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

Data Hiding Technique Using Pixel Masking & Message Digest Algorithm (DHTMMD)

Avinash
Pursuing M.Tech in VLSI Design & Embedded Systems,
Lingaraj Appa Engineering College,
Bidar, Karnataka, India.

Vivek Jaladi
Asst Prof & H.O.D,
Dept of ECE,
Lingaraj Appa Engineering College,
Bidar, Karnataka, India.

Abstract:

In this paper a data hiding technique using pixel masking and message digest algorithm (DHTMMD) has been presented. Here we are embedding a secret message/image/video into source image/video. A standard 3 x 3 mask of secret message/image bits are chosen and are embedded in a single bit position. From secret message/image a message digest MD-5 has been generated and it has to be inserted into source image for additional security purpose. Result is analyzed in terms of SNR.

Keywords:

DHTMMD, Pixel masking, Message digest, Data Communication, and GUI.

I.INTRODUCTION:

At present the internet and digital media are getting more and more popular. Internet is one of the rapidly growing technologies in the present era. Since internet is a public network, hence the requirement of secure data transmission is also increased. Nowadays it's really a big challenging task to hide the data across the network. Data hiding is the process of embedding information into digital content without changing its original perception. By embedding the information within the source data we can justify the authentication, identification and ownership of the data. Data hiding is the art and science of hiding data in such a way that, no one can realizes there is a hidden secret data except sender and the intended recipient. There are several tools & techniques to protect the originality of the image/video. In this paper DHTMMD technique has been proposed to perform the task. J.K Mandal et al. [1] proposed paper by embedding an authenticated message/image in to image/video.

The bits from authenticating message/image are embedded under each byte of the source image by choosing a standard 3 x 3 masking in a row major order. In this proposed technique the authentication process is performed by mathematical operations on 3 x 3 masks to insert bits into the source image byte. The insertion is done through mask selections in row major order for the entire image bytes so that it provides extra level of security. A message digest MD5 also been generated from authenticating message/image and it has to be inserted into the source image for additional security purpose. They compared there performance with S-Tools technique and concluded that there proposed paper performs better.

Shikha et al. [2] proposed paper Steganography: The art of hiding text into image using matlab. They proposed a method that hides the secret messages into the image using matlab. Matlab is not only programming software but also a programming environment. They encrypt the text using play fair method. First the text is encrypted using fair play method. Then they encode the encrypted text in to the image file using matlab. At the recipient end they decode the image file and extraction of text using matlab code. Finally they decrypt the text using play fair method. In their proposed technique capacity of data hiding to hide the secret messages are high.

Nammer N. EL-Eman et al. [3] proposed a steganography algorithm to hide the large amount of data with high security. They implemented new algorithm for hiding a large amount of data file into color bitmap image. The data file may be image file, audio file or text file. They used adaptive image filtering and adaptive image segmentation with bits replacement on the appropriate pixels. These pixels are selected randomly rather than sequentially.

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

The proposed algorithm allows hiding data inside other data with hopes that except intended sender and recipient no one can think to examine the contents of the file. The algorithm was described by pseudo code so that it was possible to implement a steganography algorithm to hide a large amount of data into bitmap image. They used three layers of security to secure data by obscuring the content in which it was transferred, to make it different to break through the encryption of the input data. They proposed confused steganalysis too. They compared their result with S-Tools algorithm and shown that there proposed work embeds a large amount of data with high quality output.

R. Chandramouli et al. [4] proposed work they considered image based steganography techniques. They showed that an observer can distinguish between images carrying hidden messages and images that do not carry a message. They desired a close form expression for detection and false alarm in terms of the number of bits that are hidden. There results provide an upper bond on steganography capacity. By this they showed that the number of bits that can be embedded increases significantly. That is how many bits they can embed before the warden can reliably differentiating between stego objects and cover objects. In future they are going to address an active warden who injects noise in the cover object.

S. Dumitrescu et al. [5] proposed an algorithm for detecting LSB steganography in digital signals such as images and audios. It is shown that the length of hidden messages embedded in the LSBs of signal samples can be estimated with high precision. This steganography approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. Their proposed algorithm is simple and fast. Possible attacks to the proposed steganalytic method are examined and corresponding counter measures are discussed. They conducted experiments on a set of continuous tone images. Section II of the paper deals with the proposed technique. Results are given in section III. Conclusions are mentioned in section IV.

II.THE TECHNIQUE:

The presented DHTMMD embeds the secret message or image or video into source image or video.

A standard 3 x 3 mask is chosen from the source image matrix in row major order and single bit is inserted into each byte from secret message or image. The insertion positions of the secret bits are calculated through a mathematical function, which depends on the absolute position of the pixel within the mask. The mask of size 3 x 3 is selected from the source image sequentially in row major order for the whole secret image. A 128-bits MD5 key is generated from the secret message/image and is to be inserted in to the source image in the same manner. We have split our presented work into two schematic diagrams. One is hiding message/image into image. Another is hiding an image/video into video. In our presented work we are working on images that are in bitmap format and videos that are in AVI (Audio Video Interleave) format. Our presented functions are explained clearly in the following sections.

2.1.Hiding message/image into image and extraction of it.

Figure 2.1 shows the schematic diagram of hiding secret message/image into source image. Here the size of the secret image should be less than three times of the source image in case of hiding an image into another image. Algorithm for insertion and extraction for hiding message/image into image is described in following selections.

A.Algorithm for insertion:

1)Read one character of secret message if hiding message into image else read one pixel of secret image if hiding an image into an image.

2)For each secret message/image byte do.

- Read source image matrix of size 3 x 3 mask in row major order.
- Extract the message/image bit one by one.
- Compute the position within in the mask where secret message/image bit is to be inserted.
- In the computed position the authenticating image bit has to be replaced within the mask.

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

3)Repeat the procedure 1 and 2 for the whole secret image size, content and MD5.

4)Stop.

B.Algorithm for extraction:

1)Read embedded image mask of size 3 x 3 in row major order.

2)For each embedded image mask to do

- Compute the position within the mask in row major order where secret bit is available.
- Extract the message/image bit.
- Replace message/image bit position in the mask image byte by '1'.
- For each 8 bits extraction constructs one pixel of an image.

3)Repeat procedure 1 and 2 to complete the extraction process as per the size of the secret image/

4)Stop.

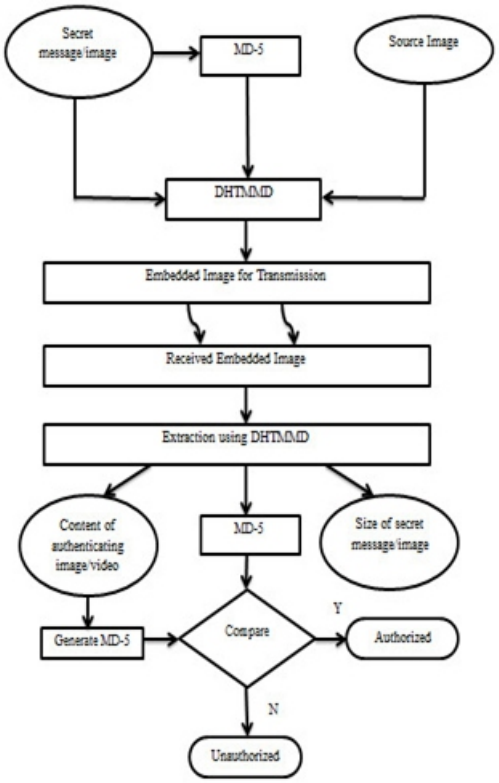

Figure 2.1: Schematic diagram for hiding message/image into image and extraction of it.

2.2.Hiding image/video into video and extraction of it.

Figure 2.2 shows the schematic diagram of hiding secret image/video into source video. Algorithm for insertion and extraction for hiding message/image into image is described in following selections.

A.Algorithm for insertion:

1)Read one pixel of secret image if hiding an image into video. In case of hiding video into video, frames have to be separated from the videos before embedding.
2)For each secret image or frames byte do

- Read source image or frame matrix of size 3 x 3 mask in row major order.
- Extract the image bit one by one.
- Compute the position within the mask where secret image bit is to be inserted.
- Replace the secret image bit in the computed position within the mask.
- Convert frames into video format. And this embedded video is transmitted.

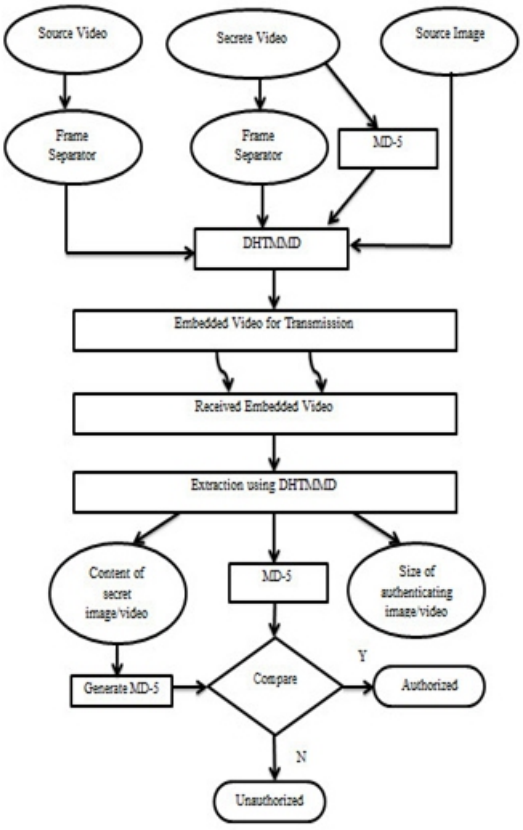

Figure 2.2: Schematic diagram for hiding image/video into video and extraction of it.

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

3)Repeat step 1 and 2 for the whole secret image size or for total number of frames, content and MD5 key.

4)Stop.

B.Algorithm for extraction:

1)The frames of the embedded video have to be separated. Read embedded video mask of size 3 x 3 in row major order.

2)For each mask do

- Compute the position within the mask in row major order where secret image bit is available.
- Extract the image bit.
- Replace image bit position in the mask image byte by '1'.
- For each 8 bits extraction construct one image pixel.

3)Repeat step 1 and 2 to complete decoding as per the size of the secret video.

4)Stop.

III.RESULTS:

In this section results are discussed. As we implemented this presented work on MATLAB software of version R2013a. Here we discussed our results in GUI windows. GUI can be created by typing 'guide' in the command window of the matlab software. Then select BLANK GUI and select OK. GUI window will appear in front of us. Select the push buttons, axis, pop-up menus et al. as per programmer required. In 3.1 section we selected 'world cup.bmp' as source image and 'we will take it back' as our secret message. This secret message is embedded in source image. We extracted this message by selecting the embedded image as input at the extraction side. In 3.2 section we selected 'Dhoni.bmp' as source image and 'world cup.bmp' as secret image. The 'world cup.bmp' image is embedded in the 'Dhoni.bmp' image. Weextracted the secret image by selecting embedded image as input at the extraction side. In section 3.3 we selected 'dhoni.avi'as source video and 'world cup.bmp' as secret image.

Here the secret image 'world cup.bmp' gets embedded in the source video file. We extracted this secret image by selecting the embedded video as input to the extraction side. In 3.4 we selected two video files. We selected 'spider.avi' as source video and 'atal.avi' as secret video. The secret video gets embedded in the source video file. We extract the secret video by selecting this embedded video as input at the extraction side.

3.1.Embedding a secret message into source image and extraction of secret message from the embedded image.

Figure 3.1: Embedding of message into an Image.

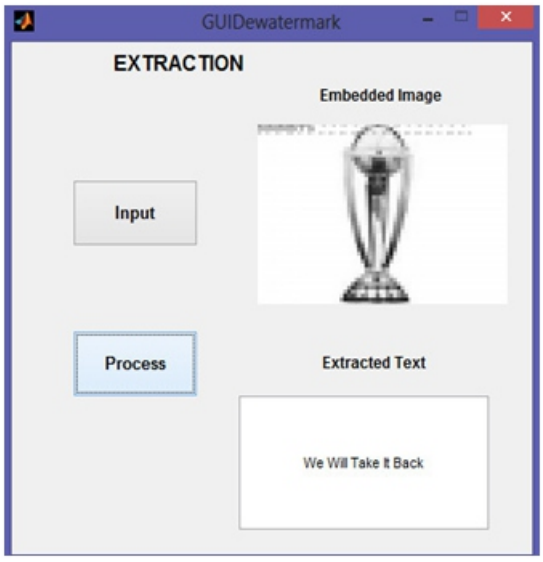

Figure 3.2: Extraction of message from Image.

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

3.2.Embedding a secret image into source image and then extraction of secret image from the embedded image.

Figure 3.3: Embedding of an Image into an Image.

Figure 3.4: Extraction of an Image from Image.

3.3. Embedding a secret image into source video and then extraction of secret image from the embedded video.

Figure 3.5: Embedding of an Image into Video.

Figure 3.6: Extraction of Image from Video.

3.4.Embedding a secret video into source video and then extraction of secret video from the embedded video.

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

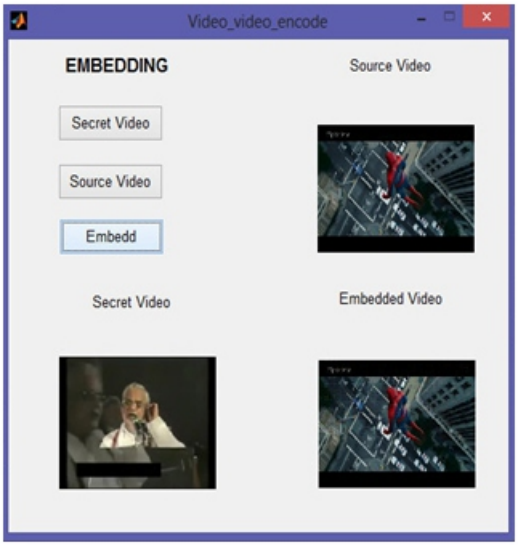

Figure 3.7: Embedding Video into Video.

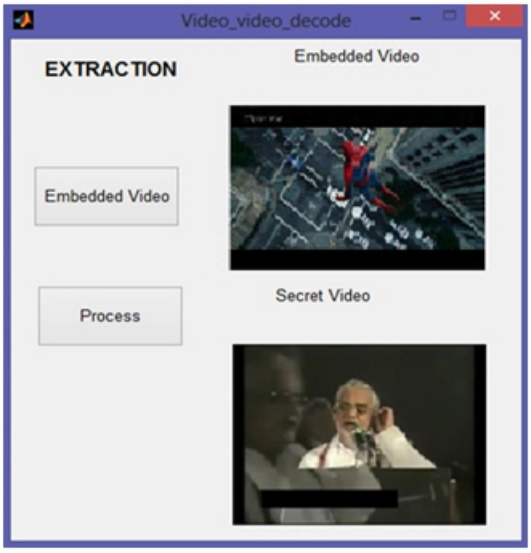

Figure 3.8: Extraction of Video from Video.

Figure 3.9shows the SNR of secret image, embedded image and that of extracted image using DHTMMD. For the purpose of analyzing the SNR, we are embedding the secret image 'world cup.bmp' into the source image 'Dhnoi.bmp'. The SNR value of the secret image before its get embedded is 13.9243. Once it gets embedded with the source image file then the SNR value of the embedded image is 12.7900. After extraction of the secret image the SNR value of the extracted secret image is 13.9243. The result shows clearly that the secret image has been recovered without any degradation in the SNR value. The result of this is shown in figure 3.9.

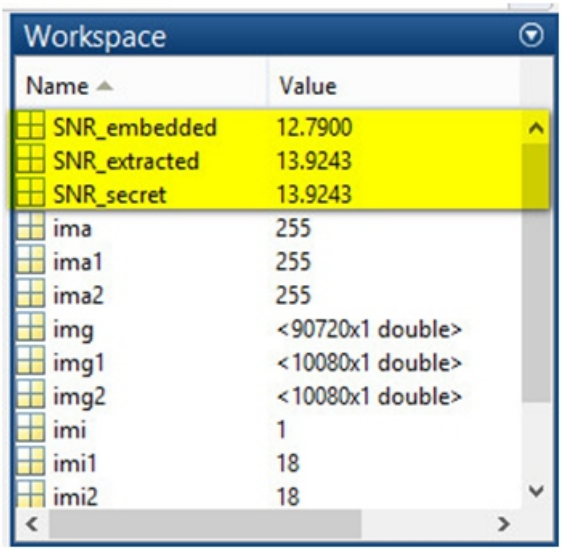

Figure 3.9: SNR of secret image, embedded image and an extracted image using DHTMMD.

IV.CONCLUSION:

The presented work is powerful for secure communication. From the analysis of the results it is clear that the image quality (like brightness, sharpness) distortion is negligible. As all are embedded within the source image/video like size of secret image/video, content of it and MD5 key within the source image/video hence no other information is needed for decoding at receiver end. Finally, it can be easily extended at the recipient.

Results are analyzed in terms of SNR of source image, an embedded image and an extracted image using DHTMMD. And this is compared with the LSB technique. The presented work better security and higher embedded capacity.

REFERENCES:

[1]N. Ghoshal, A. Sarkar, D. Chakraborty, S. Ghosh,J. K. Mandal, "Masking based data hiding and image authentication technique (MHDIAT)," Advanced Computing and Communications, ADCOM 2008, pp. 119-122, 2008.

[2]Shika and VidhuKiranDutt, "Steganography: The art of hiding text in image using MATLAB," International of Advanced Research in Computer Science and Software Engineering ISSN 2277-128X vol. 4, Issue 9, pp. 822-828, Sept. 2014.

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

[3]Nameer N. EL-Emam, "Hiding a large Amount of data with High Security Using Steganography Algorithm," Journal of Computer Science ISSN 1549-3636, vol. 3, no. 4, pp. 223-232, 2007.

[4]R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Proc. of ICIP, Thissaloniki, pp. 1019-1022, Greece, 2001.

[5]S. Dumitrescu, W. Xiaolin and Z. Wang, "Detection of LSB steganography via sample pair analysis," In: LNCS, vol. 2578, Springer-Verlag, New York, pp. 355-372, 2003.

[6]Avinash and VivekJaladi, "Hiding an image into multiple videos using message digest algorithm," International Journal & Magazine of Engineering Technology, Management and Research ISSN 2348-4845 vol. 2 (2015), Issue no. 5 (May), pp. 135-140, May 2015.

About Author:

Avinash
was born in February 1992, completed his Bachelor of Engineering in Electronics and Communication Engineering, currently pursuing M. Tech VLSI Design & Embedded System in Lingaraj Appa Engineering College. He is interested in Embedded Systems and has capability of writing own programs in assembly language 8051 microcontroller.

Vivek Jaladi
Asst Prof & H.O.D,Dept of ECE,
Lingaraj Appa Engineering College,
Bidar, Karnataka, India.