ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2350-0174
Vol.03, Issue.02
April-2023
Pages: 702-711

IMPLEMENTATION OF TEXT AND IMAGE STEGANOGRAPHY USING AES

Y.Murali krishna[1], G.Mounika[2], CH.Sirisha[3], G.Ravindhra[4], G.Yogendhra[5]

[1]*Associate professor,Department of Electronics and Communication Engineering, Kallam Haranadha Reddy Institute of Technology, Guntur, India*

[2,3,4,5]*Student,Department of Electronics and Communication Engineering, Kallam Haranadha Reddy Institute of Technology, Guntur, india*

ABSTARCT

One of the major problems faced by tworld today is Data Security. In reality communication channel which is used to transfer data from transmitter to receiver is highly insecure. To resolve this problem the data is being manipulated to another form, so that the person with access to the secret key can only read it. This process of manipulation of original data to another form so that eavesdropper cannot access it, is known as encryption. Advanced Encryption Standard (AES) is the most commonly used algorithm for data encryption. This algorithm can be applied on both text and image. In this paper the input to AES algorithm is Text and an image, which results in encrypted output. This encrypted output is given as an input to AES decryption algorithm, which results in decrypted output. The algorithm is implemented using MATLAB software.

1.INTRODUCTION

Nowadays in communication sytems security plays an important role. Datas are transfered over the internet by most of the public or government organization. The data can be achieved by evasdropper if it is transmitted to the reciever through an insecure channel. As the security of electronic data is a major issue, the public and the private sectors uses different kinds of techniques and methods to protect the data from evasdropper. Cryptography is the art of hiding information by encryption and decoding it by decryption. Through the process of encryption the plain text is converted to unreadable format known as cipher text and the cipher text is then converted back to the plain text through the process of decryption. Cryptography provides integrity, authentication and maintain secrecy of information. The ciphers are classifed into block and stream ciphers. Encryption of input data is done bit by bit in stream cipher while block cipher converts the original message into an encrypted message. There are many block cipher algorithm like DES, Two fish, AES and lot more. Here we used AES [1] [2] algorithm.

1.1 Problem Statement

- The aim of the project is **TEXT AND IMAGE STEGANOGRAPHY USING AES (ADVANCED ENCRYPTION STANDARD)**

1.2 Necessity

- With the increasing usage of digital communication, there is growing concern for privacy and security of sensitive information
- Traditional methods of transmitting information can easily be intercepted and read by unauthorized users, leading to potential harm or exploitation.
- Steganography is the art of hiding secret information within an innocuous media, such as an image or text, to prevent unauthorized access or modification.
- This project aims to develop a text and image steganography system using the Least Significant Bit (LSB) technique and Advanced Encryption Standard (AES) in MATLAB.

• The proposed system should be able to encrypt and embed secret text and secret image within an image, as well as extract and decrypt the secret text and secret image from the stego image.

1.3 Objectives

- Design and implement a text steganography system using the LSB technique in MATLAB
- Design and implement an image steganography system using discrete wavelet transform and perform AES encryption in MATLAB.
- Develop a user-friendly interface for encryption and embedding, as well as decryption and extraction of secret text.
- Evaluate the robustness and security of the proposed system through experimental results.
- Provide a comprehensive report on the implementation, performance, and evalution of the system.

2.LITERATURE SURVEY

2.1 Text Steganography using LSB

Text steganography using LSB is a simple and straightforward technique for hiding secret messages within text files. The LSB technique works by replacing the least .significant bits of the text file with the secret message. This results in a minor change to the text file that is not noticeable to the human eye, but contains the secret message.Several studies have been conducted on the performance and security of text steganography using LSB. For example, a study by Rashid and Jain (2017) evaluated the performance of text steganography using LSB on various types of text files, including ASCII, UTF-8, and Unicode text. The results showed that the LSB technique had a low capacity for hiding secret messages and was vulnerable to attacks.

2.2 Image Steganography using DWT and AES

Image steganography using DWT and AES is a more advanced and secure technique for hiding secret information within images. DWT is used to transform the image into its frequency components, which are then used to hide the secret message. AES encryption is used to encrypt the stego-image to prevent unauthorized access. A study by Al-Ani and Al-Nuaimi (2017) proposed an image steganography system using DWT and AES. The results showed that the proposed system had a higher capacity for hiding secret messages and was more secure than traditional image steganography techniques. Image Steganography using Discrete Wavelet Transform (DWT) is a technique for hiding secret information within images. DWT is a mathematical tool used to break down an image into its frequency components, which can then be used to hide the secret message

3.IMAGE AND IMAGE FILE FORMATS

3.1 Introduction to an image

An image is a two-dimensional picture, which has a similar appearance to some subject usually a physical object or a person. Image is a two-dimensional, such as a photograph, screen display, and as well as a three-dimensional, such as a statue. They may be captured by optical devices such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water surfaces. The word image is also used in the broader sense of any two-dimensional figure such as a map, a graph, a pie chart, or an abstract painting. In this wider sense, images can also be rendered manually, such as by drawing, painting, carving, rendered automatically by printing computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph

Fig 3.1: RGB and Grayscale image

An image is a rectangular grid of pixels. It has a definite height and a definite height and a definite width counted in pixels. Each pixel is square and has a fixed size on a given display

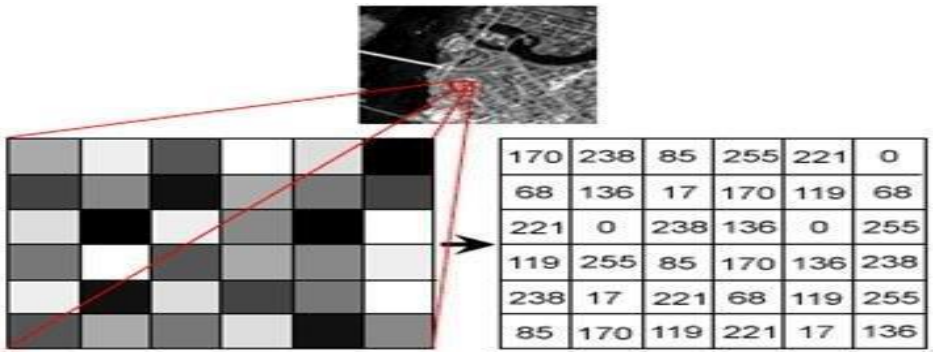


Fig 3.2: image in matrix form

Each pixel has a color. The color is a 32-bit integer. The first eight bits determine the redness of the pixel, the next eight bits the greenness, the next eight bits the blueness, and the remaining eight bits the transparency of the pixel.

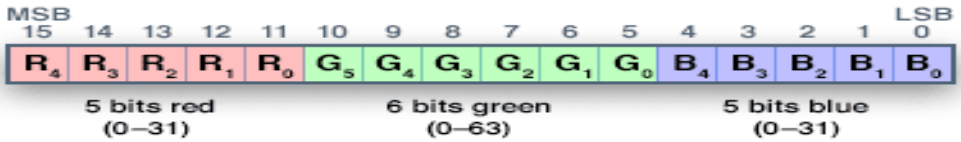


Fig 3.3 RGB Image Format

3.2 Image File Sizes

Image file size is expressed as the number of bytes that increases with the number of pixels composing an image, and the color depth of the pixels. The greater the number of rows and columns, the greater the image resolution, and the larger the file. Also, each p ixel of an image increases in size when its color depth increases, an 8-bit pixel (1 byte) stores 256 colors, a 24-bit pixel (3 bytes) stores 16 million colors, the latter known as true color.

3.3 Image File Formats

Image file formats are standardized means of organizing and storing images. This is about digital image formats used to store photographic and oiler images Image files are composed of either pixel or vector (geometric) data that are rasterized to pixels when displayed (with few exceptions) in a vector graphic display. Including proprietary types, there are hundreds of image file types. The PNG, JPEG, and GIF formats are most often used to display images Internet.

Fig 3.3: Image file formats

3.3.1 Raster Formats

These formats store images as bitmaps (also known as pix maps).

• JPEG/JFIF:

JPEG (Joint Photographic Experts Group) is compression method. JPEG compressed images are usually stored in the JFIF (JPEG File Interchange Format) file format IPEG compression is lossy compression.

• EXIF:

The EXIF (Exchangeable image file format) format is a file standard similar to the JFIF format with TIFF extensions. It is incorporated in the IPEG writing software used in most cameras, its purpose is to record and to standardize the exchange of images with image metadata between digital cameras and editing and viewing software. The metadata are recorded for individual images and include such things as camera settings, time and date, shutter speed, exposure, image size, compression, name of camera, color information, etc. When images are viewed or edited by image editing software, all of

this image information. can be displayed.

• TIFF:

The TIFF (Tagged Image File Format) format is a flexible format that normally saves 8 bits or 16 bits per color (red, green, blue) for 24-bit and 48-bit totals, respectively, usually using either the TIFF or TIF filename extension. TIFFs are lossy and lossless. Some offer relatively good lossless compression bi-level (black & white) images. Some digital cameras can save in TIFF format, using the LZW compression algorithm for lossless storage. TIFF image format is not widely supported by web browsers. TIFF remains widely accepted as a photograph file standard in the printing business. TIFF can handle device-specific color spaces, such as the CMYK defined by a particular set of printing press inks.

• PNG:

The PNG (Portable Network Graphics) file format was created as the free, opensource successor to the GIF. The PNG file format supports true color (16 million colors) while the GIF supports only 256 colors.

• GIF:

(Graphics Interchange Format) is limited to an 8-bit palette, or 256 colors. This makes the GIF format suitable for storing graphics with relatively few colors such as simple diagrams, shapes, logos and cartoon style images. The GIF GIF format supports animation and is still widely used to provide image animation effects. It also uses a lossless compression that is more effective when large areas have a single color, and ineffective for detailed images or dithered images.

• BMP:

The BMP file format (Windows bitmap) handles graphics files within the Microsoft Windows OS Typically, BMP files are uncompressed, hence they are large. The advantage is their simplicity and wide acceptance in Windows programs

3.3.2 Vector Formats

As opposed to the raster image formats above (where the data describes the characteristics of each individual pixel), vector image formats contain a geometric description which can be rendered smoothly at any desired display size. At some point, all vector graphics must be rasterized in order to be displayed on digital monitors. However, vector images can be displayed with analog CRT technology such as that used in some electronic test equipment, medical monitors, radar displays, laser shows

• CGM:

CGM (Computer Graphics Metafile) is a file format for 2D vector graphics, raster graphics, and text. All graphical elements can be specified in a textual source file that can be compiled into a binary file or one of two text representations CGM provides a means of graphics data interchange for computer representation of 2D graphical information independent from any particular application, system, platform, or device.

• SVG:

SVG (Scalable Vector Graphics) is an open standard created and developed by the World Wide Web Consortium to address the need for a versatile, scriptable and all-purpose vector format for the web and otherwise. The SVG format does not have a compression scheme of its own, but due to the textual nature of XML, an SVG graphic can be compressed using a programs

4. PURPOSE OF IMAGE PROCESSING

- Visualization-observe the objects that are not visual
- Image sharpening and restoration-to create a better image
- Image retrieval-seek for the image of interest
- Measurement of pattern-measures various objects in an image
- Image recognition-distinguish the objects in an image

4.1Types of Images

• Binary Image (Black or White)

Each pixel is just black or white since there are only two possible values for each pixel, we only need one bit for pixel. Such images can therefore be very efficient in terms of storage images for which a binary representation may be suitable include test (printed or handwriting), finger prints, artificial plans.

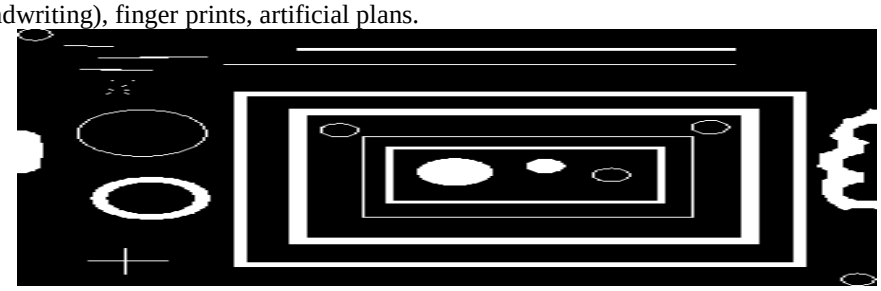


Fig 4.1: Binary Image

• Gray Scale Image

Each pixel is a shade of gray, normally from 0(black) to 255(white) this range means that each pixel can be represented by 8 bits or exactly 1 bit, or exactly 1 byte, images in this type are in shades of gray.one major reason in using gray sale image is that less information is needed for each pixel. In fact, gray is pone in which red, green and blue components all have equal intensity in RGB space, and so it is only necessary to specify single intensity value for each pixel.

Fig 4.2: Gray Image

- **True Color Image**

Here each pixel has a particular color, that color being described by the amount of RED BLUE, GREEN in it If each of these components has a range 0 to 255, this gives a total of 255 ^3=16,777,216 different possible colors in the image. Most of the colored images belong to this image, there are images that appear to the human eye as "real" colors that is combination of the additive primary colors of RED, GREEN, BLUE.

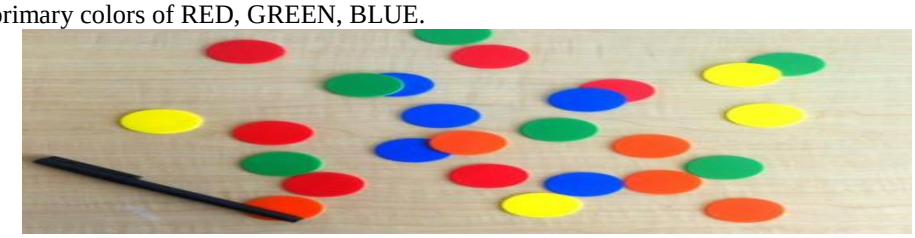
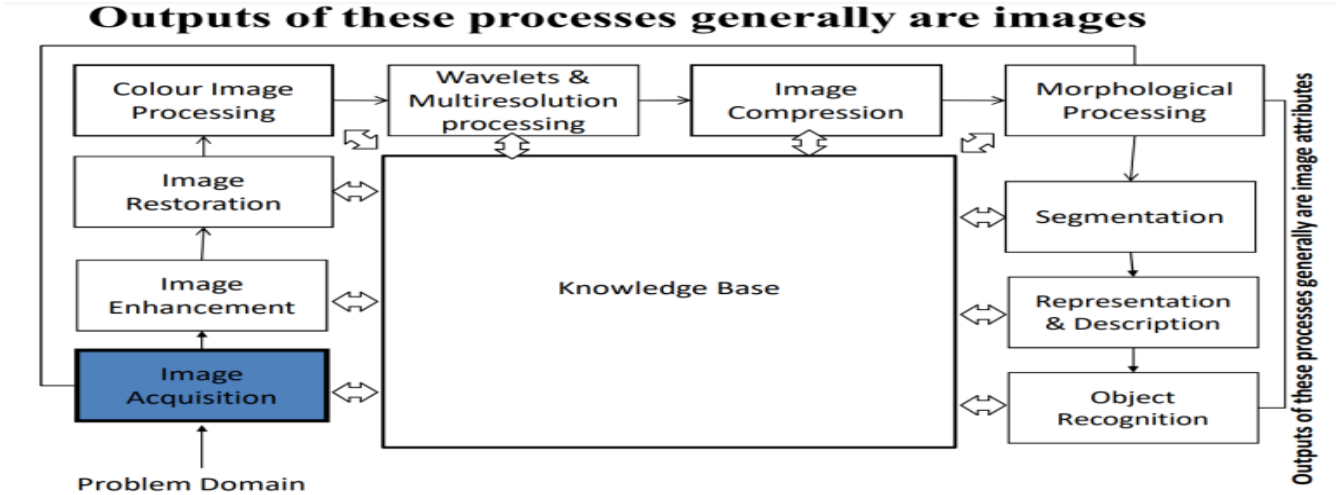


Fig 4.3: True Color Image

4.2 Fundamental Steps in Digital Image Processing



4.2.1 Image Acquisition

Image Acquisition is to acquire a digital image. To do so requires an image sensor and the capability to digitize the signal produced by the sensor. The sensor could be monochrome or color TV camera that produces an entire image of the problem domain every 1/30 sec. the image sensor could also be line scan camera that produces a single image line at a time. In this case, the objects motion past the line.

Fig 4.2.1: Image Acquisition by camera

Scanner produces a two-dimensional image. If the cap of the camera or other imaging sensor is not in digital form, an analog to digital converter digitizes it. The nature of the sensor and the image it produces are determined by the application.

Fig 4.2.1: Image Acquisition by mobile

4.2.2 Image Enhancement

Image enhancement is among the simplest and most appealing areas of digital image processing. Basically, the idea behind enhancement techniques is to bring out detail that is obscured, or simply to highlight certain features of interesting an image. A familiar example of enhancement is when we increase the contrast of an image because "it looks better." It is important to keep in mind that enhancement is a very subjective area of image processing.

. Fig 4.6: Image Enhancement

4.2.3 Image Restoration

Image restoration is an area that also deals with improving the appearance of an image. However, unlike enhancement, which is subjective, image restoration is objective, in the sense that restoration techniques tend to be based on mathematical or probabilistic models of image degradation.

Fig 4.2.3: Image Restoration

4.2.4 Color Image Processing

The use of color in image processing is motivated by two principal factors. First, color is a powerful descriptor that often simplifies objectidentification and extraction from a scene. Second, humans can discern thousands of color shades and intensities, compared to about only two dozen shades of gray. This second factor is particularly important in manual image analysis.

Fig 4.2.4: Color Image Processing

4.2.5 Wavelets and Multi Resolution Processing

Wavelets are the formation for representing images in various degrees of resolution Although the Fourier transform has been the mainstay of transform based image processing since the late 1950's, a more recent transformation, called the wavelet transform, and is now making it even easier to compress, transmit, and analyze many images Unlike the Fourier transform, whose basis functions are sinusoids, wavelet transforms are based on small values, called Wavelets, of varying frequency and limited duration

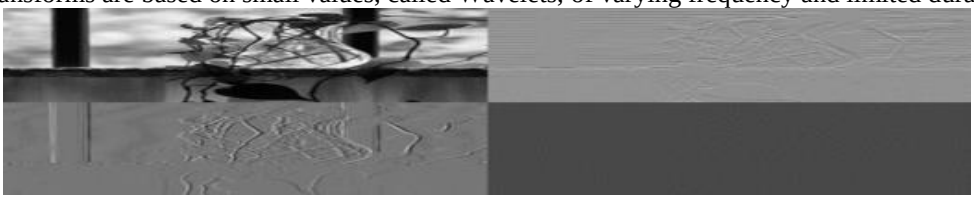


Fig 4.2.5: Wavelets and Multi Resolution Processing

4.2.6 Compression

Compression, as the name implies, deals with techniques for reducing the storage required saving an image, or the bandwidth required for transmitting it. Although storage technology has improved significantly over the past decade, the same cannot be said for transmission capacity. This is true particularly in uses of the Internet, which are characterized by significant pictorial content. Image compression is familiar to most users of computers in the form of image file extensions, such as the jpg file extension used in the JPEG (Joint Photographic Experts Group) image compression standard

4.2.7 Morphological Processing

Morphological processing deals with tools for extracting image components that are useful in the representation and description of shape. The language of mathematical morphology is set theory. As such, morphology offers a unified and powerful approach to numerous image processing problems. Sets in mathematical morphology represent, objects in an image. For example, the set of all black pixels in a binary image is a complete morphological description of the image

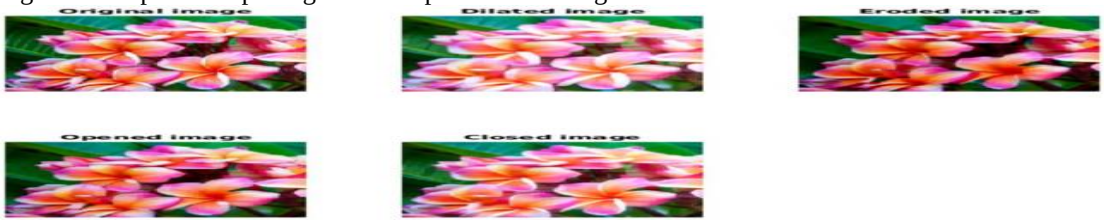


Fig 4.2.7: Morphological Processing

4.2.8 Segmentation

Segmentation procedures partition an image into its constituent parts or objects. In general, autonomous segmentation is one of the most difficult tasks in digital image processing. A rugged segmentation procedure brings the process a long way toward solution of imaging problems that require objects to be identified individually

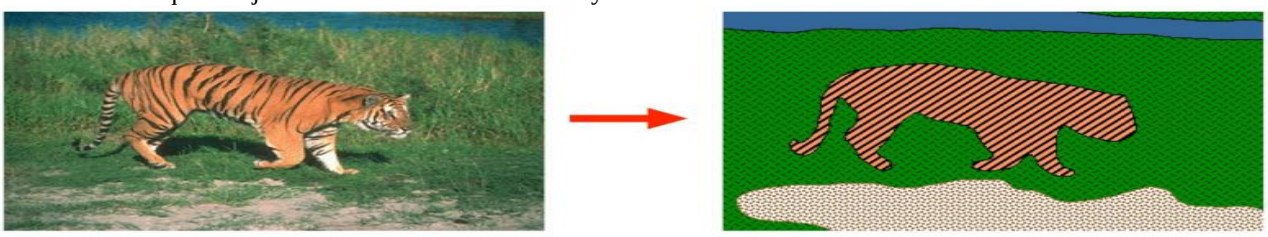


Fig 4.2.8: Segmentation

5. LSB STEGANOGRAPHY

The Least Significant Bit (LSB) technique is a method used in digital image and audio steganography to hide information within digital media. It is also used in text steganography for the same purpose. In this method, the least significant bit of each pixel in an image or sample in an audio file is used to store the hidden message. The advantage of this method is that it is not easy to detect the hidden message as it only affects the least significant bit of each pixel or samp

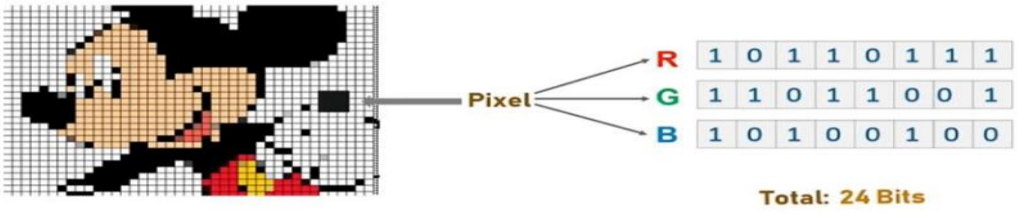


Fig 5: LSB Steganography

5.1 Embedding of Secret Text

Encrypting a text into an image using the Least Significant Bit (LSB) technique is a process that involves hiding a message within an image In such a way that it is not easily detectable. This method is commonly used in steganography, which is the practice of hiding information within digital media. LSB steganography is a popular technique because it is efficient, easy to implement, and difficult to detect

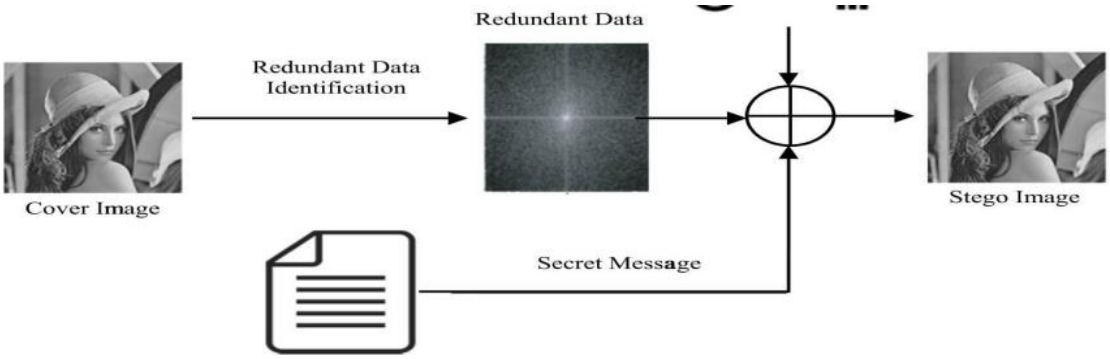


Fig 5.1: LSB Encryption

5.2 Extraction of Secret Text

Decrypting a text from a stego image using the Least Significant Bit (LSB) technique is a process that involves extracting a hidden message from an image that has been encrypted using LSB steganography. LSB steganography is a popular method of hiding information within digital media because it is efficient, easy to implement, and difficult to detect.

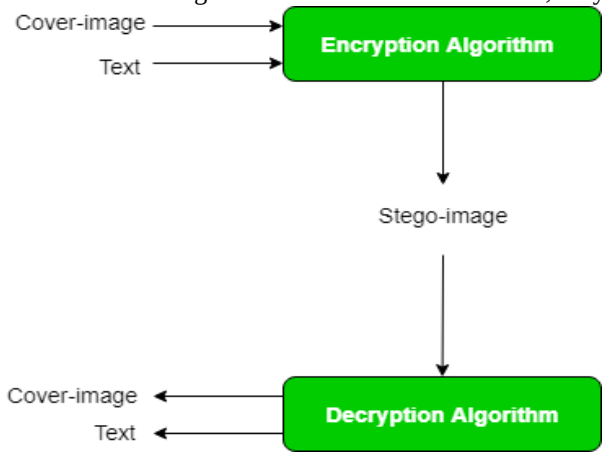


Fig 5.2: Secret text decryption

6.AES ENCRYPTION AND DECRYPTION

Advanced Encryption Standard (AES) is a widely-used symmetric encryption algorithm that can be used to encrypt images. AES uses a fixed-length key to encrypt and decrypt data, and is considered to be one of the most secure encryption algorithms available.

The process of encrypting an image using AES involves the following steps:

a) 1. Converting the image into a digital format, such as a JPEG or PNG file.
b) 2. Converting the image into a stream of bytes, as AES operates on data in byte form.
c) 3. Selecting a key size and generating a key. AES supports key sizes of 128 bits, 192 bits, and 256 bits. The key is used to encrypt and decrypt the data, and it must be kept secret.
d) 4. Dividing the image into blocks, as AES operates on fixed-sizeblocks of data. Each block is then encrypted using the key.
e) 5. Encrypting each block using a block cipher algorithm. AES uses a combination of
f) substitution and permutation operations to encrypt the data.
g) 6. Concatenating the encrypted blocks to form the encrypted image.
h) 7. Storing the encrypted image

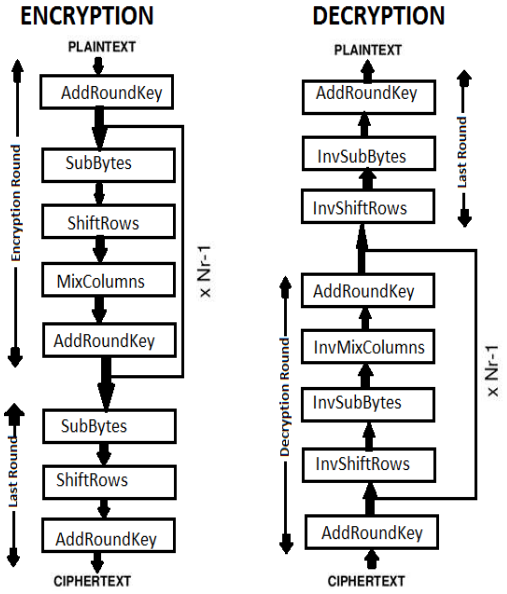


Fig 6: Advanced Encryption Standard (AES)

7.MATLAB SOFTWARE

MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming in an easy-to-use environment where problems and solutions are expressed in familiar mathematical notation Typical uses include:

1. Math and computation
2. Algorithm development
3. Data acquisition
4. Modeling, simulation, and prototyping
5. Data analysis, exploration, and visualization
6. Scientific and engineering graphics
7. Application development, including graphical user interface building

8.RESULT

The secret text from the stego image must be extracted by the receiver so as to be able to receive the secret text sent by the sender by clicking **theExtract Secret Text** button.

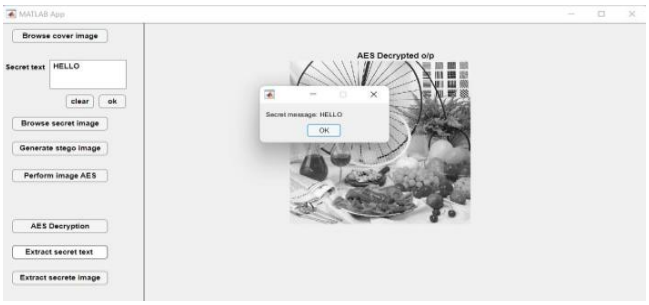


Fig 8.1 Extract Secret Text

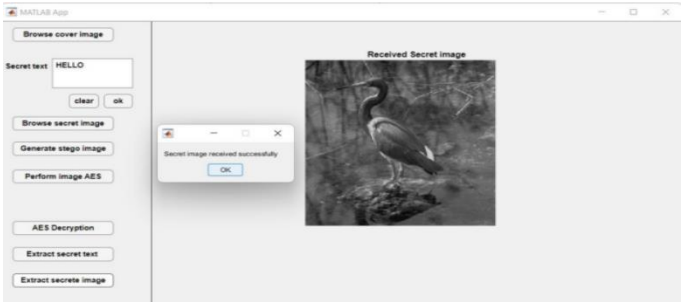


Fig 8.2 Extract Secret Image

9 APPLICATIONS

• **Secret Communication:** Steganography can be used to send secret messages or information between two or more parties without detection. This can be particularly useful for governments, military organizations, or individuals who need to transmit confidential information securely.

• **Digital Forensics:** Steganography can be used to hide evidence or information in digital images, making it a useful tool for digital forensics investigators.

10 ADVANTAGES

1. **Concealment of sensitive information** – Steganography allows for the concealment of sensitive information, making it difficult for unauthorized individuals to access or steal it.
2. **Communication secrecy** – Steganography can be used to send secret messages, allowing for covert communication between parties.
3. **Tamper-proofing –** Steganography can be used to embed digital signatures or watermarks into a file, making it possible to detect if the file has been tampered with.
4. **Data protection** – Steganography can be used to protect important data from being destroyed or altered, by embedding it in a seemingly harmless file.
5. **Avoiding censorship** – Steganography can be used to bypass censorship by disguising the content of a message, which can be useful for people living in countries with restrictive internet policies.

11 CONCLUSION

In conclusion, the project "Text and Image Steganography using AES" has successfully achieved its objectives. The implementation of LSB and DWT techniques in text and image steganography, respectively, has proven to be effective in hiding the secret message within the cover media. Furthermore, the use of AES encryption in protecting the cover image has added an extra layer of security to the steganography system. The results of the simulations showed that the secret message can be embedded and extracted accurately, and the quality of the cover media was not significantly affected.

12 REFERENCES

[1] C.C. Chang, J.C. Hsiao, and L.S. Liao, "An improved LSB image steganography using color image," International Journal of Computer Science and Network Security, vol. 5, no. 2, 2005, pp. 149-156.

[2] A.R. Ansari and S. Jain, "Steganography using LSB method on grayscale images," International Journal of Computer Applications, vol. 141, no. 2, 2016, pp. 12-17.

[3] J. Guo, X. Liu, and J. Li, "An image steganography algorithm based on DWT and SVD," Journal of Electronic Imaging, vol. 19, no. 3, 2010, pp. 033005-1-033005-7.

[4] A.R. Ansari and S. Jain, "Image Steganography Using Discrete Wavelet Transform and Encryption," Journal of Information and Communication Technology, vol. 9, no. 1, 2010, pp. 1-9.

[5] N. Khan and R. Uddin, "A review of image steganography techniques," International Journal of Computer Science and Information Security, vol. 11, no. 2, 2013, pp. 27-37