

Hiding an Image into Multiple Videos Using Message Digest Algorithm

Avinash

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

Vivek Jaladi

Asst. Prof & H.O.D of E&CE,
Lingaraj Appa Engineering College,
Bidar, Karnataka, India.

Abstract:

In this paper we propose hiding an image and extraction procedure using message digest algorithm. We are hiding an image in AVI (Audio Video Interleave) videos & extraction of an image from it. By choosing standard 3 X 3 mask of an authenticating image bits are embedded in a single bit position. From authenticating image a message digest (MD-5) has been generated & to be inserted in the source image for additional security. Results were analyzed in terms of SNR, where proposed technique shows better performance.

Keywords:

Pixel masking, Message digest, Frames, GUI, and Steganography.

I.INTRODUCTION:

Currently, internet and digital media are getting more & more popular. So, requirement of secure transmission of data also increased. Nowadays it's a big challenge to hide data across the network. Data hiding is the process of embedding information inside a source data without changing its perceptual quality. Data hiding is the art and science of writing hidden image in such a way that no one apart from the sender and intended recipient even realizes there is a hidden image. Generally, in data hiding, the actual information is not maintained in its original format. It is converted into an alternative multimedia file like image, video or audio. This apparent image is sent through the network to the recipient, where the actual image is separated from it. In this proposed paper we are hiding an image into video, then the embedded video is sent through the network to the recipient, where the actual image is going to separate from it. We are using message digest algorithm technique.

The proposed paper has a wide range of applications to protect data from potential enemy. There are several tools & techniques to protect the originality of the image/video. In this paper using message digest algorithm this technique has been proposed to perform the task. Embedded information within a source image is not visible [6, 9], and this key concept for hiding an image. In steganography [5, 7] theory the hidden data may be secret message or secret image whose presence within the source data should be undetectable. Hiding a message/image into an image without altering its visibility and properties is a challenging task.

The least significant bit (LSB) replaced by Chandrmouli et al. [5] by masking, filtering & transformation on the source image is a common method to make these alterations. Dumitrescu et al. [7] proposed an algorithm for detecting LSB steganography. Pavan et al. [8] used entropy based technique for detecting the suitable areas in the document image where data can be embedded with minimum distortion. S-Tools [12] performs by spreading the bit pattern of the file that you want to hide across least significant bits (LSBs) of the color levels in the image to prevent the prediction of potential enemy.

In recent works [2,9], it has been shown that digital data can be effectively hidden in an image so as to satisfy the criteria that the degradation to the source image is imperceptible and it should be possible to recover the hidden under a variety of attack.

This paper presents hiding an image into multiple videos using message digest algorithm. Here we have to insert the secret image into source videos. The present work emphasizes on information and protection of an image against potential enemy. The produced output will be authenticated image. Like this we can hide a single image into multiple videos.

Section II of the paper deals with the proposed technique. Working algorithm is mentioned in section III. Results are given in section IV. Conclusion is mentioned in section V.

II. THE TECHNIQUE

A. Bit plane in Image

A bit plane of an image is a set of bits corresponding to a given bit position in each of the binary numbers representing the signal. For example, for 16-bit data representation there will be 16-bit planes. The first bit plane contains the set of the most significant bit (MSB) and the 16th bit plane contains the least significant bit (LSB).

If a bit on the n th bit plane on an m -bit data is to set 1, it contributes a value of $2^{(m-n)}$; otherwise it contributes nothing. For example, in the 8-bit value 10000101 (133 in decimal), the bit planes work as follows:

Table 1: An 8-bit plane contribution.

Bit Plane	Value	Contribution	Running Total
1 st	1	$1 * 2^{(8-1)} = 128$	128
2 nd	0	$0 * 2^{(8-2)} = 0$	128
3 rd	0	$0 * 2^{(8-3)} = 0$	128
4 th	0	$0 * 2^{(8-4)} = 0$	128
5 th	0	$0 * 2^{(8-5)} = 0$	128
6 th	1	$1 * 2^{(8-6)} = 4$	132
7 th	0	$0 * 2^{(8-7)} = 0$	132
8 th	1	$1 * 2^{(8-8)} = 1$	133

Bit plane is sometimes used as synonymous to bitmap. One aspect of using bit plane is determining whether a bit plane is random noise or contains significant information. One method for calculating this, compare each pixel (X, Y) to three adjacent pixels (X-1, Y), (X, Y-1) and (X-1, Y-1). If the pixel is the same as at least twice of the three adjacent pixels, it is not noise. A noisy bit plane will have 49-51% pixels that are noisy.

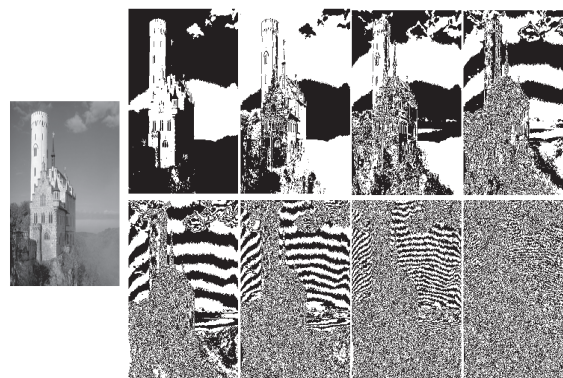


Figure 1.1: Possibility of noisy figures.

B. Proposed Methodology

The proposed technique enables authenticating image Alm, n of size $m \times n$ bits for the purpose of authentication of the source video. First the source videos are converted to image depending on number of frames.

Then for converted images a standard 3×3 mask where chosen in row major order and single bit into each byte from authenticating image is inserted.

The insertion position of the authenticating bit is calculated through a mathematical function which depends on the position of the pixel within the mask. In addition a 128-bit MD-5 key is generated from the authenticating image and is inserted it into the source video.

Figure 1.2 represents the flow diagram of the proposed technique. The block hiding an image into multiple videos using message digest algorithm performs the authentication process by embedding image & a MD-5 key. Here we selected two source videos.

Each videofiles are converted into images depending on the number of frames source video file. The authenticated video may be sent to transfer the secret image.

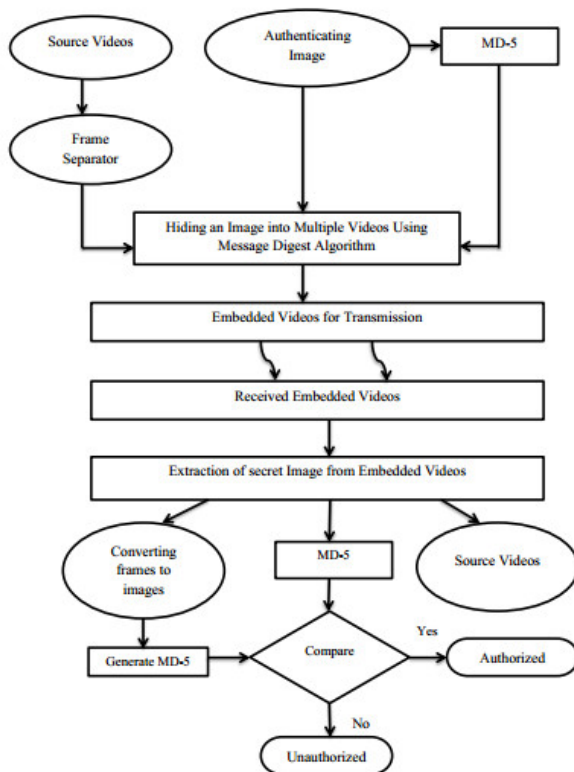


Figure 1.2: Schematic flow diagram of Image hiding and extraction using message digest algorithm.

While extracting of an image from embedded videos, we have to convert the videos into image. From these converted images we are going to generate MD-5 key & compare it with the actual MD-5 key generated while embedding. If both matches, then it is going to treat as current user as authorized. Otherwise user will be treated as unauthorized. It is also possible to reconstruct the source videos.

III. WORKING ALGORITHM

We divided the algorithms into two parts: one is embedding process & the other extraction process.

A. Algorithm for embedding an image.

[1] Read the authenticating image.

[2] Read the source video.

[3] Convert source video into image which depends on number of frames that video file

[4] For each frame to do is

- Extract the image bit one by one.
- Compute the position within the mask where authenticating image bit is to be inserted.
- In the computed position the authenticating image bit has to be replaced within the mask.

[5] Repeat the procedure 3 to 4 for other source videos.

[6] Stop.

B. Algorithm for extraction of an image.

[1] Read the embedded video file.

[2] Convert embedded video into image which depends on number of frames that video file.

[3] For each frame of embedded file is to do

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

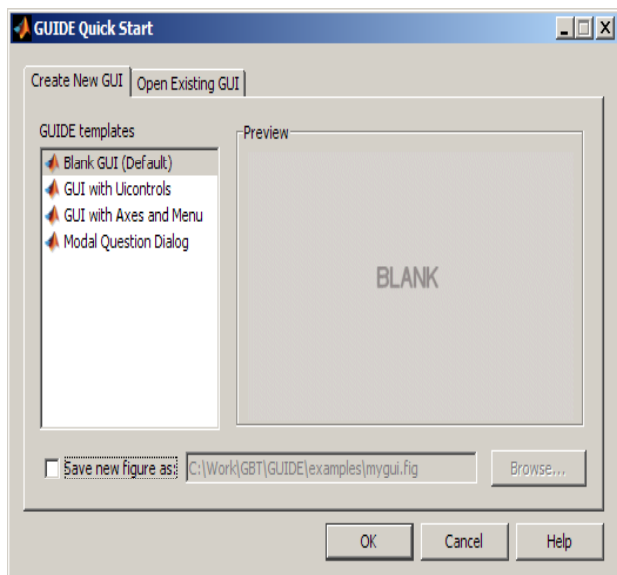
[4] Repeat the procedure 2 and 3 for other embedded videos.

[5] Stop.

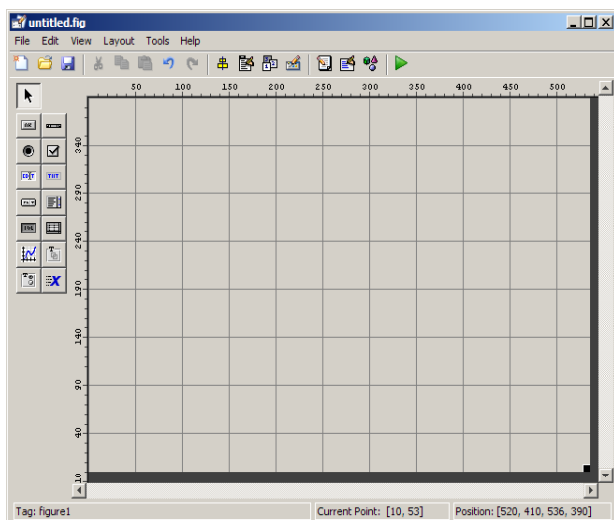
IV. RESULTS:

In this section results are discussed. Here we are using MATLAB R2013a software for implementing our proposed technique. We are creating graphical user interference (GUI) with GUIDE. GUIDE, the MATLAB GUI Development Environment, provides a set of tools for creating GUIs. Following are the steps to be followed in order to create GUI:

1. Start GUIDE by typing guide at the MATLAB prompt.



2. In the GUIDE Quick Start dialog box, select the Blank GUI (Default) template, and then click OK.

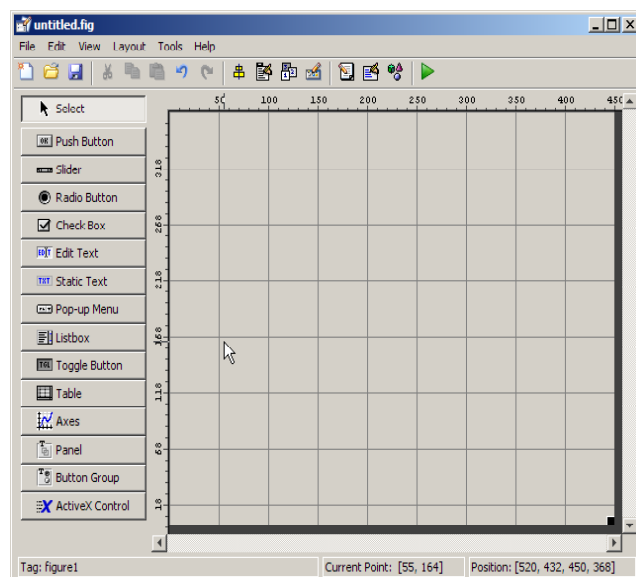


3. Display the names of the GUI components in the component palette:

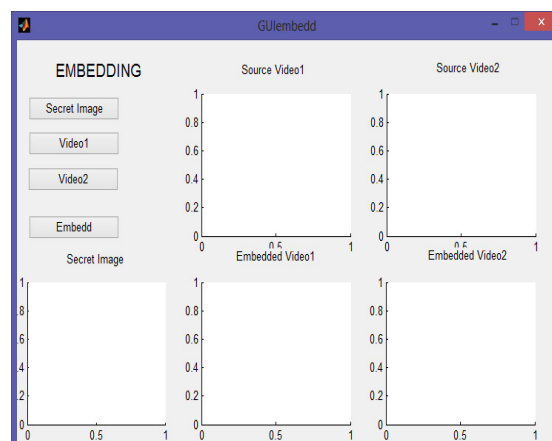
a. Select File > Preferences > GUIDE.

b. Select Show names in component palette.

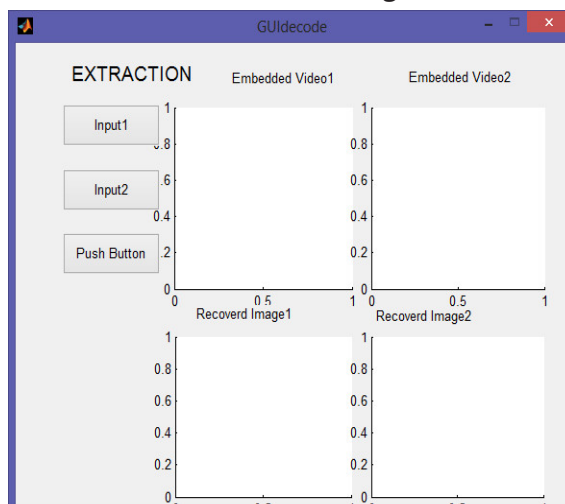
c. Click OK.



4. By selecting push buttons et al. the following GUI will be created for embedding an image.



5. By selecting push buttons et al. the following GUI will be created for extraction of an image.



We are embedding gold coin in to two video files. We select atal.avi as one of video file and spider.avi as another video file. Figure A shows the output of embedded videos. Figure B shows the extraction of images from embedded videos.

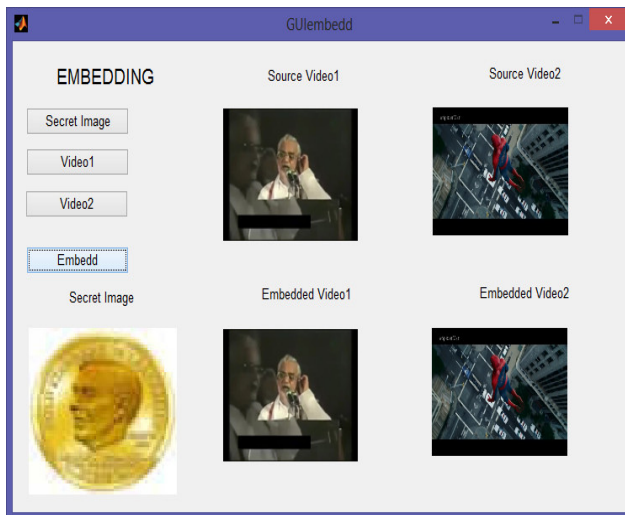


Figure A: Embedding of a Videos.

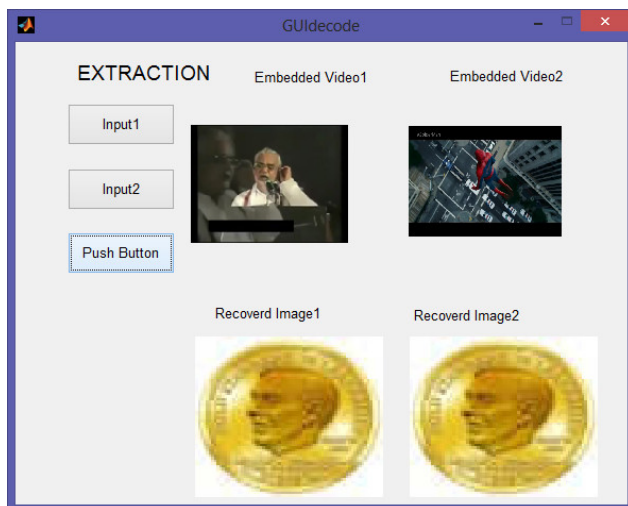
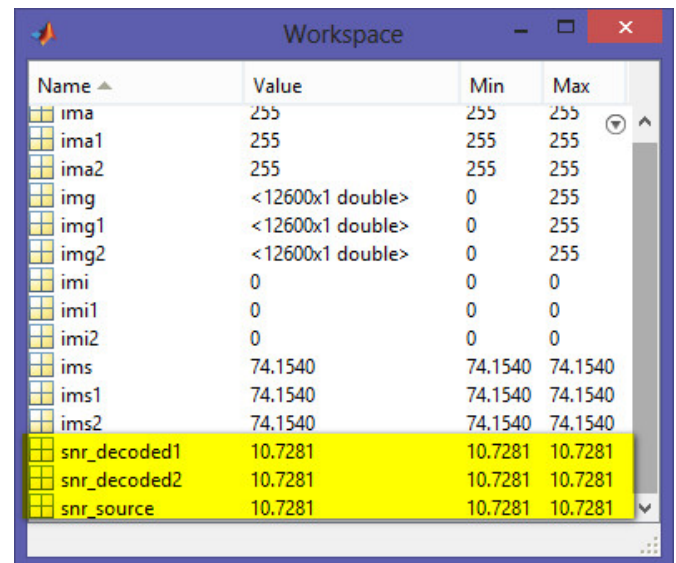


Figure B: Extraction of images from embedded Videos.

Signal-to-noise ratio (SNR) has been performed for source image & the extracted image. The values for these images are represented in figure C.



Name	Value	Min	Max
ima	255	255	255
ima1	255	255	255
ima2	255	255	255
img	<12600x1 double>	0	255
img1	<12600x1 double>	0	255
img2	<12600x1 double>	0	255
imi	0	0	0
imi1	0	0	0
imi2	0	0	0
ims	74.1540	74.1540	74.1540
ims1	74.1540	74.1540	74.1540
ims2	74.1540	74.1540	74.1540
snr_decoded1	10.7281	10.7281	10.7281
snr_decoded2	10.7281	10.7281	10.7281
snr_source	10.7281	10.7281	10.7281

Figure C: SNR of secret and extracted images.

V.CONCLUSION:

The proposed technique is powerful for communication of secret data. In this paper we propose a method that hides the secret image in to multiple videos. Since all are embedded within the source video.

Hence no need of other information required for decoding at the receiver end. Finally, it can be easily extended, and it has better data security and higher embedded capacity.

ACKNOWLEDGMENT:

The author expresses the deep sense of gratitude to the Dept. of VLSI Design and Embedded system, Lingaraj Appa Engineering College, Bidar, where the work has been carried out.

REFERENCES:

- [1]N. Ghoshal, A. Sakar, J. K. Mandal, "Masking based data hiding and image authentication technique.
- [2]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.

[3]P. Amin, N. Lue and K. Subbalakshmi, “Statistically secure digital image data hiding”, IEEE Multimedia Signal Processing MMSP05, pp. 1-4, Shnghai, China, Oct. 2005.

[4]B. Chen and G. W. Wornel, “Quantization index modulation: A class of provably good methods for digital watermarking and information embeddeing”, IEEE Trans. On Info. Theory., vol. 47, no. 4, pp-1423-1443, May 2001.

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

[6]C. Y. Lin and S. F. Chang, “A robust image authentication method surviving JPEG lossy compression,” Proc. SPIE, vol. 3312, San Jose, pp. 296-307, Jan 1998.

[7]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.

[8]H. H. Pang, K. L. Tan and X. Zhou, “Steganography schemes for file system and B-tree,” IEEE Trans. On Knowledge and Data Engineering, vol. 16, pp. 701-713, Singapore, June 2004.

[9]P. Moulin and M. K. Mihcak, “A framework for evaluating the data-hiding capacity of image sources,” IEEE transactions on Image Processing, vol. 11, pp. 1029-1042, Urbana, Illinois, Sept. 2002.

About author:



Avinash

was born in February 1992, completed his bachelor of engineering in electronics and communication, currently pursuing M.Tech VLSI Design & Embedded Systems in Lingaraj Appa Engineering College. He is interested in embedded systems and has capability of writing own programs in assembly language 8051 microcontroller.