IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 17-26

An Epitome Perspective on Image Steganographic Methods for Optimum Hiding Capacity

[1]K.Shahana,[2] S.Sindhu,[3] P.Yuvalakshmi,[4] Mrs. Saranya.S.
[1,2,3] UG Student, [4] Associate Pprofessor , Department of Electronics and Communication, Dhanalakshmisrinivasan college of engineering and technology, Mamallapuram, kancheepuram district.

Abstract: *Steganography gained importance in the past few years due to the increasing need for providing secrecy in an open environment like the internet. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. Steganography has many technical challenges such as high hiding* ***capacity and imperceptibility****. In this paper, we try to optimize these two main requirements by proposing a novel technique for hiding data in digital images by combining the use of adaptive hiding capacity function that hides secret data in the integer wavelet coefficients of the cover image with the* ***optimum pixel adjustment (OPA) algorithm****. The proposed system showed high hiding rates with reasonable imperceptibility compared to other steganography system.*

I. Introduction

1.1 Overview

Steganography is anart andscience of information hidingand invisiblecommunication.It'sunlike cryptography, wherethe goal is tosecure communications from an eavesdropper by make the datanot understood, steganographytechniquesstriveto hidetheverypresenceofthemessageitself from an observersothereisnoknowledgeoftheexistenceof the message in the first place. In somesituations, sendingencryptedinformation will arouse suspicion while invisible informationwillnotdoso. Both sciencescanbecombinedtoproducebetterprotection ofthe information. Inthiscase, whenthesteganography failsandthemessagecannot bedetectedifa cryptographytechnique isused.Hidinginformation insideimagesisapopular techniquenowadays.An imagewitha secretmessage insidecaneasilybespread overthe WorldWideWeb or ina newsgroups.

To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many color variations, so less attention will be drawn to the modification. The most common methods to make these alterations involve the usage of the least-significant (LSB). Thenext interesting application of steganography, in whichthecontentisencryptedwithonekey andcanbe decryptedwithseveral other keys,therelativeentropy betweenencryptandone specificdecryptkey corresponds to the amount of information.

When usinga 24bitcolourimage,each bit ofred, greenand bluecolourcomponentscanbeused, soatotalof3bitscanbestoredineachpixel.Thus,800×600pixelimagecancontainatotalamountof 1.440.000 bits (180.000 bytes)ofsecret data.But using just3 bitfrom thishugesize of bytesiswastinginsize. Sothe main objective ofthe present work is howto insertmorethanone bitateachbytein one pixelofthe cover-imageandgive usresultsliketheLSB(message to be imperceptible).This objective is satisfied by building new steganography algorithm to hidelargeamountofany typeofinformationthrough JPGimagebyusingmaximumnumberofbits perbyteateachpixel.

Digital multimedia data provides a robust and easy editing and modifying of data. The data can be delivered over computer networks with little to no errors and often without interference. Unfortunately, digital media distribution raises a concern for digital content owners. Digital data can be copied without any loss in quality and content. This poses a big problem for the protection of intellectual property rights of copyright owners. Watermarking is a solution to the problem. It can be defined as embedding digital data, such as information about the owner, recipient, and access level, without being detectable in the host multimedia data.

Steganography relies on hiding covert message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties. Steganography is a method of encryption that hides data among the bits of a cover file, such as a graphic or an audio file. The technique replaces unused or insignificant bits with the secret data. Steganography is not as robust to attacks since the embedded data is vulnerable to destruction.

1.2 Different Kinds Of Steganography:

The four main categories of file formats that can be used for steganography are:

1. Text
2. Images
3. Audio
4. Protocol

II. Existing Method

2.1 Introduction

Cryptography has followed man through many stages of evolution. Ancient Egyptian scribe used non-standard hieroglyphics in an inscription. Hebrew scribes used ATBASH, a reversed alphabet simple solution cipher.

Cryptography continued through history with many variations. Today cryptography has reached a new level, quantum cryptography. Quantum cryptography combines physics and cryptography to produce a new cryptosystem that cannot be defeated without the sender and receiver having the knowledge of the attempted and failed intrusion.

2.2 Definition & Terminology

Cryptography defines the art and science of transforming data into a sequence of bits that appears as random and meaningless to a side observer or attacker.

Cryptanalysis is the reverse engineering of cryptography attempts to identify weaknesses of various cryptographic algorithms and their implementations to exploit them. Any attempt at cryptanalysis is defined as an attack.

Cryptology encompasses both cryptography and cryptanalysis and looks at mathematical problems that underlie them. Cryptosystems are computer systems used to encrypt data for secure transmission and storage. Plaintext is message or data which are in their normal, readable (not crypted) form.

Encryption:

Encoding the contents of the message in such a way that hides its contents from outsiders. Cipher text results from plaintext by applying the encryption key.

Decryption:

The process of retrieving the plaintext back from the cipher text.

Key:

Encryption and decryption usually make use of a key, and the coding method is such that decryption can be performed only by knowing the proper key. Hash functions generate a digest of the message.

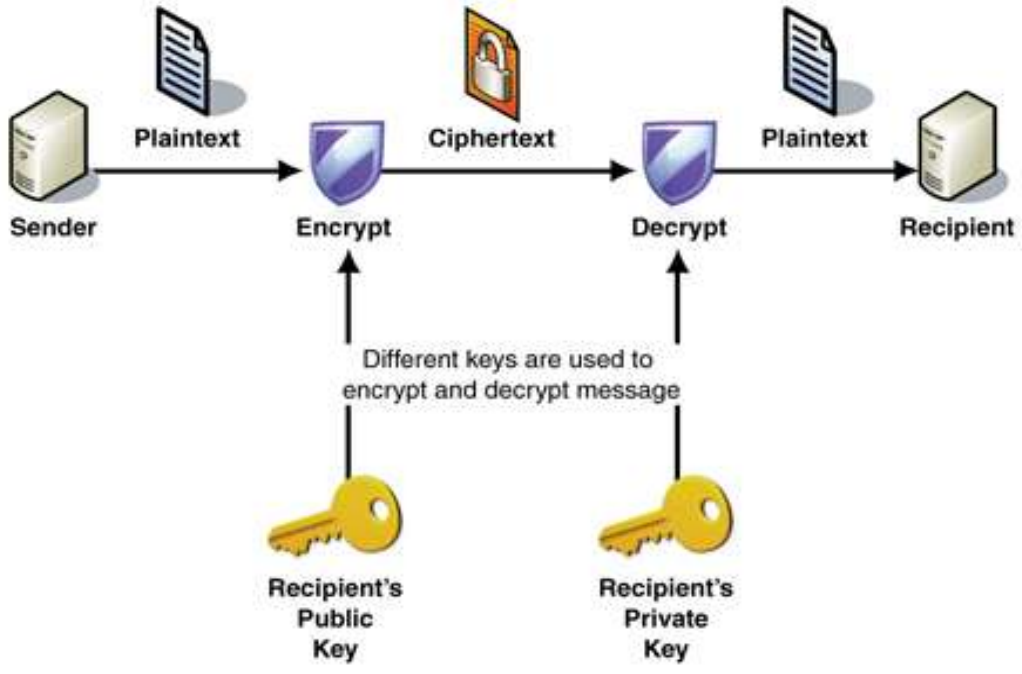


FIG:2.2.1 Encryption and decryption process

Substitution cipher involves replacing an alphabet with another character of the same alphabet set. Mono-alphabetic system uses a single alphabetic set for substitutions. Poly-alphabetic system uses multiple alphabetic sets for substitutions.

2.3 Cryptography

Cryptography is an important element of any strategy to address message transmission security requirements. Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is the practical art of converting messages or data into a different form, such that no-one can read them without having access to the 'key'.

The message may be converted using a 'code' (in which case each character or group of characters is substituted by an alternative one), or a 'cypher' or 'cipher' (in which case the message as a whole is converted, rather than individual characters).Cryptology is the science underlying cryptography.

1. Methodology for transforming plain text to cipher text.

All encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.

2. Methodology for number of keys used.

There are some standards methods[1] which is used with cryptography such as secret key, public key and hash function.

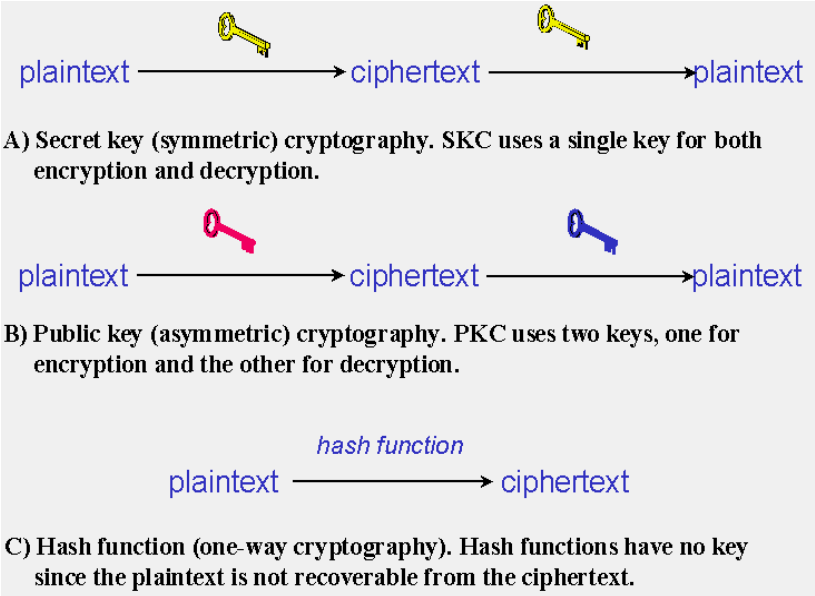


Figure 24.1 :Three types of cryptography: secret key,publickey,hash function.

2.4 Difference Between Cryptography And Stegnography

CRYPTOGRAPHY	STEGNOGRAPHY
The encrypted letter could be seen by anyone but cryptography make the message not understandable.	Stegnography is hiding the message in another median so that nobody will notice the message.
The end result in cryptography is the cipher text.	The end result of information hiding is the stego-medium.
The goal of a secure cryptography is to prevent an cryptographic is to prevent an intercepter from gaining any information about the plaintext from the interchanged ciphertext.	The goal of secure stegnography methods is to prevent an observant intermediary from even obtaining knowledge of the mere presence of the secret data.
Any person has the ability of detecting and modifying the encrypted message.	The hidden message is imperceptiable to anyone.
Steganography cannot be used to adapt the robustness of cryptographic system.	Stegnaography can be used in conjuction with cryptography by hidng encrypted message.
Cryptography alter the structure of the secret message.	Stegnography does not alter the structre of the secret message.

Table2.6.1 Difference between crytography and stegnograp

III. Detailed Decription Of The Proposed System

3.1 Overview

Hiding the information within an image is most common procedure used at present. Through the internet secret messages canbe spread easily by inserting the secret message in an image.To conceal a message inside an image without altering its visible properties, "noisy" areas which have color changes can be changed for the cover image .The general technique used to make the changes engaged is the usage of the Least-Significant Bit (LSB), masking, filtering and transformations on the cover image

The main aim of the project is to insert more than one bit at each byte in one pixel of the cover-image and obtain the results like the LSB. This aim can be reached by developing a Steganography algorithm to hide large amount of any type of information through JPG image by using maximum number of bits per byte at each pixel. Any type of data can be hidden in a JPG image which has 24- bits by using the Steganography algorithm. The 24 bits has three bytes of RGB colors, each byte has four bits called as Nibbles. The highest value is stored in the left nibble and the lowest value is contained in the right nibble in a byte [1, 2].

3.2 Steganography Algorithm

Steganographyis the art of hiding the existence of data in another transmission medium to achieve secret communication.

It provides invisible communication .In the present steganography algorithm, two part (data hiding at the sender side and at extracting the receiver side)

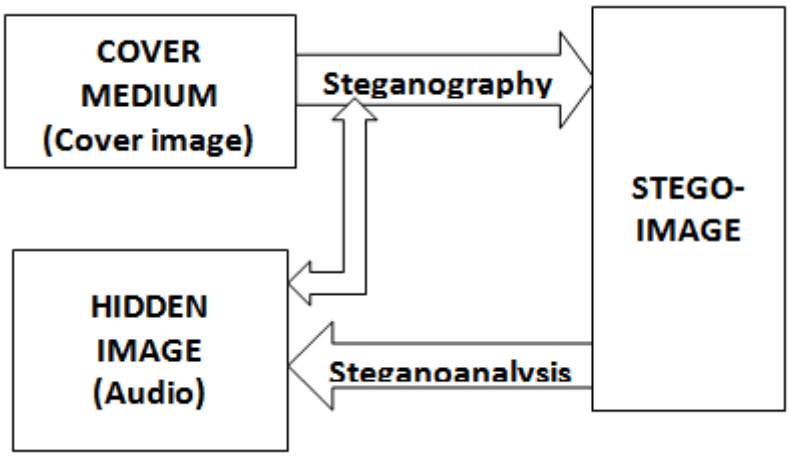


Figure 3.1 (Steganography and steganoanalysis model)

3.2.1characteristics:

Though steganography is most obvious goal is to hide data, there are several other related goals used to judge a method's steganographic strength. These include;

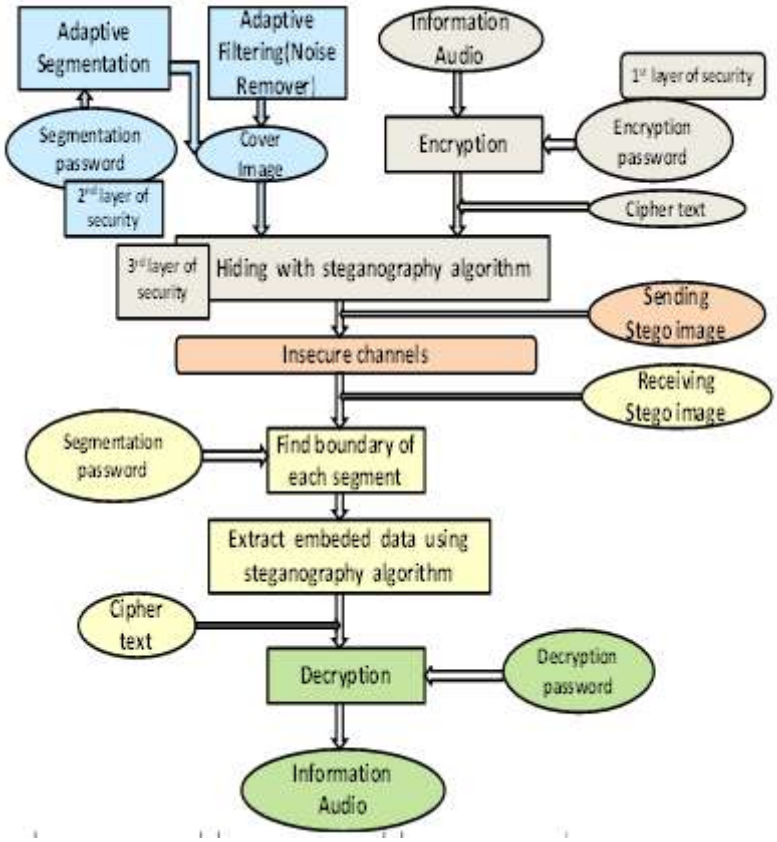
1. Capacity (how much data can be hidden)
2. Invisibility (inability for humans to detect a distortion in the stego-object)
3. Undetectability (inability for a computer to use statistics or other computational methods to differentiate between covers and stego-objects)
4. Robustness (message's ability to persist despite compression or other common modifications)
5. Tamper resistance (message's ability to persist despite active measures to destroy it)
6. Signal to noise ratio (how much data is encoded versus how much unrelated data is encoded).

3.3 Architecture Of Stegnography

Block Diagram for the Steganography Algorithm

1. Data hiding
2. Data extraction.

3.3.1architecture Of Stegnography



3.4 Embedding Process:

The embedding process is concerned with hiding a secret message within a cover Work, and is the most carefully constructed process of the two. A great deal of attention is paid to ensuring that the secret message goes unnoticed if third party were to intercept the cover Work. The extracting process is traditionally a much simpler process as it is simply an inverse of the embedding process, where the secret message is revealed at the end**.**

inputs are required for the embedding process:

1. Secret message - audio file that contains the message you want to transfer
2. Cover Work - used to construct a stegogramme that contains a secret message

3.4.1 Image Type:

Indexed images : m-by-3 color map
Intensity images : [0,1] or uint8
Binary images : {0,1}
RGB images : m-by-n-by-3

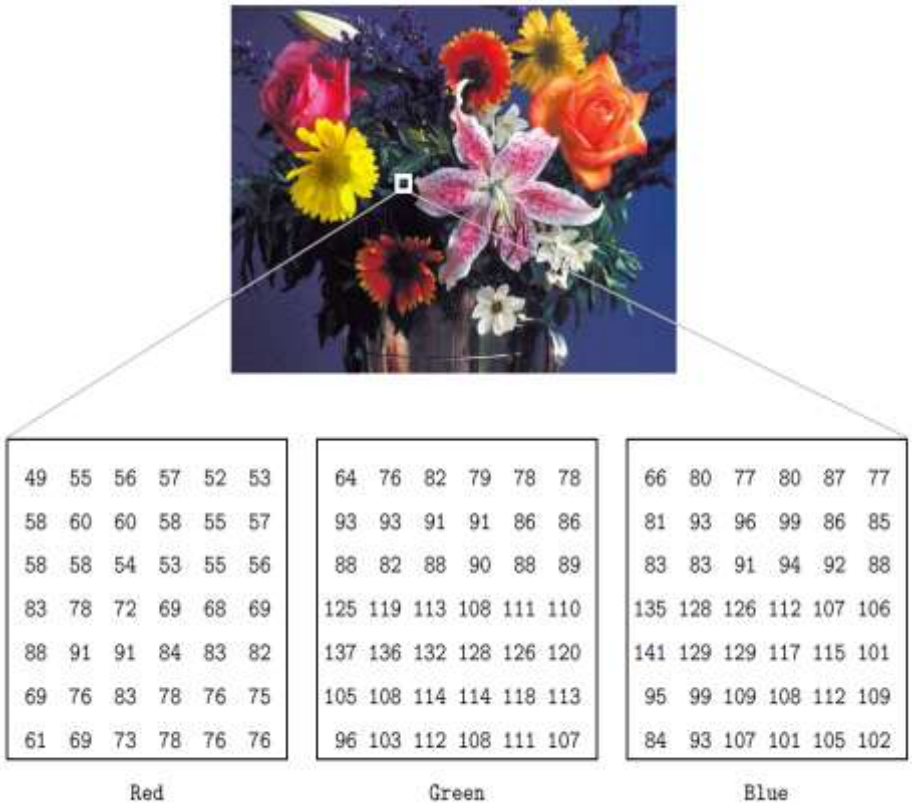


Figure 3.6

Digital image processing, involves using a computer to change the nature of a digital image. It is necessary to realize that these two aspects represent two separate but equally important aspects of image processing. A procedure which satisfies,

- Condition1 : A procedure which makes an image ”look better” may be the very worst procedure for satisfying
- Condition 2 :Humans like their images to be sharp, clear and detailed; machines prefer their images to be simple and uncluttered.

3.4.2 Adaptive Segmentation:

Color image segmentation its very interesting and intensive topic in image processing .This can viewed as a extension of gray level image segmentation ,there are various methods which can be categorized they are:

1. Cluster based segmentation
2. Contour detection based segmentation
3. Area extraction based segmentation
4. Probabilistic models based segmentation

Fig. 3: Original "flower" image.

1.

(a) (b)

Fig. 4: (a) Segmentation result of [7] (5 colors). (b) The Segmentation using the proposed method (5 colors).

Fig 3.7 Adaptive segmentation

3.5 Encryptionprocess :

3.5.1 Advanced Encryption Standard

Advanced Encryption Standard (AES) is implemented using MATLAB. Data Encryption Standard (DES) is used to implement cryptographic techniques since long time, AES is the advanced technology development for DES which is based on block cipher. MATLAB is a Matrix-oriented programming language, which can be absolutely used for the matrix-based Data- Structure of AES. This can be used for encryption of randomly chosen plain text to chipper text.

3.5.2 Mathematical Representation Of Data:

3.5.2.1 Arthmetics Of Finite Field:

A byte can be represented in different forms. A finite field has basic arithmetic's which are illustrated below. A finite field can also be named as Galois Field, which consist finitely many elements .The finite field GF(24) consists of the 24=16 with different numbers ranging from (0…16) which represents 4 bits. Special XOR and modulo-operations are used to check whether the sum and product of two finite field elements are in the similar range of the same finite field.

3.5.2.2 DIFFERENT FORMS OF BYTE REPRESENTATION:

There are four ways of representation of a finite field element. They are binary representation, decimal representation, hexa-decimal representation, polynomial representation.

3.5.2.3 POLYNOMIAL REPRESENTATION:

A byte can be represented as a polynomial it is same as converting from binary to decimal. Every digit is multiplied by x to the corresponding coefficients.

1.x7+0.x6+0.x5+1.x4+0.x3+1.x2+0.x1+0.x0= x7+x4

It is important to note that the polynomials can only be 1's or 0's accordingly.

3.6.1 Implementation Of Present Algorithm :

Assume that we have a cover-image which contains three types of MC: MC1, MC2 and MC6 and we have three types of pixels: MC1 with SC3, MC2 with SC5 and MC6 with SC1. Now, we try to hide 2- bytes 01010101, 01010101. Before we perform hiding, we must compute the number of segments in the Cover-image through the followingsteps:

1. Let L be a number of characters in the input password (PS).
2. Find N=round(L/2)
3. Find a number of segments on the vertical and horizontal directions (Segv , Segh) by using the following formulas:

$$Segv = \sum_{i=1}^{N} Val(PS_i)$$

$$Segh = \sum_{i=N+1}^{2N} Val(PS_i)$$

- where, Val(PSi) represents the value of the ith character at the PS.

4. Find the size of non-uniform segments on both directions.
5. Perform segmentation by using column wise indexing on the cover-image into (Segv xSegh) segments through non-uniform size of segments. The present algorithm performs hiding into each segment separately according to row wise scanning.

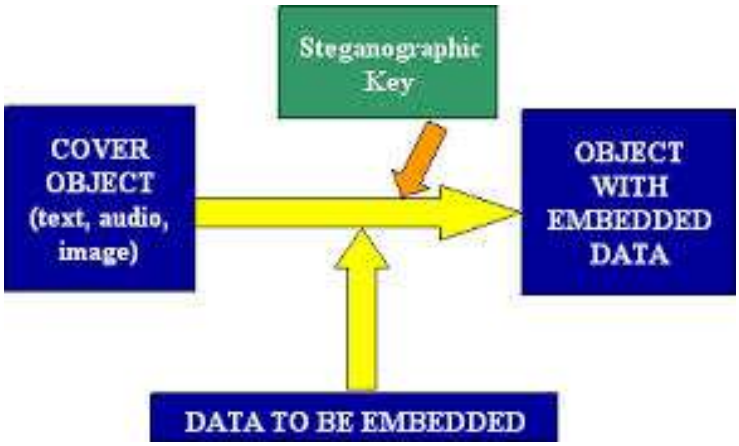


Figure 3.8

3.7 Security Requirements :

- New Steganography algorithm by using three layers of security has been constructed. These layers are developed from previous works to acquire high security and they work independently to provide unbreakable security wall .
- Encryption mechanism
- Adaptive segmentation of the cover-image
- Pixel selection style

3.6 Extraction Process:

1. The password given for encryption.
2. The pixels are scanned based on password.
3. The data is extracted.
4. The extracted data is decrypted based on password.

3.8.1encryption Password:

The password does not get embedded in the image, usually. Instead, the password is used to influence how the hidden information is to be written. Then when the end user wants to extract the hidden information, they must supply the password and the password is used to influence how the hidden information gets read back. If they did not supply the right password, the information retrieved will not look correct. If we put in enough error detection coding, you can detect with relatively high probability whether the data was retrieved correctly. Then cover image save message as the stego file. It will do the same when user want to extracting message from stego image: user needs to input the correct password.

3.8.2 Scanning :

A scanning pattern is the pattern or order in which the pixels are accessed to embed data. Instead embedding the first k bits in first pixel, second k bits in second pixel and so on, the data bits are embedded in a pseudo-random order.

We use three scan methods Raster scan method, snake scan, and Z scan method each in both horizontal and vertical embedding schemes.

In Raster horizontal scanning method, the secret data is embedded in a row wise manner. After embedding data in a row, the next row is scanned starting from the first pixel.

In Raster vertical the scanning is done vertically, in a column wise manner.

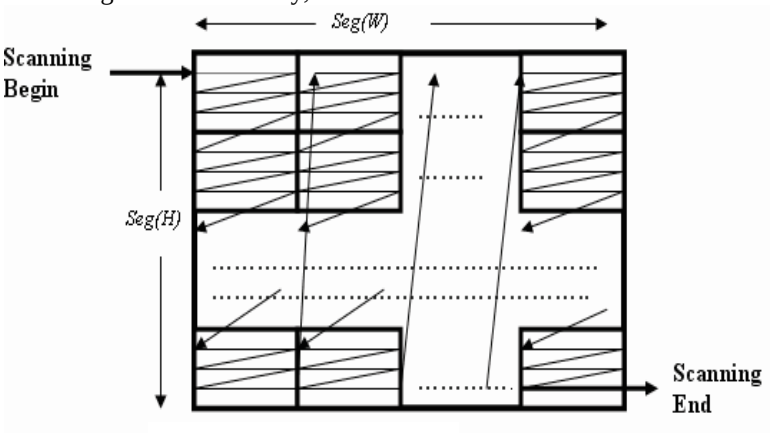


Figure 3.9

3.8.3 Extracted Segment:

1. Specify a name for the file to contain the extracted data.
2. Select the image file within which the data is hidden.
3. Specify the stego key.

3.8.4 Decryption Output :

The activity of making clear or converting from code into plain text; "a secret key or password is required for decryption".Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

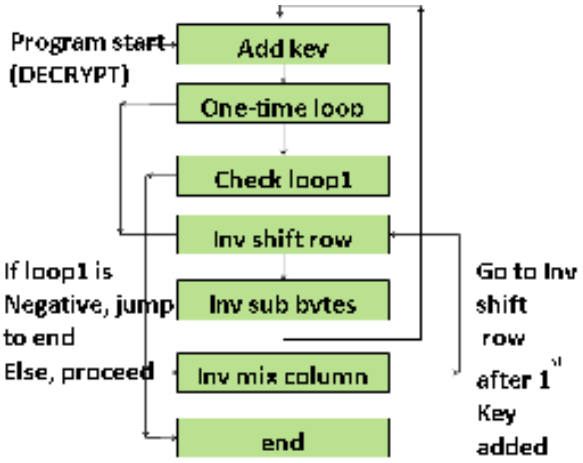


Figure:3.10 (AES Algorithm)

IV. Conclusion

The proposed method modifies the amplitude of the cover image file to embed the secret message. To increase the security of the proposed scheme, we use a key to adjust the hiding technique. The experiment shows that our method is secure, imperceptible and can be used for hiding data in the image file. In the future research, we plan to use the error correction code to increase the robustness of this scheme.

At the end, feasibility of image Steganography was evaluated by considering it's the pros and cons. In summary, if implemented correctly and in conjunction with cryptographic methods to secure the embedded data before insertion to a cover medium, many of the data hiding methods described above could become powerful tools for the transmission of undetectable and secure communication.

References

[1]. R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
[2]. Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003.
[3]. K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images",Technical Report, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,Bangalore University, December 2004.
[4]. An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.
[5]. Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen", Computer Journal, February 1998.
[6]. "Detecting LSB Steganography in Color and Gray-Scale Images" Jessica Fridrich, Miroslav Goljan, and Rui Du State University of New York, Binghamton.
[7]. Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, "Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Lett. 36 (25) (2000) 20692070.
[8]. Hiding data in images by simple LSB substitution by Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.
[9]. "A Tutorial Review on Steganography" by Samir K Bandyopadhyay, DebnathBhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.
[10]. International Journal of Computer Science Engineering Technology (IJC-SET) "ModernSteganographic technique: A Survey" by Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology .
[11]. A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). "Digital image steganography: survey and analysis of current methods." Signal Processing Journal.
[12]. P. Kruus, C. Scace,M.Heyman, and M. Mundy.(2003), "A survey of steganography techniques for image files." Advanced Security Research Journal.
[13]. A Review of Data Hiding in Digital Images by E Lin, E Delp Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, IN 47907-2086.