ISSN:0975-9646

# LSB Approach for Video Steganography to Embed Images

K. Steffy Jenifer , G. Yogaraj , K. Rajalakshmi
*CSE, P.B.College of Engineering, Sriperumbudur, India – 602 105*

***Abstract* – Video Steganography to embed Image is an art and science of hiding images by embedding images within the video file, seemingly harmless images. An encrypted image or files may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen. The LSB approach is used along with the Masking-Filtering and Transformations techniques to hide the secret image or any other files.**

***Keywords:* Masking-Filtering, Transformation technique, LSB bits.**

## I. Introduction

In network technology, secure transmission refers to the transfer of data such as confidential or proprietary information over a secure channel. Many secure transmission methods require a type of encryption. The most common email encryption is called PKI. In order to open the encrypted file an exchange of keys is done. Many infrastructures such as banks rely on secure transmission protocols to prevent a catastrophic breach of security. Secure transmissions are put in place to prevent attacks such as ARP spoofing and general data loss.

Various confidential data such as military maps and commercial identifications are transmitted over the Internet. One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. While transferring secret images, various image secret sharing schemes have been developed.

Steganography (literally meaning *covered writing*) dates back to ancient Greece, where common practices consisted of etching messages in wooden tablets and covering them with wax, and tattooing a shared messenger's head, letting his hair grow back, then sharing it again when he arrived at his contact point.

Steganography mechanism is used to hide data like secret images and any other files within another file. Steganography and the cryptography mechanisms are combined together to send a secret data with full security.

The best steganographic method that works in this domain is the LSB (Least Significant Bits), which replaces the least significant bits of pixels selected to hide the information.

## II. Problem Statement

The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguist. In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly.

Many different carrier file formats can be used to hide the images or any other files, but digital images are the most popular because of their frequency on the internet.

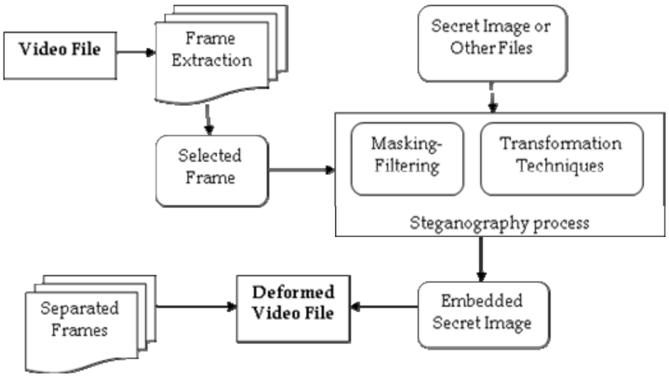

Fig. 1 Flow of Video Steganography algorithm

For hiding secret images in videos, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. So we prepare this application, to make the information hiding simpler and user friendly.

## III. Frame Conversion

Video Conversion process is used to reduce the spatial and temporal redundancy of Group of Pictures. Temporal redundancy can be reduced by registering differences between frames. Spatial redundancy is reduced by registering differences between parts of a single frame.

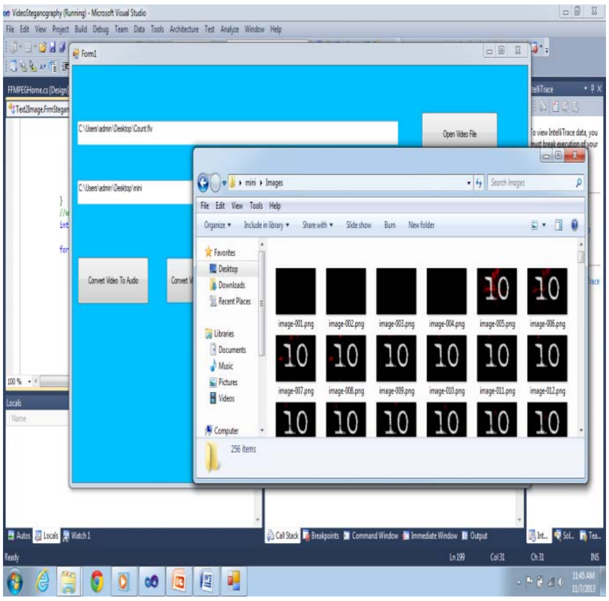

Fig. 2 Separating frames from selected video file

Video to frame conversion is the process of converting a video to cinematic motion picture. The number of still pictures per unit of time can be separated from the video using this Stego model. 120 or more frames per second of images can be retrieved from new professional cameras as efficiently with clarity motion pictures.

## IV. Masking-Filtering

Masking & Filtering techniques usually restricted to 24 bits and gray scale image, hide information by marking an image, in a manner similar to paper watermarks. This technique is used to perform analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to cover image than just hiding it in the noise level.

### A. *Grayscale Image*

In order to provide the security the original image is converted into the gray scale image which contains the black and white pixels.

Grayscale images are distinct from one-bit bi-tonal black-and-white images, which in the context of computer imaging are images with only the two colors, black, and white (also called bi-level or binary images). Grayscale images have many shades of gray in between. Grayscale images are also called monochromatic, denoting the presence of only one (mono) color (chrome).

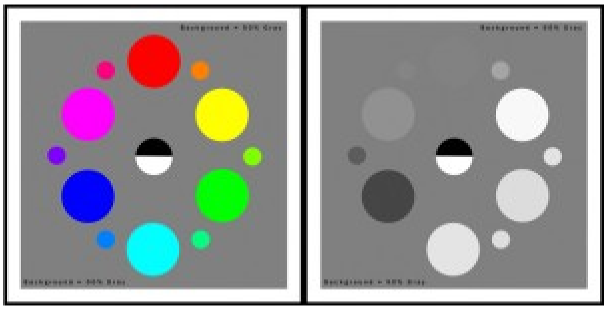

Fig. 3 Conversion of color image into grayscale image

Conversion of a color image to grayscale is not unique; different weighting of the color channels effectively represent the effect of shooting black-and-white film with different-colored photographic filters on the cameras.

For the sRGB color space, gamma expansion is defined as

$$C_{\mathrm{linear}} = \begin{cases} \frac{C_{\mathrm{srgb}}}{12.92}, & C_{\mathrm{srgb}} \le 0.04045 \\ \left(\frac{C_{\mathrm{srgb}}+0.055}{1.055}\right)^{2.4}, & C_{\mathrm{srgb}} > 0.04045 \end{cases}$$

Where $C_{\mathrm{srgb}}$ represents any of the three gamma-compressed sRGB primaries ($R_{\mathrm{srgb}}$, $G_{\mathrm{srgb}}$, and $B_{\mathrm{srgb}}$, each in range [0,1]) and $C_{\mathrm{linear}}$ is the corresponding linear-intensity value ($R$, $G$, and $B$, also in range [0,1]). Then, luminance is calculated as a weighted sum of the three linear-intensity values. The sRGB color space is defined in terms of the CIE 1931 linear luminance $Y$, which is given by

$$Y = 0.2126R + 0.7152G + 0.0722B$$

The coefficients represent the measured intensity perception of typical trichromat humans, depending on the primaries being used; in particular, human vision is most sensitive to green and least sensitive to blue.

## V. Transform Techniques

Transform techniques embed the message by modulating coefficient in a transform domain, such as the Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover image, which make them more robust to attack. Transformations can be applied over the entire image, to block throughout the image, or other variant.

### A. *Discrete Fourier Transform*

The Fourier Transform is an important image processing tool which is used to decompose an image into its sine and cosine components. The output of the transformation represents the image in the Fourier or frequency domain, while the input image is the spatial domain equivalent. In the Fourier domain image, each point represents a particular frequency contained in the spatial domain image.

The Fourier Transform is used in a wide range of applications, such as image analysis, image filtering, image reconstruction and image compression.

For a square image of size N×N, the two-dimensional DFT is given by:

$$F(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} f(i,j)\, e^{-\iota 2\pi \left(\frac{ki}{N} + \frac{lj}{N}\right)}$$

Where *f(a,b)* is the image in the spatial domain and the exponential term is the basis function corresponding to each point *F(k,l)* in the Fourier space. The equation can be interpreted as: the value of each point *F(k,l)* is obtained by multiplying the spatial image with the corresponding base function and summing the result.

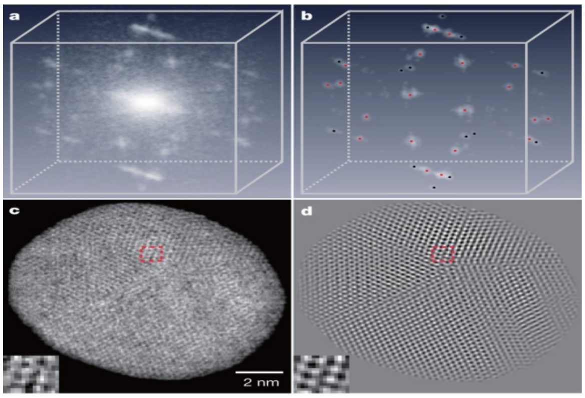

Fig. 4 **a**, 3D Fourier transform of the raw reconstruction of the nanoparticle. **b**, 3D Fourier transform of the reconstruction after 3D Fourier filtering where the {111} and {200} Bragg peaks are labelled with red and black dots, respectively. **c**, A 2.6-Å-thick central slice in the *x*–*y* plane of the raw reconstruction, where the *z* axis is along the beam direction. **d**, The same slice of the 3D structure after applying a 3D Fourier filter, in which nearly all the atoms (in white) are visible.

In a similar way, the Fourier image can be re-transformed to the spatial domain. The inverse Fourier transform is given by:

$$f(a,b) = \frac{1}{N^2} \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} F(k,l)\, e^{\iota 2\pi\left(\frac{ka}{N}+\frac{lb}{N}\right)}$$

## B. *Wavelet Transform*

As a mathematical tool, wavelets can be used to extract information from many different kinds of data, including – but certainly not limited to – audio signals and images. Sets of wavelets are generally needed to analyze data fully. A set of "complementary" wavelets will decompose data without gaps or overlap so that the decomposition process is mathematically reversible. Thus, sets of complementary wavelets are useful in wavelet based compression/decompression algorithms where it is desirable to recover the original information with minimal loss.

## VI. LSB APPROACH

Least Significant Bit (LSB) is a simple approach which is used to embed image into video file. Here, the bits of the image are directly embedded into least significant bit plane of the cover-frame in a deterministic sequence. Modulating the least significant bit cannot be identified in human perceptible difference because the amplitude of the change is small. In this technique, the embedding capacity can be increased by using two or more least significant bits. At the same time, not only the risk of making the embedded message statistically detectable increase but also the image fidelity degrades. Hence a variable size LSB embedding schema is presented, in which the number of LSBs used for message embedding/extracting depends on the local characteristics of the pixel. The advantage of LSB-based method is easy to implement and high message pay-load.

Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image.

Therefore, a system named Video Steganography System to embed secret image is proposed to improve the LSB scheme. It overcomes the sequence-mapping problem by embedding the massage into a set of random pixels, which are scattered on the cover-image.

## VII. STEGANOGRAPHY MODEL

The steganography model for embedding secret image into a video file consists of Carrier Video, Secret Image and Stego Key. Carrier is also known as cover-object, in which the image is embedded and serves to hide the presence of the message.

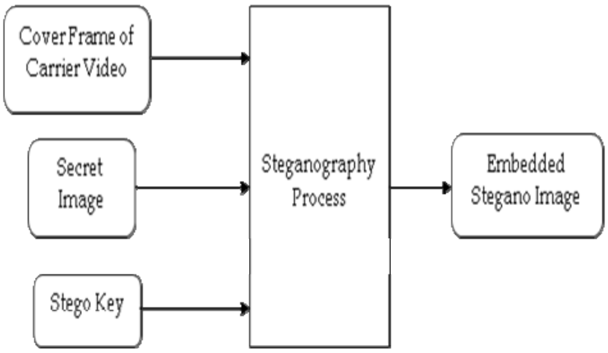

Fig. 5 A sample steganography model for embedding secret image into selected cover frame

Cover frame is the Frame image that is selected from the carrier video file. It can be any type of video files. The secret image is the selected personal image and it may any other file which can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Stego-key, which ensures that only recipient who knows the corresponding decoding key, will be able to extract the image from a cover-frame of carrier video file. The cover-frame with the secretly embedded image is then called the Embedded Stegano-Image.

## VIII. RECOVER IMAGE

Recovering image from a embedded Stegano-image requires the cover-frame itself and a corresponding decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message. However, the secret image is extracted from the received deformed video file.

## IX. CONCLUSION

The proposed construction of video steganography was realized by embedding the secret image into the meaningful cover image of any type of video file using LSB approaches. Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Enhancement of the image steganography system is printed out using LSN approach to provide a means of secure communication. A stego-key has been applied to the system during embedment of the message into the cover image. We also proposed a method to improve the visual quality of the share images. The proposed embedded video steganography has many specific advantages such as user friendliness, simple and effective process of embedding secret image with more security.

## ACKNOWLEDGEMENT

We thank the management of P.B. College of Engineering for their support to carry out this work efficiently.

## REFERENCES

[1]. Ashish T. Bhole, Rachna Patel, “Steganography over Video File using Random Byte Hiding and LSB Technique” 2012 IEEE International Conference on Computational Intelligence and Computing Research.

[2]. Juan Jose Roque, Jesus Maria Minguet, “SLSB: Improving the Steganographic Algorithm LSB”.

[3]. Deepika R.Chaudhari, Ranjit Gawande, “Data hiding in Motion Vectors of Compressed Video Based On their Associated Prediction Error” International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 2, Issue 10, October 2012).

[4]. Mamta Juneja, Parvinder Singh Sandhu, “ Information Hiding using Improved LSB Steganography and Feature Detection Technique” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[5]. Mamta.Juneja and Parvinder S. Sandhu, “An improved LSB based Steganography with enhanced Security and Embedding/Extraction”, 3rd International Conference on Intelligent Computational Systems (ICICS'2013) January 26-27, 2013 Hong Kong (China).

[6]. Poonam V Bodhak, Baisa L Gunjal, “Improved Protection In Video Steganography Using DCT & LSB”, ISSN: 2277-3754 International Journal of Engineering and Innovative Technology (IJEIT) Volume 1, Issue 4, April 2012.

[7]. Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, “Advanced Video Steganography Algorithm”, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 1, January -February 2013, pp.1641-1644.

[8]. Mritha Ramalingam, “Stego Machine – Video Steganography using Modified LSB Algorithm” World Academy of Science, Engineering and Technology 50 2011.