DATA ENCRYPTION IN THE IMAGE

Abhishek kastey,akshay vanjara,ashish gautam

Smt radhikatai pandav college of engineering,nagpur

abhi.kastey@gmail.com,ashish.gautam.td@gmail.com, vakshay9@gmail.com

8055689107,8793682429,9545101611

 Abstract:- In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. This paper proposes a novel scheme for separable reversible data hiding in encrypted images. In the first phase, a content owner encrypts the data into the cover image . Data-hiding may be done replacing the LSB bits of the cover image and replacing it with the desired bits of secret image

INTRODUCTION

Steganography is one of many techniques that are used to hide secret information to prevent any attackers to make damage in this information or use it in illegal form. Steganography can be defined as the technique used to embed data or other secret information inside some other object commonly referred to as cover, by changing its properties. The purpose of steganography is to set up a secret communication path between two parties such that any person in the middle cannot detect its existence; the attacker should not gain any information about the embedded data by simply looking at cover file or stego file. Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means “covered writing.” It includes a vast array of secret communications methods that conceal the message’s very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum.

 This paper proposes image steganography. The reason behind the popularity of image steganography is the large amount of redundant information present in the images that can be easily altered to hide secret messages inside them, and because it can take advantage of the limited power of the human visual system (HVS). With the continued growth of strong graphics power in computer and the research being put into image based steganography, this field will continue to grow at a very rapid pace.

TECHNIQUES:

 Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data. For example a grid for 3 pixels of a 24-bit image can be as follows

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

In sample **200** is represented in the form of **11001000**

(0010110**1** 0001110**1** 1101110**0**)

(1010011**0**  1100010**1** 0000110**0**)

(1101001**0**  1010110**0** 01100011)

 Although number was embedded into the first 8 bytes of the grid, only the three underlined bits needed to be changed. On average only half of the bits on an image need to be modified to hide a secret message.

 WORKING OF IMAGE STEGANOGRAPHY:

* Secret Message - The message to be embedded
* Cover Image – An image in which Secret Message will be embedded.
* Stego Image - Cover image that contain embedded message.
* Key – Additional data that is needed for embedding and extracting process.
* Embedding Steganography Algorithm - Steganography Algorithm used to
* embed secret message with cover image.
* Extracting Steganography Algorithm - Inverse function of embedding, in which
* it is used to extract the embedded message (secret message) from stego image.



: IMAGE PROCESSING TOOLBOX

 Image Processing Tool box provides a comprehensive set of reference standard algorithms and graphical tools for image processing, analysis, visualization, and algorithm development. You can perform image enhancement,image deblurring, feature detection, noise reduction, image segmentation, geometric transformations, and image registration. Many toolbox functions are multithreaded to take advantage of multicore and multiprocessor computers.

Image Processing Tool box supports a diverse set of image types, including high dynamic range, gigapixel resolution, embedded ICC profile, and tomographic. Graphical tools let you explore an image, examine a region of pixels, adjust the contrast, create contours or histograms, and manipulate regions of

 interest (ROIs). With toolbox algorithms you can restore degraded images, detect and measure features, analyze shapes and textures, and adjust color balance.

Key Features

▪ Image enhancement, filtering, and deblurring

▪ Image analysis, including segmentation, morphology, feature extraction, and measurement

▪ Spatial transformations and image registration

▪ Image transforms, including FFT, DCT, Radon, and fan-beam projection

▪ Workflows for processing, displaying, and navigating arbitrarily large images

▪ Modular interactive tools, including ROI selections, histograms, and distance measurements

▪ ICC color management

▪ Multidimensional image processing

▪ Image-sequence and video display

APPLICATION

* LEGITIMATE
* Digital Watermarking
	+ Prevent illegal modification , copying and distribution
	+ Identification in ownership disputes and content authentication
	+ Provide explanatory information with the image
* Use to hide the sensitive information on storage media
* **ILLEGITIMATE**
* Corporate espionage
	+ Theft of trade secrets
	+ Terrorism
	+ USA article by Jack Kelly-”Terror group hide behind the web encryption”(05-02-2001)
	+ Hiding secrets in websites like e-bay, Amazon etc

CONCLUSION:-The LSB stegenography leads to transfer of desired text or image by encrypting them into the host image.As only LSB are replaced in host image the resultant image is not distorted and data encryption cannot be visually detected.

**REFERENCE**

* Silman, J., “Steganography And Steganalysis: An Overview”, SANS Institute, 2001
* Jamil, T., “Steganography: The Art Of Hiding Information Is Plain Sight”, IEEE Potentials, 18:01, 1999
* Xinpeng Zhang ,”Separable Reversible Data Hiding in Encrypted Image”, IEEE Transactions, Vol. 7, No. 2, April 2012
* Artz, D., “Digital Steganography: Hiding Data within Data”, IEEE Internet Computing Journal, June 2001
* Dr Hans Georg Schaathun, University of Surrey, Spring 2009