the data hiding. In future Secured APPM may have a chance to increase the capacity of data embedding in the cover images of it. Also there may be a chance of little improvement of MSE in it and chance to provide more

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

REFERENCES:

- J. Fridrich, Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge, U.K.: Cambridge Univ. Press, 2009.

- N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security Privacy, vol. 3, no. 3, pp. 32–44, May/Jun. 2003.

- A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, pp. 727–752, 2010.

- T. Filler, J. Judas, and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization," in Proc. SPIE, Media Forensics and Security, 2010, vol. 7541, DOI: 10.1117/12.838002.

- S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar. 2006.

- J. Fridrich, M.Goljan, and R.Du, "Reliable detection of LSB steganography in color and grayscale images," in Proc. Int. Workshop on Multimedia and Security, 2001, pp. 27–30.

- A. D. Ker, "Steganalysis of LSB matching in grayscale images," IEEE Signal Process. Lett., vol. 12, no. 6, pp. 441–444, Jun. 2005.