ISO 9001 - 2015

ISSN 2349 - 4891

Monthly

IJRRAS

IF
4.665

Volume 4,Issue 9, September 2017

International Journal of

Recent Research and Applied Studies

SURRAGH PUBLICATIONS

ISSN: 2349 - 4891

International
Journal of Recent Research and Applied Studies
(Multidisciplinary Open Access Refereed e-Journal)

A Empirical Study on Steganography Concepts and its Applications

P.Parimala[1] & R.Dharmarajan[2]

[1]*Research Scholar, Thanthai Hans Roever College, Perambalur, Tamilnadu, India.*
[2]*Asst. Prof. in Comp. Sci., Thanthai Hans Roever College, Perambalur, Tamilnadu, India.*

Received 1st August 2017, Accepted 5th September 2017

Abstract

The increased popularity of digital media has raised serious concerns over its security related issues. Security attacks in the form of eavesdropping, masquerading and tampering and in many other forms is very common nowadays. Data hiding is one of the emerging techniques that aim to provide for security by hiding secret information into the multimedia contents by altering some nonessential components in the host or cover file. Security of data is very important in data communication. Everyday a lot of information is transferred from one user to another on internet and so the possibility of data theft also increases. Steganography provides a solution for the security of information during data transmission. Steganography is the science which makes the valuable information invisible to prevent it from unauthorized user. A steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload (payload is the bits that get delivered to the end user at the destination). So in this project image stegnography technique is proposed to hide data in image in the transform domain using CMD approach. The data in any format (MP3 or WAV or any other type) is encrypted and carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the stego signal.

Keywords: Steganography, Concepts, Applications.

Introduction

The increased popularity of digital media has raised serious concerns over its security related issues. Security attacks in the form of eavesdropping, masquerading and tampering and in many other forms is very common nowadays. Data hiding is one of the emerging techniques that aim to provide for security by hiding secret information into the multimedia contents by altering some nonessential components in the host or cover file. Security of data is very important in data communication. Everyday a lot of information is transferred from one user to another on internet and so the possibility of data theft also increases. Steganography provides a solution for the security of information during data transmission. Steganography is the science which makes the valuable information invisible to prevent it from unauthorized user. A steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload (payload is the bits that get delivered to the end user at the destination). So in this project image stegnography technique is proposed to hide data in image in the transform domain using CMD approach. The data in any format (MP3 or WAV or any other type) is encrypted and carried by the image without revealing the existence to anybody. When the secret information is hidden in the carrier the result is the stego signal.

Correspondence
R.Dharmarajan
E-mail: rd.thrc@gmail.com, Ph. +9194438 05020

Purpose of Image processing

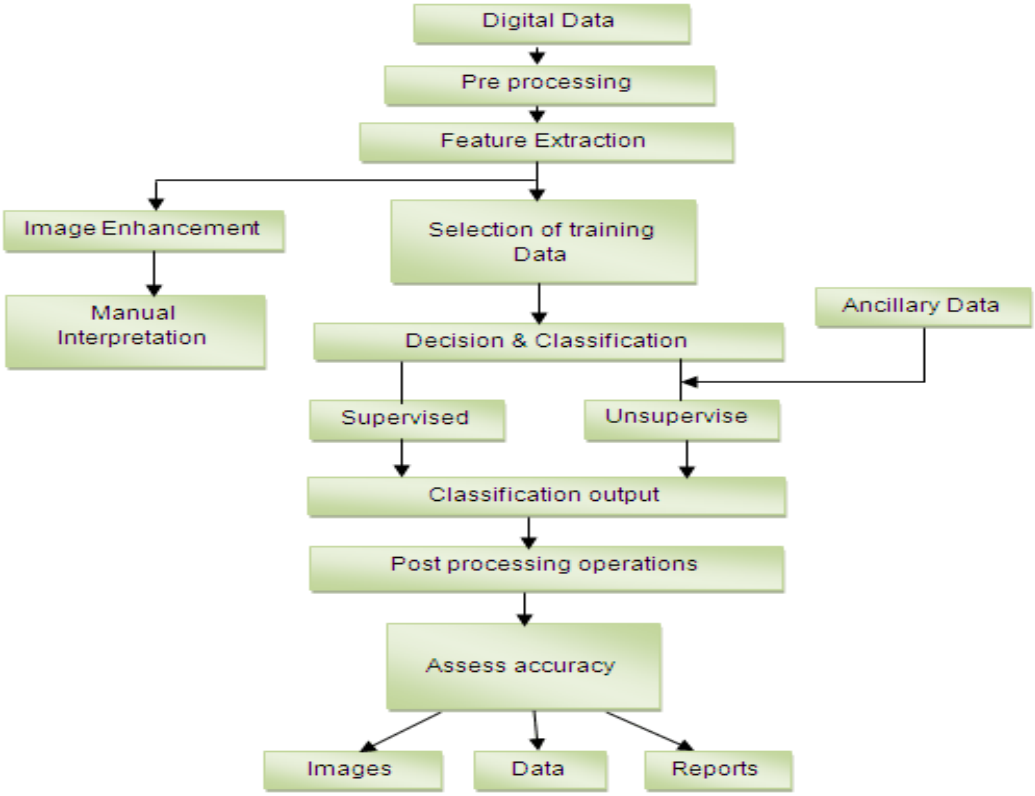
The purpose of image processing is divided into 5 groups. They are:

1. Visualization - Observe the objects that are not visible.
2. Image sharpening and restoration - To create a better image.
3. Image retrieval - Seek for the image of interest.
4. Measurement of pattern – Measures various objects in an image.
5. Image Recognition – Distinguish the objects in an image.

Methods

The two types of **methods used for Image Processing** are **Analog and Digital** Image Processing. Analog or visual techniques of image processing can be used for the hard copies like printouts and photographs. Image analysts use various fundamentals of interpretation while using these visual techniques. The image processing is not just confined to area that has to be studied but on knowledge of analyst. Association is

another important tool in image processing through visual techniques. So analysts apply a combination of personal knowledge and collateral data to image processing. Digital Processing techniques help in manipulation of the digital images by using computers. As raw data from imaging sensors from satellite platform contains deficiencies. To get over such flaws and to get originality of information, it has to undergo various phases of processing. The three general phases that all types of data have to undergo while using digital technique are Pre- processing, enhancement and display, information extraction.

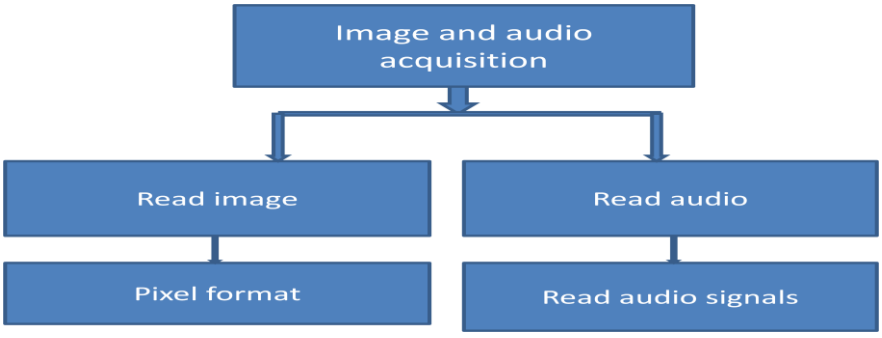


Modules

- Image and data acquisition
- Pixel conversion
- Embedding the data
- Extraction of the data
- Evaluation criteria

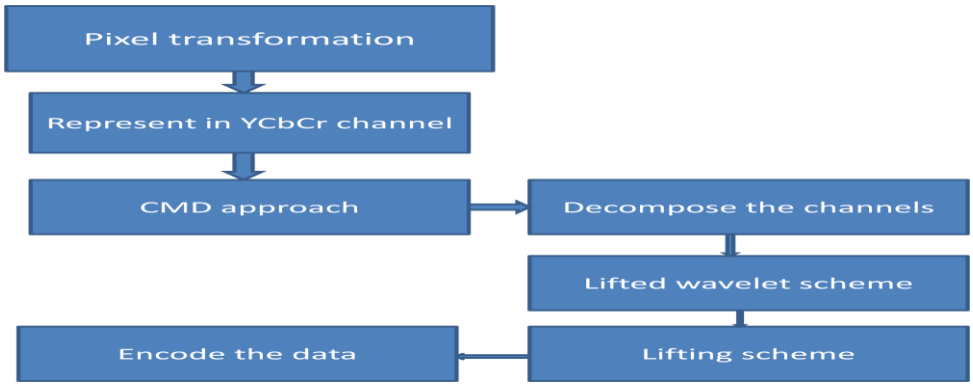
Image and data acquisition

Steganography is an art of hiding some secret message in another message without letting anyone know about presence of secret message except the intended receiver. The message used to hide secret message is called host message or cover message. Once the contents of the host message or cover message are modified, the resultant message is known as stego message. In this module, user can upload the cover data and image which is hiding in cover video. Then read the data as pixel format and audio as signal format. We can upload any type of data and image.



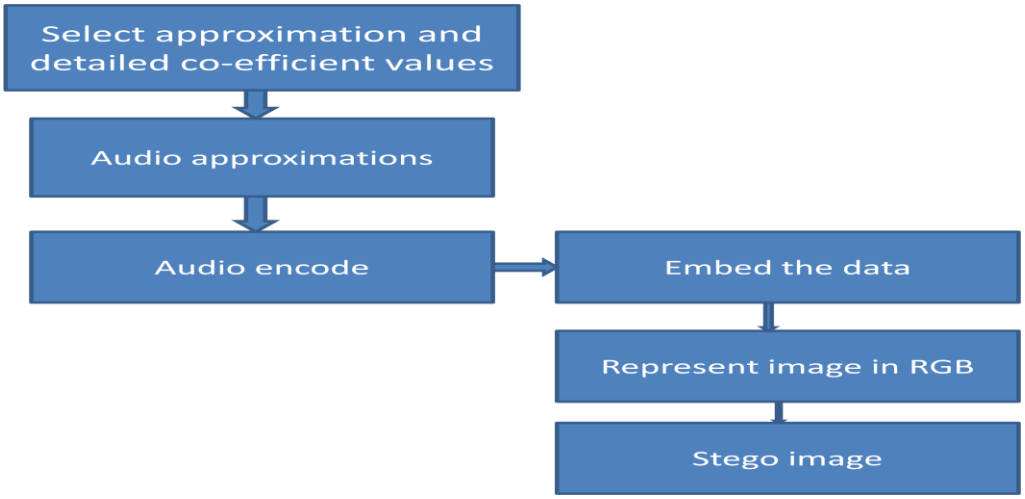
Pixel conversion

Cover image is represented in YCbCr channel. Then using clustering modification transformation approach which is a decomposition of a function into a linear combination of the spatial features. The inverse wavelet transform shows that the original signal may be synthesized by summing up all the projections of the signal onto the spatial basis. In this sense, the continuous transform behaves like an orthogonal transform. Lifted wavelet transform approach which uses integer to integer transformation which is implemented using lifting wavelet transformation (LWT). LWT uses Lifting Scheme (LS). In LS, among the various wavelets available, appropriate wavelet is chosen. As integer coefficients are required, 'int2int' transformation has to be specified. Based on the LS, apply the LWT to cover audio to get detail and approximation coefficients, CD and CA respectively. Convert CD to binary. And also do the same process in audio signals.



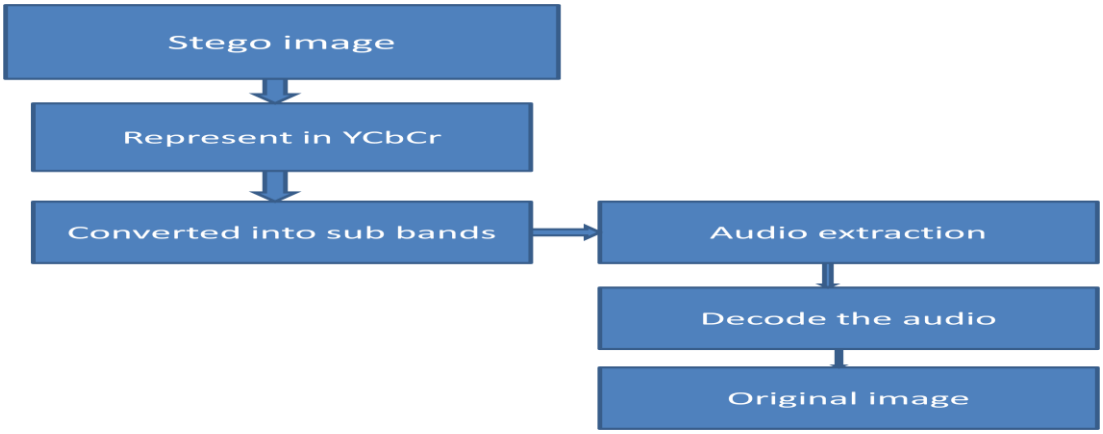
Embedding the data

In this module, select the approximation and detailed co-efficient values. Then hide the audio in approximation coefficients in second plane. This process is known as data encryption. In this model we will use the XOR based algorithm, which will convert the data, which provide a high security. And this data is stored in image after that video can be send. At the receiving side, the shares are retrieved and converted to original image by stacking them together. After that implement inverse approach to get stegno image. Stegno image is then converted in RGB format.



Extraction of data:

In this module, original data and image is extracted with improved manner. We can read the stegno image and convert it into YCbCr format and get the inverse sub bands from stego image. Then decode the stegno image to get the audio in encrypted format. Apply decryption to get original data. We can get the binary values of data to convert into the decimal values. Finally using inverse lifting wavelet transform to extract cover image and data.



Evaluation criteria

In this module, we evaluate the performance of the system using Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), and Universal Image Quality Index (UIQI). The quality of extracted secret data signal is measured by Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC).

Conclusion

The information hiding is the principle of segregation of the design decisions in a computer program that are most likely to change, thus protecting other parts of the program from extensive modification if the design decision is changed. The protection involves providing a stable interface which protects the remainder of the program from the implementation (the details that are most likely to change).

Future Enhancement

In future work, we can extend our project in image domain to provide an efficient and a secure method for video steganography. The proposed method creates an index for the secret information and the index is placed in a frame of the image itself. When steganographed by this method, the probability of finding the hidden information by an attacker is lesser when compared to the normal method of hiding information frame-by-frame in a sequential manner.

References

1. J. J. Chae and B. S. Manjunath, "A Robust Embedded Data from Wavelet Coefficients," University of California, Santa Barbara, CA 93106.
2. Yun Q. Shi, "Reversible Data Hiding," New Jersey Institute of Technology, Newark, NJ 07102, USA.
3. Kamrul Hasan Talukder and Koichi Harada, "Haar Wavelet Based Approach for Video Compression and Quality Assessment of Compressed Video," Issue EICA2012-1, February 10, 2012.
4. Musbah J. Aqel , Ziad A. Alqadi , Ibraheim M. El Emary, "Analysis of Stream Cipher Security Algorithm," Journal of Information and Computing Science, ISSN 1746-7659, vol. 2, no. 4, 2007, pp. 288-298.
5. S.Imaculate Rosaline, C. Rengarajaswamy, "A Steganographic Substitution technique using APPM for encrypted pixels,".
6. Sapna Sasidharan and Deepu Sleeba Philip, "A Fast Partial video Encryption Scheme with Wavelet transform and RC4," International Journal of Advances in Engineering & Technology,.©IJAET ISSN: 2231-1963.
7. Manikandan R, Uma M, " Reversible Data Hiding for Encrypted Video," Journal of Computer Applications ISSN: 0974 – 1925,vol. 5,
8. C. Rengarajaswamy, K. Vel Murugan, "Separable Extraction of Concealed Data and Compressed Video,".
9. P. Tsai, Y. C. Hu, and H. L. Yeh, "Reversible video hiding scheme using predictive coding and histogram shifting," *Signal Process.*, vol. 89, pp. 1129–1143, 2009.