International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 2, Issue 12, December 2015)

Secret Communication through Video for Defense Applications

Tabasum Guledgudd[1]
H.OD & Associate Professor
Secab Institute of Engineering and Technology,
nauraspur, Bagalkot Road,Vijayapur.
tabuag85@gmail.com

Easari. Parusharamu[2]
Assistant professor
Sri Indu College of Engineering and Technology,
Shariguda(V), RR Dist. Hyderabad.
parushuece@gmail.com

Abstract: The aim of this review is to study the methods of steganography using the video file as a cover carrier. The video based steganography can be used as one video file, separated images in frames or images and audio files. Since that, the use of the video based steganography can be more eligible than other multimedia files. As a result of this study, the video based steganography has been discussed and the advantages of using the video file as a cover carrier for steganography have been proposed. Steganography is the technique of hiding confidential information within any media. Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between the two is in the appearance in the processed output; the output of steganography operation is not apparently visible but in cryptography the output is scrambled so that it can draw attention. In this article we have tried to elucidate the different approaches towards implementation of steganography using 'multimedia' file (text, static image, audio and video) and Network IP datagram as cover. Also some methods of steganalysis will be discussed.

Keywords: steganography, Watermark, digital, Video, CMV

I. INTRODUCTION

Data hiding and watermarking in digital images and raw video have wide literature. This paper targets the internal dynamics of video compression, specifically the motion estimation stage. We have chosen this stage because its contents are processed internally during the video encoding decoding which makes it hard to be detected by image steganalysis methods and is lossless coded, thus it is not prone to quantization distortions. In the literature, most work applied on data hiding in motion vectors relies on changing the motion vectors based on their attributes such as their magnitude, phase angle, etc.

The data bits of the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold, and are called candidate motion vectors (CMVs). A single bit is hidden in the least significant bit of the larger component of each CMV, the data is encoded as a region where the motion estimation is only allowed to generate motion vectors in that specified region.

The authors in and embed the data in video using the phase angle between two consecutive CMV. These CMV are selected based on the magnitude of the motion vectors as in. The message bit stream is encoded as phase angle difference in sectors between CMV. The block matching is constrained to search within the selected sector for a magnitude to be larger than the predefined threshold. The methods in focused on finding a direct reversible way to identify the CMV at the decoder and thus relied on the attributes of the motion vectors. In this paper, we take a different approach directed towards achieving a minimum distortion to the prediction error and the data size overhead. This approach is based on the associated prediction error and we are faced by the difficulty of dealing with the nonlinear quantization process.

Steganography is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient, suspects the existence of the message, a form of obscurity. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

A **digital watermark** is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks, digital watermarks are only

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 2, Issue 12, December 2015)

perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

LSB based video Steganography: In the current endeavor, a video file with ".avi" extension has been selected as host file. It is assumed that the least Significant bits of that file should be modified without degrading the image quality.

II. DESCRIPTION

BLOCK DIAGRAM

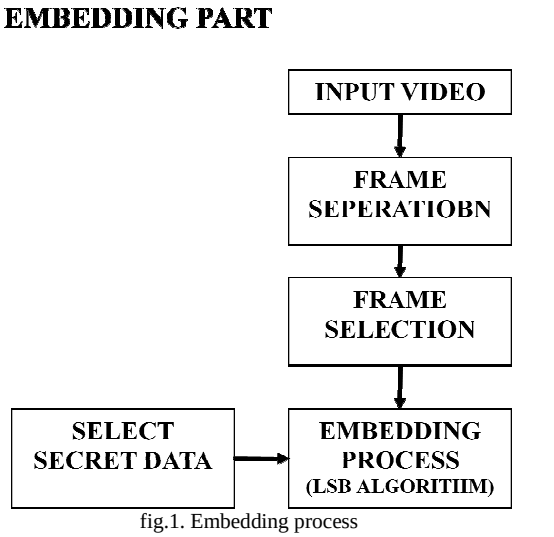

fig.1. Embedding process

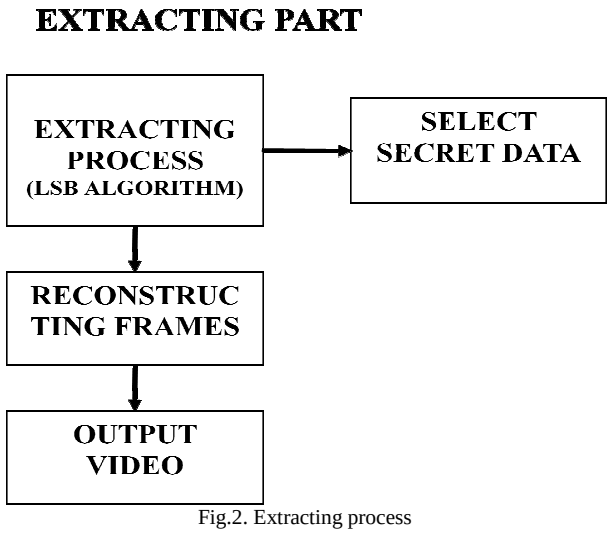

Fig.2. Extracting process

Frame Separation: Frame processing is the first step in the background subtraction algorithm, the purpose of this step is to prepare the modified video frames by removing noise and unwanted object's in the frame in order to increase the amount of information gained from the frame and the sensitivity of the algorithm.

Preprocessing is a process of collecting simple image processing tasks that change the raw input video info a format. This can be processed by subsequent steps. Preprocessing of the video is necessary to improve the detection of moving object's For example, by spatial and temporal smoothing, snow as moving leaves on a tree, can be removed by morphological processing of the frames after the identification of the moving object's as shown in fig. 3

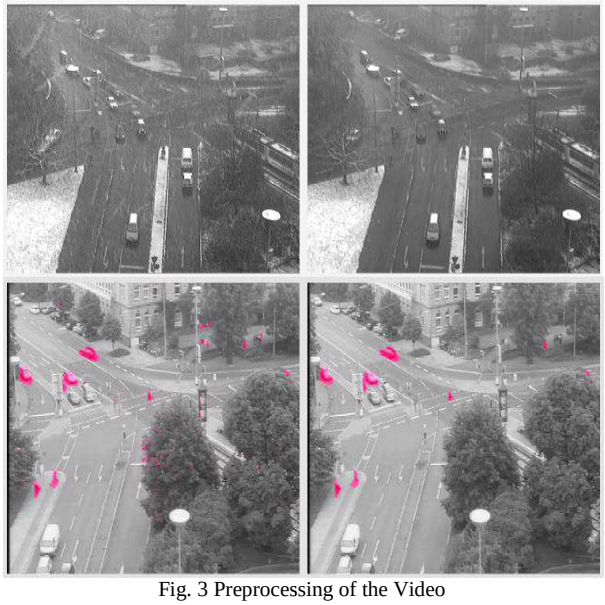

Fig. 3 Preprocessing of the Video

Another key issue in pre processing is the data format used by the particular background subtraction algorithm. Most of the algorithm handles luminance intensity, which is one scalar value per each pixel, however, color image, in either RGB or HSV color space, is becoming more popular in the background subtraction algorithms.

Coding for Frame Separation

```
file=aviinfo('movie1.avi');
frm_cnt=file.NumFrames
str2='.bmp'
   h = waitbar(0,'Please wait...');
for i=1:frm_cnt
   frm(i)=aviread(filename,i);
   frm_name=frame2im(frm(i));
   frm_name=rgb2gray(frm_name);
   filename1=strcat(strcat(num2str(i)),str2);
   imwrite(frm_name,filename1);
   waitbar(i/frm_cnt,h)
end
close(h)
```

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 2, Issue 12, December 2015)

Separation logic facilitates reasoning about:

1. Programs that manipulate pointer data structures — including information hiding in the presence of pointers;
2. "transfer of ownership" (avoidance of semantic frame axioms); and
3. Virtual separation (modular reasoning) between concurrent modules.

Separation logic supports the developing field of research described by Peter O'Hearn and others as local reasoning, whereby specifications and proofs of a program component mention only the portion of memory used by the component, and not the entire global state of the system. Applications include automated program verification (where an algorithm checks the validity of another algorithm) and automated parallelization of software.

III. IMPLEMENTATION

Introduction of LSB: Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware selected as the cover media. These images are called cover of the existence of the hidden messages. In this paper, 8-bit grayscale images are cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. One of the common techniques is based on manipulating the least-signi7cant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity.

Data hiding by simple LSB substitution: In this section, the general operations of data hiding by simple LSB substitution method are described.

Let C be the original 8-bit grayscale cover-image of $M_C \times N_C$ pixels represented as $C = \{x_{ij}\}$

$$C = \left\{x_{ij} \middle| 0 \le i < M_c, 0 \le j < N_c, x_{ij} \epsilon \{0, 1, .., 255\}\right\}$$

M be the n-bit secret message represented as

$$M = \{m_i | 0 \le i < n, m_i \epsilon \{0, 1\}\}$$

Suppose that the n-bit secret message M is to be embedded into the k-rightmost LSBs of the cover-image C. Firstly, the secret message M is rearranged to form a conceptually k-bit virtual image M_ represented as

$M' = \left\{m'_i \middle| 0 \le i < n', m'_i \epsilon \{0, 1, \ldots\ldots, 2^k - 1\}\right\}$ Where $n' < M_c \times N_c$. the mapping between the n-bit secret message $M = \{m_i\}$ and the embedded message $M' = \{m'_i\}$

$$m'_i = \sum_{j=0}^{k-1} m_{i \times k+i} \times 2^{k-1-j}$$

Secondly, a subset of n_ pixels $\{x_{l1}; x_{l2}; :::: ; x_{ln}\}$ is chosen from the cover-image C in a prede7ned sequence. The embedding process is completed by replacing the k LSBs of x_{li} by m_i . Mathematically, the pixel value xli of the chosen pixel for storing the k-bit message m_i is modi7ed to form the stego-pixel x_li as follows:

$$x'_{li} = x_{li} - x_{li} mod 2^k + m'_i$$

In the extraction process, given the stego-image S, the embedded messages can be readily extracted without referring to the original cover-image. Using the same sequence as in the embedding process, the set of pixels $\{x'_{l1}, x'_{l2}, \ldots\ldots, x'_{ln'}\}$ storing the secret message bits are selected from the stego-image. The k LSBs of the selected pixels are extracted and lined up to reconstruct the secret message bits. Mathematically, the embedded message bits Mi' can be recovered by

$$m'_i = x'_{li} mod 2^k$$

PSNR of the obtained stego-image can be computed by

$$PSNR_{worst} = 10 \times log_{10} \frac{255^2}{WMSE}$$

$$= 10 \times log_{10} \frac{255^2}{(2^k - 1)^2} dB$$

Table 1 tabulates the worst PSNR for some k = 1–5. It could be seen that the image quality of the stego-image is degraded drastically when k>=4.

Table.1 Trade-off between speed and quality for kadak test set

	JPEG 2000 5/3			PGF		
Ratio	enc	dec	PSNR	enc	dec	PSNR
2.7	1.86	1.35	64.07	0.34	0.27	51.10
4.8	1.75	1.14	47.08	0.27	0.21	44.95
8.3	1.68	1.02	41.98	0.22	0.18	40.39
10.7	1.68	0.98	39.95	0.14	0.13	38.73
18.7	1.61	0.92	36.05	0.12	0.11	35.18
35.1	1.57	0.85	28.86	0.10	0.09	31.67

Optimal pixel adjustment process: In this section, an optimal pixel adjustment process (OPAP) is proposed to enhance the image quality of the stego-image obtained by the simple LSB substitution method. The basic concept of the OPAP is based on the technique proposed

Letp_i, p'_i and p''_i be the corresponding pixel values of the ith pixel in the cover-image C, the stego-image C' obtained by the simple LSB substitution method and the refined stego-image obtained after the OPAP. *Let* $\delta_i = p'_i - p_i$ be the embedding error between p_i and p'_i . According to the embedding process of the simple LSB substitution method, p'_i is obtained by the direct replacement of the k LSBs of p_i with k message bits, therefore$-2^k < \delta_i < 2^k$. The value of δ_i can be further segmented into three intervals, such that

$$Interval\ 1: -2^k < \delta_i < 2^k,$$
$$Interval\ 2: -2^{k-1} \le \delta_i \le 2^{k-1},$$
$$Interval\ 3: -2^k < \delta_i < 2^{k-1}.$$

Based on the three intervals, the OPAP, which modifies p'_i to form the stego-pixel p''_i, can be described as follows:

$$Case\ 1(2^{k-1} < \delta_i < 2^k) : If\ p'_i \ge 2^k, then\ p''_i = p'_i - 2^k;\ otherwise\ p''_i = p'_i;$$

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 2, Issue 12, December 2015)

$$Case\ 2(-2^{k-1} \le \delta_i \le 2^{k-1}) : p''_i = p'_i;$$
$$Case\ 3(-2^k < \delta_i < 2^{k-1}) : If\ p'_i < 256 - 2^k,$$
$$then\ p''_i = p'_i + 2^k;\ otherwise\ p''_i = p'_i.$$

Let $\delta'_i = p''_i - p_i$ be the embedding error between p_i and p''_i. δ'_i can be computed as follows:

$$Case\ 1\left(2^{k-1} < \delta_i < 2^k\ and\ p'_i \ge 2^k\right)$$
$$\delta'_i = p''_i - p_i = p'_i - 2^k - p_i = \delta_i - 2^k$$
$$\Rightarrow 2^{k-1} - 2^k < \delta'_i < 2^k - 2^k$$
$$\Rightarrow -2^{k-1} < \delta'_i < 0.$$
$$Case\ 2\left(2^{k-1} < \delta_i < 2^k\ and\ p'_i < 2^k\right)$$
$$\delta'_i = p''_i - p_i = p'_i - p_i = \delta_i$$
$$\Rightarrow 2^{k-1} < \delta'_i < 2^k.$$
$$Case\ 3(-2^{k-1} \le \delta_i \le 2^{k-1})$$
$$\delta'_i = p''_i - p_i = p'_i - p_i = \delta_i$$
$$\Rightarrow -2^{k-1} < \delta'_i < 2^{k-1}.$$
$$Case\ 4\left(-2^k < \delta_i < 2^{k-1}\ and\ p'_i < 256 - 2^k\right)$$
$$\delta'_i = p''_i - p_i = p'_i + 2^k - p_i = \delta_i + 2^k$$
$$\Rightarrow -2^k + 2^k < \delta'_i < -2^{k-1} + 2^k.$$
$$\Rightarrow 0 < \delta'_i < 2^{k-1}.$$
$$Case\ 5\left(-2^k < \delta_i < 2^{k-1}\ and\ p'_i \ge 256 - 2^k\right)$$
$$\delta'_i = p''_i - p_i = p'_i - p_i = \delta_i$$
$$\Rightarrow -2^k < \delta'_i < 2^{k-1}.$$

Least-Significant-Bit (LSB) Matching Method: In order to keep the embedding of the same amount of information as LSB matching and detect the secret data harder than the conventional LSB matching method, Mielikainen proposed a robust LSB matching method in 2006. There are two major properties in his scheme as following:

$$f(l-1,n) \ne f(l+1,n), \forall l,n \epsilon Z.$$
$$f(l,n) \ne f(l,n+1), \forall l,n \epsilon Z.$$

Therefore, embedding message is performed for two pixels *X* and *Y* of a cover image at a time and then adjusting one pixel of the (*X*, *Y*) to embed two secret bits message *s1s2*. The embedding flowchart is shown in Fig.2 and the embedding procedure is described as following:

Step.1. If the LSB of *X* is the same as *s1*, go to step 2. Otherwise, go to step 3.

Step.2. If the value of *f* (*X, Y)* is the same as *s2*, do not change any pixel. Otherwise, the value of pixel *Y* is increased or decreased by 1.

Step.3. If the value of *f* (*X* −1, *Y) is* the same as *s2*, the value of pixel *X* is decreased by 1. Otherwise, the value of pixel *X* is increased by 1. Where the function *f* (*X, Y)* is defined as Eq.1:

$$f(X',Y') = LSB\left(\left\lfloor \frac{X'}{2} \right\rfloor + Y'\right)$$

Since this new LSB matching method just only increase or decrease 1 in two adjacent pixels, the difference of the two neighborhood pixel between cover image and stego-image is very small. Hence, it can keep high quality while hiding data.

Hiding Secret Files is a security product based on an unrivalled data hiding method. As a result of many months of research, this product hides and safely protects your private information from being erased. Would you be happy to find your priceless financial plans, your personal ideas or projects, your private photos or movies in foreign hands, altered or erased? Hide Secret Files is the ultimate tool allowing you to have exclusive secured access to sensitive information based on a password. No one except you, who know the password, will be able to access the secured data. Not even your own operating system will have permission to alter the information. The latest, and one of the most annoying secondary products of the Internet evolution, is the spy-ware activity, and thankfully it is absolutely inoffensive against the protection guaranteed by Hide Secret Files. The hidden data won't be visible even for your own OS so the Safe Mode booting or moving the hard drive in another PC won't make it possible to reveal, the data protected by Hide Secret Files. For this to work you will need WinRAR installed on your computer and Microsoft Windows with access to the command prompt. If you do not have WinRAR installed on your computer you can find a link to download this program through our recommended download section.

Hiding a message or other data:

1. Create a text file with your secret message or hidden data and highlight it and highlight each of the files you wish to secretly add to the image file. In this example we created one text file called **message.txt**.
2. Once highlighted right-click the highlighted file and click **add to "message.rar"**, where message.rar is the name of the file you right-clicked on.
3. Open a Windows command line window.
4. Move to the directory that contains the .rar file and the image you wish to hide the text in.
5. Type a command similar to the below command. copy /b secret.jpg + message.rar hidden.jpg

In the above example, "secret.jpg" is the name of the image you're using, the .rar file is the name of the file used earlier, and hidden.jpg is the name of the new image with the hidden message within it. See the copy command page for additional information about this command.

Once the above steps have been completed you should now have an image called hidden.jpg that contains the hidden message. It's a good idea to make sure you're still able to open and view the image before saving it, posting it on the Internet, or otherwise distributing it. Below is an example of the hidden.jpg we created doing the above steps.

To view the hidden message or hidden files you must have followed the above steps. If the above steps were performed to create the image follow the below steps to view the data.

1. Save the image to the computer if you're viewing it online.
2. Open WinRAR by clicking Start, Programs, WinRAR, and then WinRAR.
3. Within WinRAR click File and Open archive. Within the open window make sure your files of type option are all files and not just compressed files.

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 2, Issue 12, December 2015)

4. Browse to the location of the image and double-click the image to open it.
5. Once open it should display the file(s) contained within the image that can be extracted from the image.
6. How to use data selection to explore available data and drill down to selected properties
7. Using the data comparison condition
8. Using the set a data value action
9. That Rules recognizes different types of data, and verifies when necessary
10. That Rules knows that not all data is writable, and verifies when necessary
11. How to create composite tokens, extending the tokens listed in the replacement patterns
12. Making field values accessible to Rules
13. Using reference fields to access new data, such as tags on an article or nodes in a node reference field

Steganography replaces unneeded bits in image and sound files with secret data. Instead of protecting data the way encryption does, steganography hides the very existence of the data. And it's undetectable under traditional traffic-pattern analysis. There are few legitimate uses for steganography, say forensics professionals. And despite reports circulating about terrorists using steganography to communicate secretly, experts doubt that's the case. "Most people study steganography either as an academic discipline or a curiosity, but I don't know if even terrorist groups would actually use it," says Chakraborty. Last year, after reading a USA Today article about steganography and terrorism, Neils Provos, a Ph.D. student in computer science at the University of Michigan in Ann Arbor, decided do his dissertation on steganography. Provos developed detection and cracking tools to analyze images for signs of steganography, such as overly large files and uneven bit mapping. He tested the tools and then used them to compare 2 million images on San Jose-based eBay Inc.'s Web site, which has been cited as a possible place for posting and retrieving hidden messages. Provos found no cases of steganography. "Steganography becomes the focus of attention, dies down, and then the public is all over it again," says Provos. "But it will never be pervasive, because the amount of data you can actually hide in the images is fairly small. And if someone wanted to steal intellectual property, it'd be easier to copy the data on a disk and carry it out in your pocket." Even if steganography is present, forensics experts prefer to start by investigating less complex areas. But in some cases, the only evidence might be hidden in image or sound files, so investigators need to be aware of steganography and the tools used to detect and crack it.

IV. RESULTS

Using MATLAB visual basics develop the explorer windows and observed output result

Input selection processes:

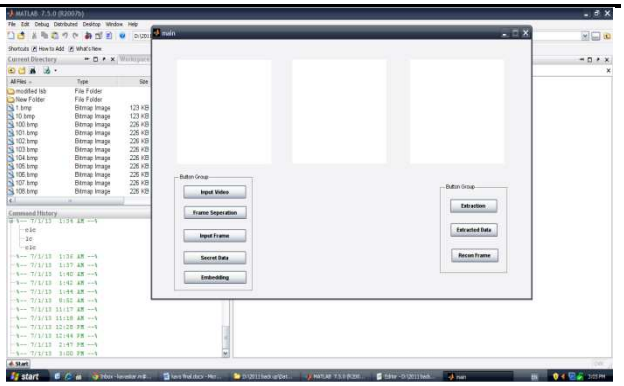

Fig.6

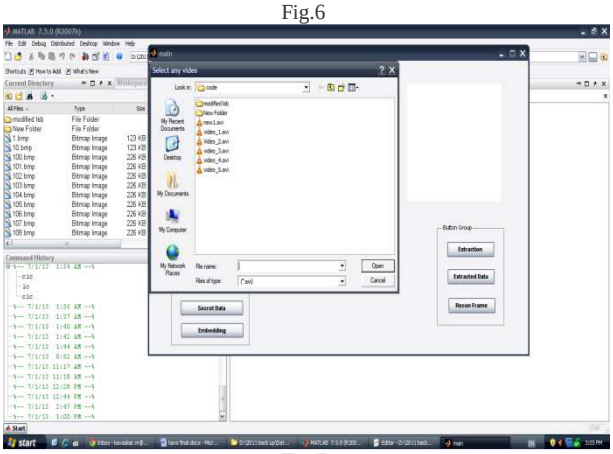

Fig.7

Frame selection processes:

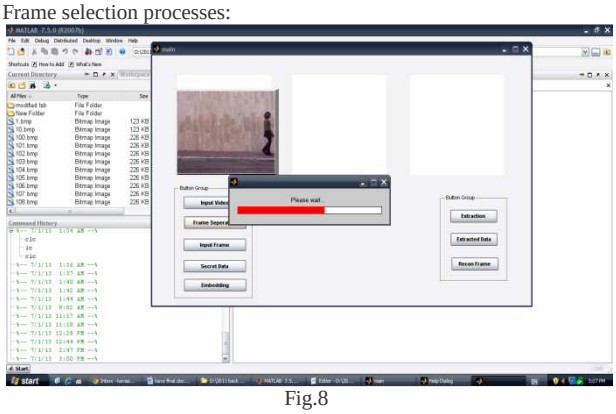

Fig.8

Selecting frame:

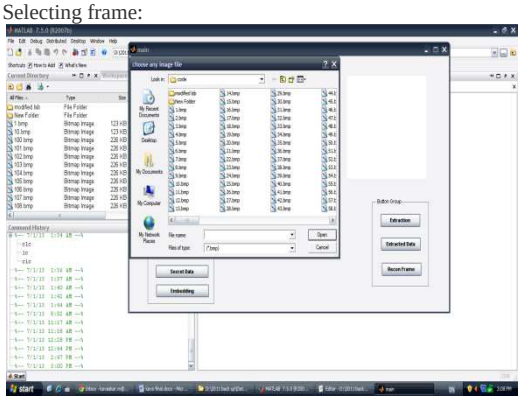

Fig.9

Select secrete data processes:

International Journal of Advanced Research Foundation
Website: www.ijarf.com, Volume 2, Issue 12, December 2015)

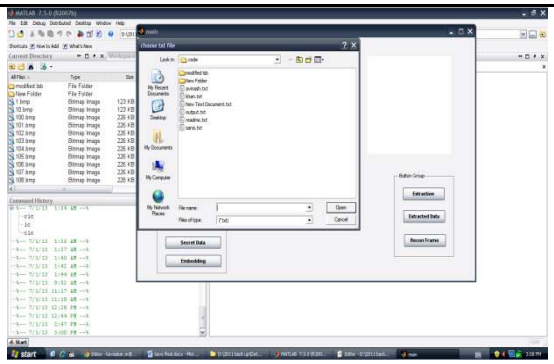

Fig.10

Extracting processes:

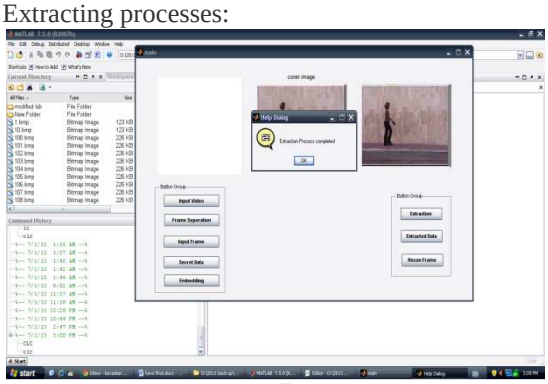

Fig.11

Extracting data:

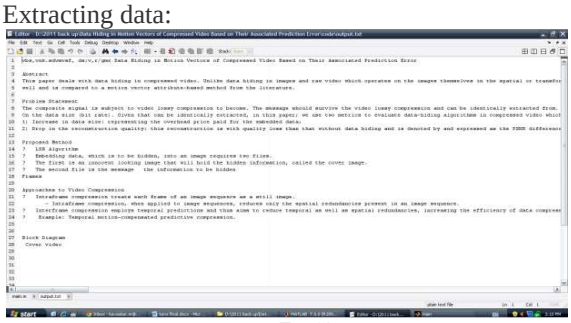

Fig.12

V. CONCLUSION

In this paper, a data hiding method by simple LSB substitution with an optimal pixel adjustment process is proposed. The image quality of the stego-image can be greatly improved with low extra computational complexity. Extensive experiments show the effectiveness of the proposed method. The results obtained also show significant improvement than the method proposed with respect to image quality and computational efficiency. Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. As with the other great innovations of the digital age: the battle between cryptographers and cryptanalysis, security experts and hackers, record companies and pirates, steganography and Steganalysis will continually develop new techniques to counter each other.

In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate.

REFERENCES

[1]. A.Z. Tirkel, R.G. Van Schyndel, C.F. Osborne, A digital watermark, Proceedings of ICIP 1994, Austin Convention Center, Austin, Texas, Vol. II, 1994, pp. 86–90.

[2]. W. Bender, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3/4) (1996) 313–336.

[3]. T.S. Chen, C.C. Chang, M.S. Hwang, A virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Process. 7 (10) (1998) 1485–1488.

[4]. L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans.Image Process. 8 (8) (1999) 1075–1083.

[5]. Anderson R.J. and Petitcolas F.A.P., “On the Limits of steganography,” J. Selected Areas in Comm., vol. 16, no.4,1998, pp. 474–481.

[6]. Bailey, K. and Curran, K. “An evaluation of image-based steganography methods”. International Journal of Digital Evidence, Fall 2003.

[7]. Chapman, M. Davida G, and Rennhard M.. “A Practical and Effective Approach to Large-ScaleAutomatedLinguistic Steganography” found online at http://www.nicetext.com/doc/isc01.pdf

[8]. Dai Y., Liu G., and WangBreaking Z., “Predictive - Coding-Based Steganography and Modification for Enhanced Security”, IJCSNS International Journal of Computer Science and Network Security, vol.6 no. 3b, March 2006.

About the authors:

TABASUM GULEDGUDD[1] Currently working as a H.OD & Associate Professor in ECE in Secab Institute of Engineering and Technology.

EASARI PARUSHA RAMU[2], Currently works as assistant professor of ECE in Sri Indu College of Engineering & Technology