International Journal of Engineering, Management and Humanities (IJEMH)
Volume 3, Issue 5, pp: 54-58 www.ijemh.com

Secure Text –Authentication Scheme Using Bit Encoding and Decoding Technique

Ms.J.Sri Arunaa,M.E,*Assistant professor,*
Department of Electronics and Communication Engineering
Apollo Engineering College

B.Swathi,B.E,
Department of ME VLSI DESIGN
Engineering Students of Apollo Engineering College

Date of Submission: 15-09-2022 Date of Acceptance: 30-09-2022

ABSTRCT-Text encryption is process of hiding the text into the image in order to prevent unauthorized persons to gain access to confidential message. Message is the transfer of information from the sender to the receiver through a particular medium. Encryption is the most effective process for achieving data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. In existing, texts were hidden by the watermark method. The proposed method called bit planes, using that method extract the selected image by hiding the text to the selected planes. An original image is encrypted with a secret key, without knowing the encryption key the text will not be retrieved. During the decryption process, the secret message can be extracted with the secret key

I. INTRODUCTION

An image may be define as two dimensional function. F(x,y),where x and y are spatial coordinates and the amplitude of any pair of coordinates (x,y) is called the intensity or a grey level of the image at that point. When x,y and the amplitude values of f are all finite, discrete quantities, we call the image as digital image.

DIGITAL IMAGE PROCESSING

The field of digital image processing refers to processing digital images by means of a digital computer. A digital image composed of a finite number of elements, each of which has a particular location and value. These elements are referred to as picture elements, image elements, pels, and pixels.

IMAGE PROCESSOR

An image processor does the functions of image acquisition, storage, preprocessing, segmentation, representation, recognition and interpretation and finally displays or records the resulting image. The following block diagram gives the fundamental sequence involved in an image . As detailed in the diagram, the first step in the process is image acquisition by an imaging sensor in conjunction with a digitizer to digitize the image. The next step is the preprocessing step where the image is improved being fed as an input to the other processes. Preprocessing typically deals with enhancing, removing noise, isolating regions, etc. Segmentation partitions an image into its constituent parts or objects. The output of segmentation is usually raw pixel data, which consists of either the boundary of the region or the pixels in the region themselves. Representation is the process of transforming the raw pixel data into a form useful for subsequent processing by the computer. Description deals with extracting features that are basic in differentiating one class of objects from another. Recognition assigns a label to an object based on the information provided by its descriptors. Interpretation involves assigning meaning to an ensemble of recognized objects. The knowledge about a problem domain is incorporated into the knowledge base. The knowledge base guides the operation of each processing module and also controls the interaction between the modules. Not all modules need be necessarily present for a specific function. The composition of the image processing system depends on its application. The frame rate of the image processor is normally around 25 frames per second.

APPLICATIONS OF DIGITAL IMAGE PROCESSING

Digital image processing has a broad spectrum of applications, such as remote sensing via satellites and other spacecraft's, image transmission and storage for business applications, medical processing, radar, sonar and acoustic image processing, robotics and automated inspection of industrial parts.

MEDICAL APPLICATIONS

In medical applications, one is concerned with processing of chest X-rays, cine angiography, projection images of Transaxial tomography and other medical images that occur in radiology, nuclear magnetic resonance (NMR) and ultrasonic scanning. These images may be used for patient screening and monitoring or for detection of tumors or other disease in patients.

SATELLITE IMAGING

Images acquired by satellites are useful in tracking of earth resources; geographical mapping; prediction of agricultural crops, urban growth and weather, flood and fire control, and many other environmental applications. Space image applications include recognition and analysis of objects contained in image obtained from deep space-probe missions.

COMMUNICATION

Transmission and storage applications occur in broadcast television, teleconferencing, and transmission of facsimile images for office automation, communication of computer networks, closed-circuit television based security monitoring systems and in military communications.

RADAR IMAGING SYSTEMS

Radar and sonar images are used for detection and recognition of various types of targets or in guidance and maneuvering of aircraft or missile systems.

DOCUMENT PROCESSING

It is used in scanning, and transmission for converting paper documents to a digital image form, compressing the image, and storing it on magnetic tape. It is also used in document reading for automatically detecting and recognizing printed characteristics.

DEFENSE/INTELLIGENCE

It is used in reconnaissance photo-interpretation for automatic interpretation of earth satellite imagery to look for sensitive targets or military threats and target acquisition and guidance for recognizing and tracking targets in real-time smart-bomb and missile-guidance systems.

BIT PLANE EXTRACTION

Gray scale image are basically those image which we say black and white image. Each pixel of gray scale image has a value lies in between 0 – 255 which decides at which position, the image will be black and at which position, it willbe white. If pixel value is 0, it means that pixel color will be fully black and if pixel value is 255, then that pixel will be fully white and pixel having intermediate value will be having shades of black and white. We are given a Gray scale Image. Since pixel value of gray scale image lies between 0 -255, so its information is contained using 8 bit. So, we can divide that image into 8 planes (8 Binary Image). Binary image are those images whose pixel value can be either 0 or 1. So, our task is to extract each bit planes of original image to make 8 binary images. Let particular pixel of gray scale image has value 212. So, its binary value will be 11010100. So, its 1st bit is 0, 2nd is 0, 3rd is 1, 4th is 0, 5th is 1, 6th is 0, 7th is 1, 8th is 1. In this manner, we will take this 8 bit of all pixels and will draw 8 binary images. We have to do this all the pixels and generate new images.

GREY SCALE IMAGE

Greyscale images consist of only grey tones of colors, which are only 256 steps .In other words, there are only 256 grey colors. The main characteristics of greyscale images is the equality of the red, green, blue color levels .The color code will be like RGB(R,R,R) or (G,G,G) or (B,B,B) where R,G,B is a number between 0 and 255 individually .To convert the image from RGB full color to greyscale, there are many ways has they are all mathematical solution

IMAGE FILES

To a computer, an image is an array of numbers that represent light intensities at various points or pixels. These pixels make up the image's raster data. A common image size is 640 * 480 and 256 colors (or 8 bits per pixel). Such an image could contain about 300 kb of data. Digital images are typically stored as either 24-bit or 8- bit files. A 24-bit image provides the most space for hiding information , however, it can be quite large except for the JPEG images. A 24-bit image of 1,024 pixels width and 768 pixels height has more than two million pixels, each having 24-bits, which would produce a file exceeding 2 Mega bytes. Such a file would attract attention during transmission.

File compression would thus be beneficial, if not necessary, to transmit such a file.

FILE COMPRESSION

There are two types of file compression methods- lossless and lossy. Both methods save storage space but have different results, interfering with the hidden information, when information is uncompressed. Lossless compression lets us reconstruct the original message exactly; therefore it is preferred when the original information must remain intact (as with steganographic images). Lossless compression is typical of images saved as GIF and 8-bit BMP.

Lossless compression, on the other hand, saves space but may not maintain the original image’s integrity. This method typifies images saved as JPEG. Due to the lossy compression algorithm, which we discuss later, the JPEG formats provide close approximations to high-quality digital photographs but not an exact duplicate. Hence the term called as “lossy compression”.

EMBEDDING:-

The embedding system data, which is to be hidden,into an image requires two files. The first is the innocent looking image that will hold the hidden information, called the cover image. The second file is the message (the information to be hidden). A message may be plain text, cipher text, other images, or anything that can be embedded in a bit stream. when combined, the cover image and the embedded message make a stego- image. A stego-key (a type of password) may also be used to hide, and then later decode, the message.

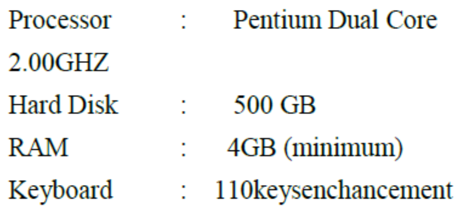
Most steganographic software neither supports nor recommends using JPEG images. But recommends instead the use of lossless 24-bit images such as BMP. The next best alternative to 24-bit images is 256- color or gray scale images. The most common of these found on the Internet are GIF files.

In 8-bit color images such as GIF files, each pixel is represented by a single byte, and each pixel nearly points to a color index table (a palette) with 256 possible colors. The pixels value is between 0 and 255. The software simply paints the indicated color on the screen at the selected pixel position.

Many steganography experts recommend the use of images featuring 256 shades of gray. Gray scale images are preferred because the shades change very gradually from byte to byte, and the less the value changes between palette entries, the better they can hide information.

When considering an image in which to hide information, you must consider the image as well as the palette. Obviously, an image with large areas of solid colors is a poor choice, as variances created from the embedded massage will be noticeable in the solid areas.

HARDWARE SPECIFICATIONS0



Processor	:	Pentium Dual Core 2.00GHZ
Hard Disk	:	500 GB
RAM	:	4GB (minimum)
Keyboard	:	110keysenchancement

SOFTWARE SPECIFICATIONS

The software details of the project are given below:- MATLAB 8.6 Version R2016a MATLAB (matrix laboratory) numerical computing environment and fourth-generation programming language. Developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine, allowing access to symbolic computing capabilities. An additional package, Simulink, adds graphical multi-domain simulationand Model-Based Design for dynamic and embedded systems.

In 2004, MATLAB had around one million users across industry and academia. MATLAB users come from various backgrounds of engineering, science, and economics. MATLAB is widely used in academic and research institutions as well as industrial enterprises.

MATLAB was first adopted by researchers and practitioners in control engineering, Little's specialty, but quickly spread to many other domains. It is now also used in education, in particular the teaching of linear algebra and numerical analysis, and is popular amongst scientists involved in image processing. The MATLAB application is built around the MATLAB language. The simplest way to execute MATLAB code is to type it in the Command Window, which is one of the elements of the MATLAB Desktop. When code is entered in the Command Window, MATLAB can be used as an interactive mathematical shell. Sequences of commands can be saved in a text file, typically using the MATLAB

Editor, as a script or encapsulated into a function, extending the commands available.

MATLAB provides a number of features for documenting and sharing your work. You can integrate your MATLAB code with other languages and applications, and distribute your MATLAB algorithms and applications.

D. Block Diagram

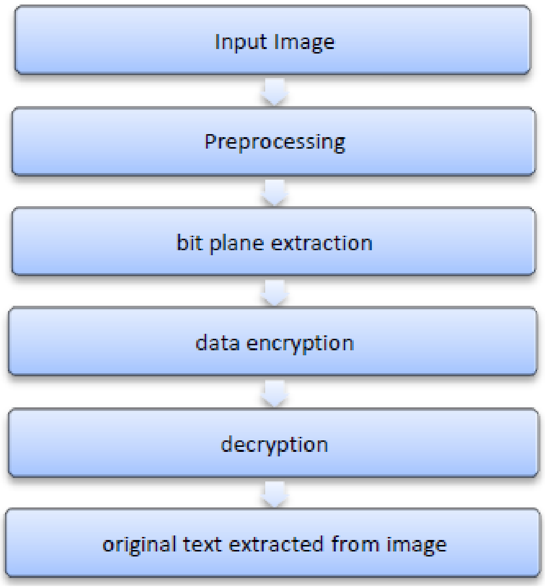


Fig 5 Block Diagram

SNAPSHOTS

1. Show the input image

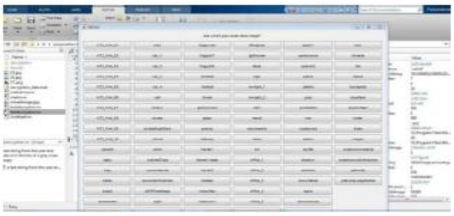


Fig2.1input image

2. Select the image and add the text

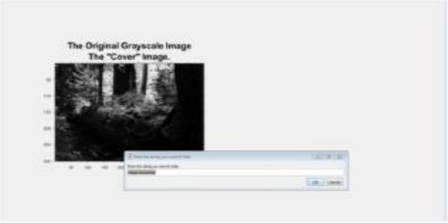
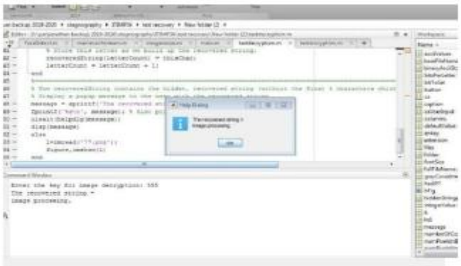


Fig2.2 select image and adding text

5. Encrypt the text to the image



```
Enter the key for image decryption: 555
The recovered string =
image processing.
```

Fig 2.5 Encrypting text into image

6. Decrypt with correct key

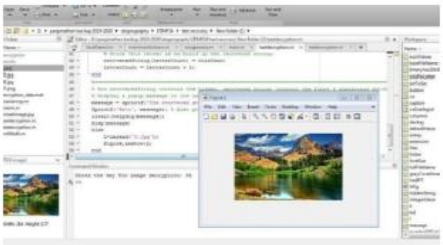


Fig2.6 decrypt with correct key

3. Select the bit plane number

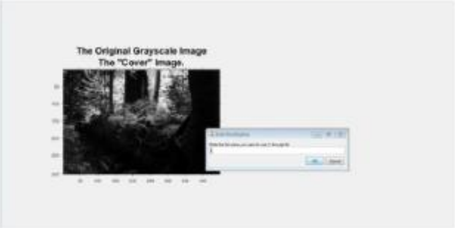


Fig2.3 select bit plane number

4. **Convert text into pixel**

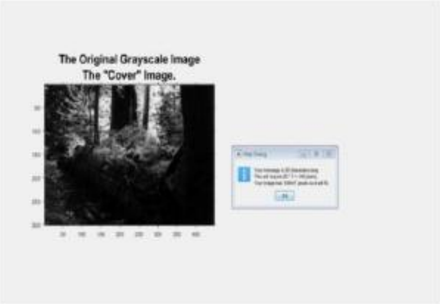


Fig 2.4 Converting text into pixel

7. Decrypt with the wrong key

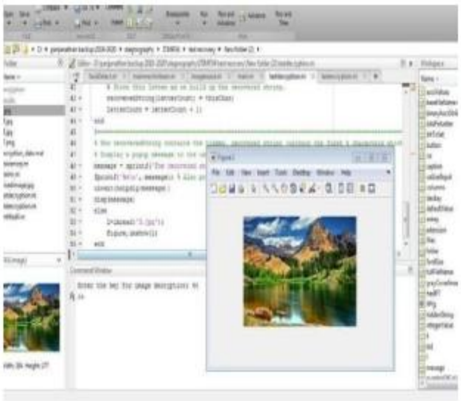


Fig2.7Decrypt with wrong key

II. CONCLUSION AND FUTURE WORK :

In, this paper analyzed the security performance of a text encryption scheme based on bit-plane extraction. Based on the identified security defects, we proposed efficient know- plaintext and chosen-plain text attacks for recovering some information of the original plain text. Adopting a statistical value of the plain-image in the diffusion phase; building a relation mechanism between each position of the LSBs plane with the corresponding position in the MSBs plane to reduce the correlation among neighboring pixels of the plain-text.

REFERENCES

[1]. Image encryption based on Independent Component Analysis and Arnold's Cat Map NidaaAbdulMohsin Abbas University of Babylon, College of IT, Iraq Received 27 May 2015; revised 3 October 2015; accepted 16 October 2015.

[2]. Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images Dalel Bouslimi, Member, IEEE, Member, IEEE, Michel Cozic, and Christian Roux, Fellow, IEEE.,VOL. 16, NO. 5, SEPTEMBER 2012.

[3]. Digital image watermarking: its formal model, fundamental properties and possible attacks Hussain Nyeem1*, Wageeh Boles2 and Colin Boyd2,3., Nyeem et al. EURASIP Journal on Advances in Signal Processing 2014, 2014:135.

[4]. Hiding in encrypted images: a three tier security data hiding technique Shabir A. Parah1 · Javaid A. Sheikh1 · Umer I. Assad2 · Ghulam M. Bhat1., Received: 19 August 2014 / Revised: 13 August 2015 / Accepted: 27 August 2015.

[5]. H.-C. Lin, C.-N.Yang, C.-S.Laih, and H.-T. Lin, ``Natural language letter based visual cryptography scheme," J. Vis. Commun. Image Represent., vol. 24, no. 3, pp. 318331, 2013.

[6]. S. A. Sattar, S. Haque, M. K. Pathan, and Q. Gee, ``Implementation challenges for Nastaliq character recognition," in Proc. Int. Multi Topic Conf. Berlin, Germany: Springer, 2008, pp. 279285.