INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 3, Issue 6)
Available online at www.ijariit.com

Implementation of Image Steganography using LabVIEW

Shanthamma .K
GSSS Institute of Engineering and Technology For Women, Mysuru, Karnataka
meghashanthik97@gmail.com

Sanket N. Shettar
GSSS Institute of Engineering and Technology For Women, Mysuru, Karnataka
sanket@gsss.edu.in

Senthilkumar .S
Kaynes Technology, Mysuru, Karnataka
ssenthil@kaynes.com

Abstract: Steganography is the one of the technique to hide secret messages within a larger one in such way that someone can not know the presence or contents of the hidden message. The purpose of Steganography is to maintain secret communication between two parties. This paper presents the implementation of a highly secured data hiding technique called Steganography. This technique is applicable for image data type. The main aim of this technique is to encode the data image within the cover image such that the data image's existence is concealed. Here we use the data as an image for Steganography. It deals with the encoding data image information in a given image (called cover image) without making any visible changes to it. LabVIEW graphical programming environment is a tool for realizing the image acquisition and processing. This software has several advantages: simple implementation, modularity, flexibility, attractive user interface and the possibility to develop very easy new features.

Keywords: Steganography, Image Processing, LabVIEW, Virtual Instrumentations (VI), Data Hiding.

I. INTRODUCTION

Steganography is one of the most used techniques for secure communication. It is used for to hiding the secret messages within a cover image to protect the data from the third person. To keep the message secret there are different methods to encrypt the data one of these is cryptography. In cryptography, the security was done by encryption and decryption of massage. In case of steganography, data information is hiding in cover information. Steganography overcomes the disadvantage of cryptography that the existence of message is also not visible because in some communications it is not enough to encrypt the data. In this paper, Image steganography is implemented [1]. Image steganography uses both data and covers information in image format. It hides the data information in a cover media without making any visible changes in it and the data media existence is concealed. Steganography is mainly applied to Text, Audio, Video, Image and also protocol.

II. SIGNIFICANCE OF STEGANOGRAPHY

The main importance of data hiding techniques comes from the fact the there is no reliability over the medium through which the information is sending, in other words, the medium is not secured. So, that some important methods are implemented it becomes very difficult for unintended user difficult to the unintended user to extract the data information from cover information [2]. Few reasons behind data hiding are.

- Personal and private data
- Sensitive data
- Confidential data and trade secrets
- To avoid misuse of data
- Unintentional damage to data, human error and accidental deletion of data

- Monetary and blackmail purposes
- To hide traces of crime

III. IMAGE STEGANOGRAPHY

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information.Many different file formats are used like Text, Audio/Video, and Image for steganography but images are more frequently used because of their frequency on the Internet. In image steganography, we see the different stenographic technique to hide secrete information in an image like. Least significant bit, Pixel value differencing Edges based data embedding method, Random pixel embedding method, mapping pixel to hidden data method, Labeling or connectivity method, Pixel intensity or gray level value based method, Texture based method, Histogram based methods, Spread Spectrum based methods and Color Palette based methods [3].

Steganography is used for the hiding of data from the third person in secrete communication. Cryptography is also one of the techniques to hide the data from an unauthorized user; here security was done by using encryption and decryption algorithm. In steganography data image is hiding in the cover image to overcome the problem of cryptography that the existence of message is also not visible because in some communications it is not enough to encrypt the data [4].It uses both data and covers information in image format. It hides the data information in a cover media without making any visible changes in it and the data media existence is concealed. Fig. 1 shows the four main categories of file formats that can be used for Steganography.

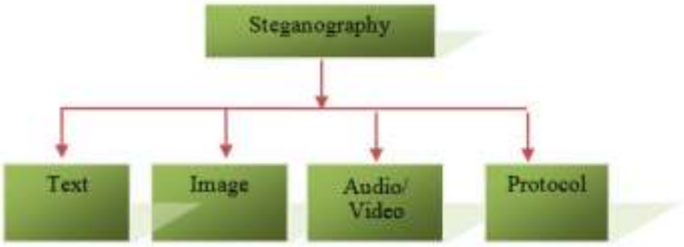

Fig 1: Categories of Steganography

IV. ENCODING

Encoding is the first process in steganography means encoding data image in the cover image. Data image is secreting message which should be invisible to the third person. The hide data image is converting the image into pixels values in RGB format. The data image, as well as cover image, is converted into three matrixes corresponding to Red, Green and Blue components. Data image of the value of each pixel of the matrix has been searching for the corresponding cover image and store it has a global variable. From encoding process, we obtained three global variables as corresponding to Red, Green and Blue format [5].So that these global variables are key for decoding the image as shown in Fig.2.

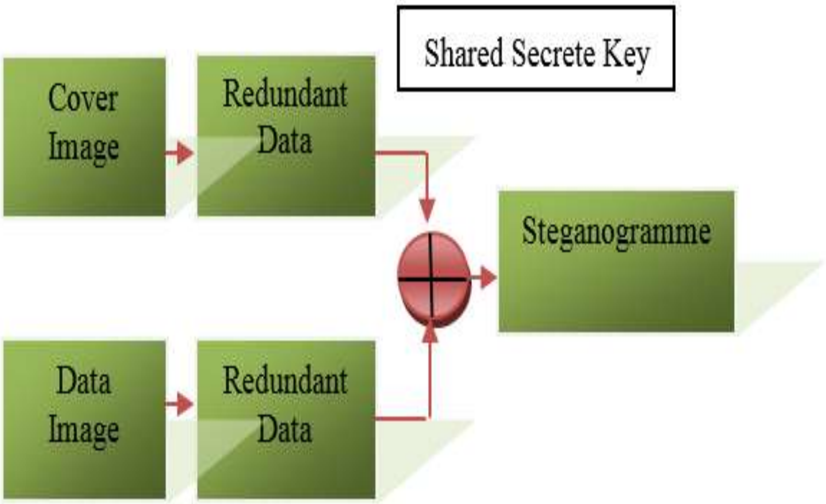

Fig 2: Encoding Process

V. DECODING

Decoding is the reverse process of encoding here we recover the hidden image from the cover image. In the decoding process, we obtained global variables called as secrete shared key.This key provides the array of Red, Green and Blue pixel values. Using these arrays to search in whole image and result will give the data image. Fig 3 shows the decoding process [6].

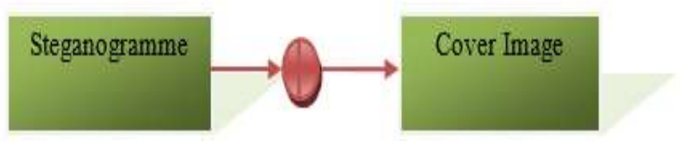

Fig 3 Decoding Process

Here the shared secret key is a global variable which is obtained from the encoder. Final data image received is created from a cover image according to the location stored in global variable [7].Data image should not be greater in size that covers image because in between data image and cover image there should be some correlation so that location of data image can be stored in global variables [8].

VI. PROCEDURE INVOLVED IN BOTH ENCODING AND DECODING PROCESS

For encoding first, we choose the cover image from file location in PC, Extract the pixels value of the cover image and then extract the RGB value of each pixel value of the cover image. Reshape the 2D RGB array of the cover image into a 1D array. After we take the data image through Vision acquisition. Extract the pixel value of data image and then reshape the 2D R, G, B array of data image to 1D array. In the encoding process, we extract the column and row size of data image and send it to global variables. Search each value of R, G, B of Data Image from the reshaped 1D R, G, B array of Cover Image and give its index value. Send this index value of RGB to global variables [8].

In decoding, we take same cover image used in encoding VI.RGB values of each pixel are extracted from the cover image and after it converts 2D RGB array of data image into a 1d array.Search the element of RGB of Data image from the Cover Image. Take the global variable for searching which is same in encoding part.It is helpful to extract 2D RGB values of data Image. Combine the RGB values and extract data image.

VII. IMPLEMENTATION AND RESULTS

Laboratory virtual instrumentation engineering workbench (LabVIEW) is a platform and development environment for a visual programming language from National Instruments. It is very user friendly and easy software to program any system without very deep knowledge of programming. The programming in LabVIEW is graphical programming, not a text based programming. Due to graphical programming syntax is not used so it is very easy to understand for an

Engineer. In LabVIEW, we have seen two windows like Front panel and Block diagram window respectively [9]. In front panel input and output are present. This window is accessible to users, another window which in the block diagram is responsible for programming.

a) Block diagram for Encoder: Encoder is implemented using LabVIEW First takes the data image and cover images are converted into a matrix of pixels values of R, G, B.pixel value of data image search in pixel values of cover image and location is stored in global variables. This global variable is used as a key for the decoder. The upper part of the figure is programming for extraction of the cover image and the lower part is for extraction of data image [10].

b) The front panel of Encoder: Here we take two inputs images, one is data image another one is the cover image. Both images are selected once and run the program so that encoding is done and pixel values of the corresponding image will be shown on the front panel. In the figure, upper image is data image and the lower image is the cover image.Here data image is encoded in cover image and then the pixel value of data image and the cover image is also as shown in the front panel [11].

c) Block diagram for Decoder: In the decoding process, we use the global variables as key for decoder obtained from encoding VI to extract the data image from the cover image. Here the reverse process of encoding takes place.

d) **The front panel of Decoder:** In front panel of decoder we select the same cover image used in encoding. Process. Global variables used as a key for decoding Process.From these global variables, we extract the data image in the cover image. The encoded image is given as input and output is data image. So third person cannot track easily secrete information [12].

VIII. CONCLUSION

Steganography is one of the techniques used for secrete communication to protect the data from the third person. Here Steganography is implemented for security purpose where the objective is to send massage image within a cover image. It would be helpful to provide better security for the transmission of an image. Its future scope is the algorithm can be implemented in the text, audio, and video transmission. NI LabVIEW with Motion and Vision toolkit is helpful in implementing the algorithm of steganography.

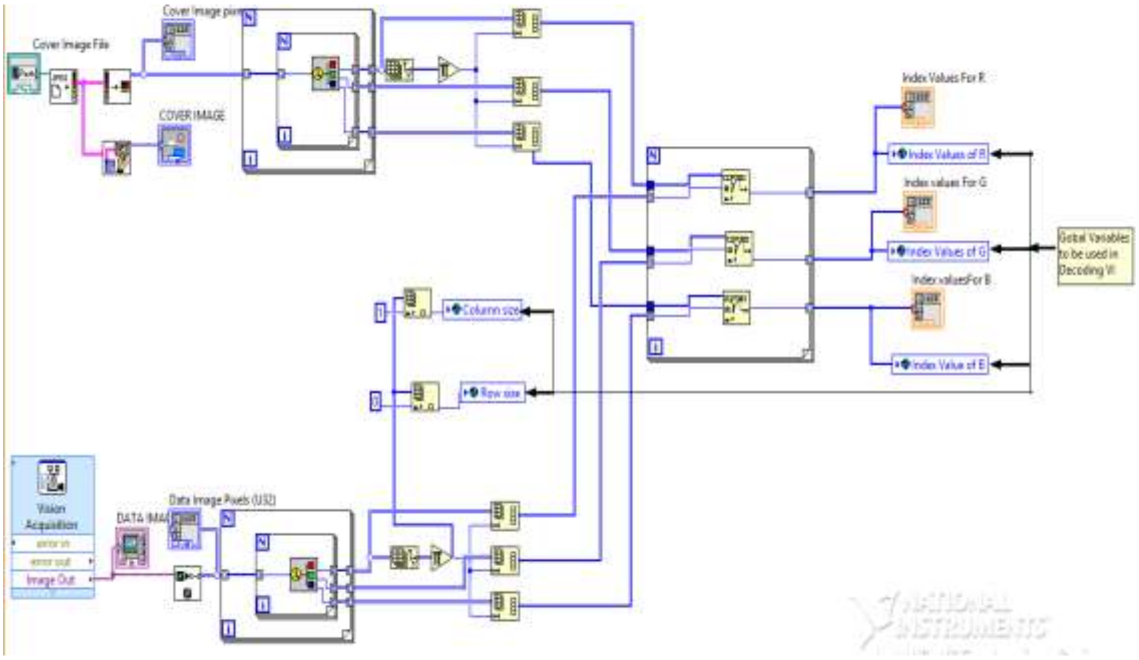

Fig 4 Block Diagram of Encoder

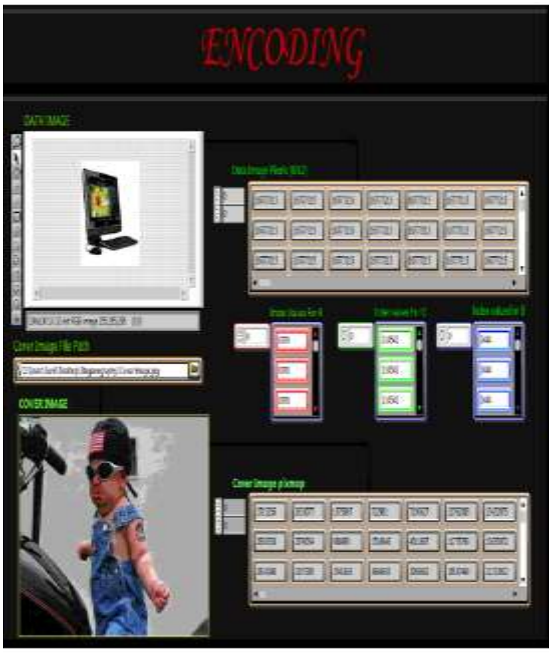

Fig 5: Front Panel of Encoder

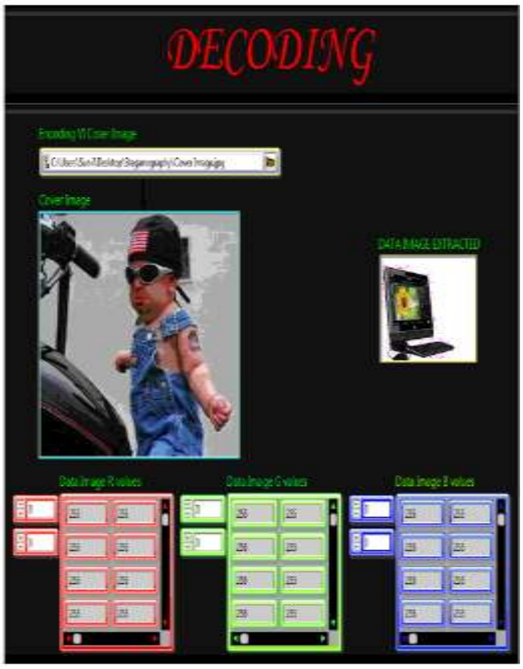

Fig 7: Front Panel of Decoder

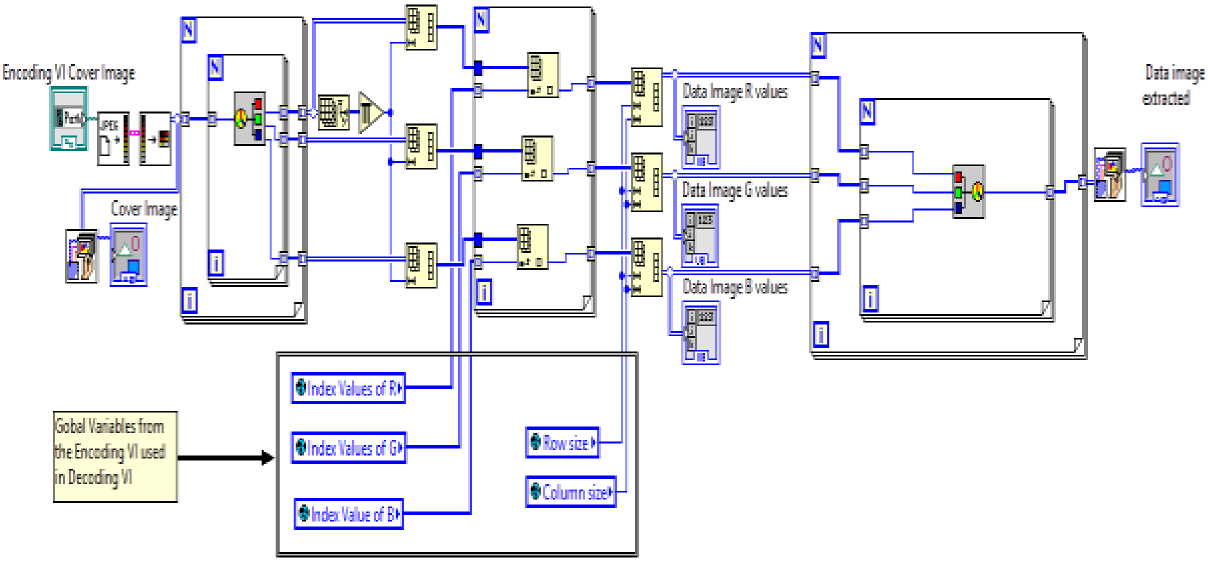

Fig 6: Block Diagram of Decoder

REFERENCES

1. Md. Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal, and Md. Delowar Hossain: “An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography”. 3rd International Conference on Informatics, Electronics ans Vision, pp. 1-6, May 23-24, Dhaka (2014).
2. Lita, I.; Visan, D.A.; Cioc, I.B: “LabVIEW application for movement detection using image acquisition and processing”. *IEEE 16th International Symposium on Design and Technology in Electronic Packaging (SIITME)*, pp. 225-228 (2010).
3. Saket Kumar, Ajay Kumar Yadav, Ashutosh Gupta, Pradeep Kumar: “RGB Image Steganography on Multiple Frame Video using LSB Technique”. International Conference on Computer and Computational Sciences (ICCCS), pp. 226-231, Jan 26-27, Noida (2015).
4. Rig Das, Themrichon Tuithung: “A Novel Steganography Method for Image Based on Huffman Encoding”. 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS), pp. 14-18, March 30-31, Shillong (2012).
5. Caixia Liu: “The Development Trend of Evaluating Face-Recognition Technology”. *IEEE International Conference on Mechatronics and Control (ICMC)*, pp. 1540-1544, (2014).
6. G. Prabhu Teja, S. Ravi: “Face Recognition using Subspaces Techniques”. *IEEE International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 103-107, (2012).
7. Taketo Horiuchi, Takuro Hada: “A Complementary Study for the Evaluation of Face Recognition Technology”. *IEEE 47th International Carnahan Conference on Security Technology (ICCST)*, pp. 1-5, (2013).
8. Johnson, Garn LabVIEW graphical programming. 2nd Edition, *TMH*, (1997).
9. Jerome, Jovitha: “Virtual Instrumentation using LabVIEW”.1st Edition, PHI, (2010).
10. Wang Lei, Shen Yuming: “Design of Machine vision applications in Detection of defects in high-speed bar copper”. *IEEE International Conference on E-Product E-Service and E-Entertainment (ICEEE)*, pp. 1-4, (2010).
11. I. Laptev, J. Wills, P. Perez, S. J. Belongie: “Periodic Motion Detection and Segmentation via Approximate Sequence Alignment”. IEEE International Conference on Computer Vision, vol. 1, pp. 816 – 823, (2005).
12. Surekha, P. and Sumathi, S.: “LabVIEW based Advance Instrumentation”. 1st Edition, Springer (2007).