ISSN:0975-9646
Sneha A. Deshmukh et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2409-2414

An Authentication of Secretely Encrypted Message Using Half-Tone Pixel Swapping From Carrier Stego Image

Sneha A. Deshmukh[1] , P.B.Sambhare[2]

[1]*Student ME 2nd CSE P.R.Pote(Patil) College of Engineering & Management ,Amravati.*
[2] *Assistant Professor P.R.Pote(Patil) College of Engineering & Management ,Amravati*

Abstract- Many techniques are used to hide data in various formats in steganography. The most widely used mechanism on account of its simplicity is the use of the Least Significant Bit. Least Significant Bit or its variants are normally used to hide data in a digital image. Using steganography alone with simple LSB has a potential problem that the secret message is easily detectable from the histogram analysis method. To improve the security as well as the image embedding capacity we are using Steganography with Half-Tone Pixel Swapping.

Keywords- Higher LSB, Stegnography, Multi- carrier, Information hiding,Data Encryption.

1.INTRODUCTION

Information Hiding [1] techniques have been receiving much attention today. The main motivation for this over encryption and decryption is that here the information is imperceptibly hidden and therefore does not attract attention. This art of hiding information is known as Steganography.

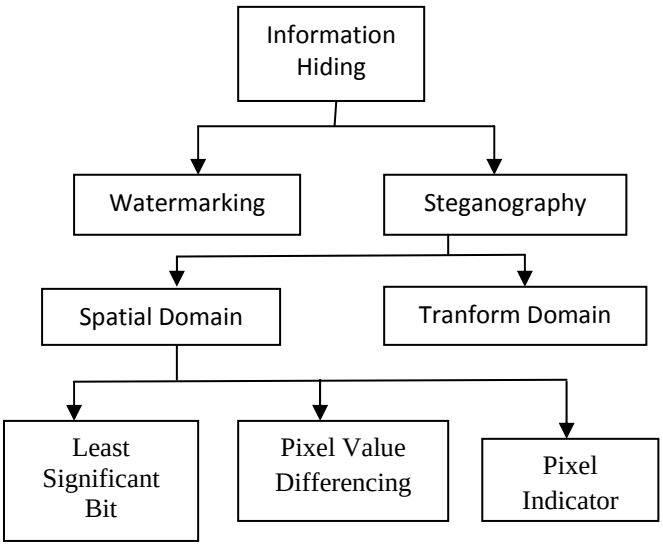


Fig: Information Hiding Technique

Steganography [2] is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message. One of the other main uses for Image Steganography is for the transportation of high-level or top-secret documents between international Governments. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another".

Steganography[3] can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav, mainly because of their popularity on the Internet and the ease of use of the steganographic tools that use these data formats. These formats are also popular because of the relative ease by which redundant or noisy data can be removed from them and replaced with a hidden message.
The main goal of visual secret sharing [4] scheme is to protect important secret data, from being lost or destroyed without accidental exposure. The protection of participants is not the main concern but security of data is important factor. Since there is no restriction on the behavior of the participants, any participant, called a cheater, who can reveal a fake share on purpose. Of course, cheaters may collude in an attempt to increase their profits. In 2006, Horng et al. showed that cheating is possible in a k-out-of-n visual secret-sharing scheme . So, designing cheating-prevention visual secret- sharing (CPVSS) schemes has been proposed by many researchers to overcome cheating problem from existing VC.

Cryptography [5] focuses on keeping the content of the message secret whereas data hiding concentrates on keeping the existence of the message secret . Data hiding[10] is the other technique for secured communication. Data hiding involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Data hiding is the process of hiding a secret message within cover medium such as image, video, text, audio. Hidden image has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the

internet. Hidden image allows for two parties to communicate secretly and covertly.

The strength of data hiding [4] gets amplified if it combines with cryptography. The terminologies used in data hiding are cover-image, hidden image, secret message, secret key and embedding algorithm. Cover-image is the carrier of the message such as image, video or audio file. Cover- image carrying the embedded secret data is the hidden image. Secret message is the information that is to be hidden in a cover image. The secret key is used to embed the message depending on the hiding algorithm . The embedding algorithm is the way, which is used to embed the secret information in the cover image.

The security of the transformation of hidden data can be obtained by two ways: encryption and data hiding. A combination of the two techniques can be used to increase the data security. In encryption, the message is changed in such a way so that no data can be disclosed if it is received by an attacker. Whereas in Data hiding, the secret message is embedded into an image often called cover image, and then sent to the receiver who extracts the secret message from the cover message. When the secret message is embedded into cover image then it is called a hidden image. The visibility of this image should not be distinguishable from the cover image, so that it almost becomes impossible for the attacker to discover any embedded message.

Cryptography [6] is a technique for securing the secret information. Sender encrypts the message using the secret key and then sends it to the receiver. The receiver decrypts the message to get the secret information. Cryptography focuses on keeping the content of the message secret where as data hiding concentrates on keeping the existence of the message secret [1]. Data hiding is the other technique for secured communication. Data hiding involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information [2]. Data hiding is the process of hiding a secret message within cover medium such as image, video, text, audio. Hidden image has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Hidden image allows for two parties to communicate secretly and covertly.

2. LITERATURE REVIEW

Tung-Hsiang Liu and Long-Wen Chang [7] Proposed data hiding technique for binary images in 2004. The proposed method embeds secure data at the edge portion of host binary image. We find the best changeable pixels in a block by changing distance matrix dynamically and compute its changeable score by weighting mechanism. The proposed method uses the pseudo random number generator based on Rabin Public Key Cryptography System to embed secret data into a binary image. According to the pseudo random number generator, we can distribute secret data into the binary image to make binary image quality better and get high security.

H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang [8] In order to improve the capacity of the hidden secret data and to provide an imperceptible stego-image quality, a novel steganographic method based on least-significant-bit (LSB) replacement and pixel-value differencing (PVD) method is presented. First, a different value from two consecutive pixels by utilising the PVD method is obtained. A small difference value can be located on a smooth area and the large one is located on an edged area. In the smooth areas, the secret data is hidden into the cover image by LSB method while using the PVD method in the edged areas. Because the range width is variable, and the area in which the secret data is concealed by LSB or PVD method are hard to guess, the security level is the same as that of a single using the PVD method of the proposed method. From the experimental results, compared with the PVD method being used alone, the proposed method can hide a much larger information and maintains a good visual quality of stego-image.

Beenish Mehboob and Rashid Aziz Faruqui [9] Many techniques are used to hide data in various formats in steganography. The most widely used mechanism on account of its simplicity is the use of the Least Significant Bit. Least Significant Bit or its variants are normally used to hide data in a digital image. The other bits may be used but it is highly likely that image would be distorted. This paper discusses the art and science of Steganography in general and proposes a novel technique to hide data in a colorful image using least significant bit.

M.B. Ould MEDENI M.B. Ould MEDENI [10] propose a novel steganographic method for hiding information within the spatial domain of the gray scale image. The proposed approach works by dividing the cover into blocks of equal sizes and then embeds the message in the edge of the block depending on the number of ones in left four bits of the pixel. Our experimental results have shown that the proposed method not only has an acceptable image quality but also provides a large embedding capacity. Our results are compared with the PVD method , and the values obtained are better than the PVD method.

Tasnuva Mahjabin [11] Information hiding is a historical but on demand fascinating research area. Now, in today's world, the availability of information has become so easy that the security and insecurity of information goes side by side. In order to provide security of information a science called, Steganography has emerged. Steganography conceals the existence of information into images to formulate a secure communication. In this paper, a Steganographic method based on Pixel Value Differencing (PVD) and LSB Substitution method is proposed. To meet the increasing demand for privacy and secrecy the method focused mainly on making it a robust, secured technique of information hiding. An efficient and dynamic embedding

algorithm is proposed in this paper that not only hides the secret data with an imperceptible visual quality and increased capacity but also make secret code breaking a good annoyance for the attacker. This method also represents an extraction algorithm that effectively extracts the entire secret message without any loss of a single data.
Ming Li,Michel K. Kulhandjian, Dimitris,A. Pados,,Stella N. Batalama, and Michael J. Medley[12] We consider the problem of extracting blindly data embedded over a wide band in a spectrum (transform) domain of a digitalmedium (image, audio, video).We develop a novelmulticarrier/ signature iterative generalized least-squares (M-IGLS) core procedure to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. Neither the original host nor the embedding carriers are assumed available. Experimental studies on images show that the developed algorithm can achieve recovery probability of error close to what may be attained with known embedding carriers and host autocorrelation matrix.

In 2012, Shuo-Fang Hsu et al [13] were first researchers to present Verifiable Visual Cryptography scheme. This scheme provides a verifiable visual cryptography (VC) technique for checking the validness to the shares available in a VC decoding instance. Compare to the reported cheating prevention VC schemes, the verifiable visual cryptography scheme maintains the original pixel expansion in VC scheme without cheating prevention ability. The basic idea used in this scheme is to stamp a continuous pattern on the shares belonging to the same secret image. Also a part of the pattern can be revealed through aligning and stacking half of two share images together. Basically, the visual coherent among the revealed patterns of all pair of share images provides evidence to the genuine of the shares engaged in the decoding process. In this scheme the share verification process is done without resorting to any additional verification image. In addition to this, the proposed verification mechanism can easily be attached to any VC schemes in the literature to endow legitimate user with the ability to prevent cheating from malicious participants in secret sharing mechanism.

In 2014, Jana B. et al [14] were first researchers to advise the Cheating prevention in Visual Cryptographic Schemes using message embedding. This scheme attempts to give a hardware based practical overview about cheating prevention of information hiding technique using Steganography and Visual Cryptographic Schemes (VCS). A combined technique has been proposed here, which allows visual information like printed text, handwritten notes, and images etc. to be distributed into 'n' secret shares as transparencies and embedding message into share became stego share for share authentication. In this scheme finally each of these stego shares embeds into a cover image using hardware module. At the time of recovering secret image the receiver first decode each stego shares from the cover work and then extract secret message from share to prevent cheating. The original secret image can be retrieve by overlapping the share images. They proposed encoding and decoding scheme for share generation is implemented in software module and embedding of message into share images and stego share into cover image are implemented in hardware-based system for 2-D images.

Many studies focused on the cheating problems in VCS, and consequently many cheating immune visual cryptography schemes (CIVCS) have been proposed. The classified techniques proposed in these CIVCSs as follows:

1. Make use of an online trusted authority who can verify the validity of the stacked shares.
2. Generate extra verification shares to verify the validity of the stacked shares.
3. Expand the pixel expansion of the scheme to embed extra authentication information.
4. Generate more than n shares to reduce the possibility that the cheaters can correctly guess the distribution of the victims' shares.
5. Make use of the genetic algorithm to encrypt homogeneous secret images.

In 2010, Bin YU. et al [15] were researchers to advise the Co Cheating prevention in Visual Cryptographic Schemes using trusty third party as the verifier and extra verification shares. Based on a trusty third party, a co-cheating prevention visual cryptography scheme (CCPVCS) is proposed and evaluated with extra verification shares. Also checking efficiency is improved by verifying the truth of several shares simultaneously, with designed special verification shares. Since the scheme idea is different from previous ones, the pixel expansion is small and the recovered secret image is good for viewing. By introducing a trusty third party as the verifier, the CCPVCS could prevent co-cheating through verifying the truth of several shares simultaneously.

3.PROPOSED METHODOLOGY

Steps for data hiding

1. Select Input Carrier Image
2. Select Second Level Carrier Image
3. Crop an image
4. Select Feature Extraction
5. Split an Image into multi carrier objects
6. Select Strong (Max) 4 Features
7. Select Secrete Data and apply Encryption on that for Hiding
8. Split Data into 4 Segments
9. Select Hide Data & Data can be hided into an Image
10. Select Pixel Swapping for encrypted Stego Image
11. Select Extract Features(Second Level Carrier Image)
12. Split Image into 4 Segments
13. Select Data Hiding Menu & Hide Stego Encrypted Share into each of the Segments from Second Level Carrier Image
14. Join Multi Carriers Objects to create single Image
15. Stop.

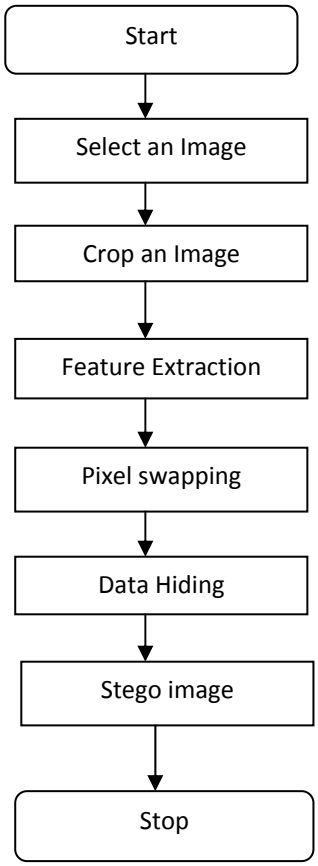


Fig: Data Hiding

Algorithm for Data Hiding

1. Input Image
2. Select Secrete Data
3. Convert Carrier Image & Secrete Data into Binary
4. Sample Binary Secrete Data
5. For i=1 to length (Binary Sample)
   Hide[(R,G,B),Sample(Data)]
   End
6. Save Stego image
7. Stop

Steps for data extraction

1. Select Stego Image
2. Split Stego Imega
3. Select Data Extraction(with password 9600,20,20) using Higher LSB Data Extraction Algorithm
4. Select Decode Secrete Share
5. Select Length Key
6. Extract Data from Stego Image
7. Select Assemble Data
8. Select Decode Extracted Data
9. Use Password & Encryption Algorithm to Decode Text
10. Decrypt Data
11. Stop.

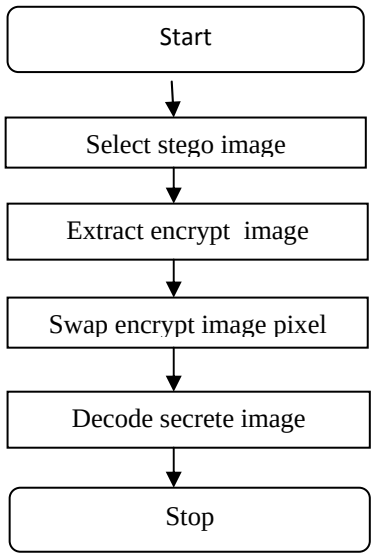


Fig: Data Extraction

Algorithm for Data Extraction

1. Input Stego Image
2. Extract Secrete Data
3. Convert Stego Image & Secrete Data into Binary
4. Sample Binary Secrete Data
5. For i=1 to length (Binary Sample)
   Extract (5 Bits from L,S,B)
   End
6. Save image
7. Stop

The below given diagram shows the red,green,blue color showing the msb & lsb side.

Fig: Showing Red, Green, Blue color with MSB & LSB side

In the proposed method we are going to replece 5-bit of LSB with secrete data as given in the below

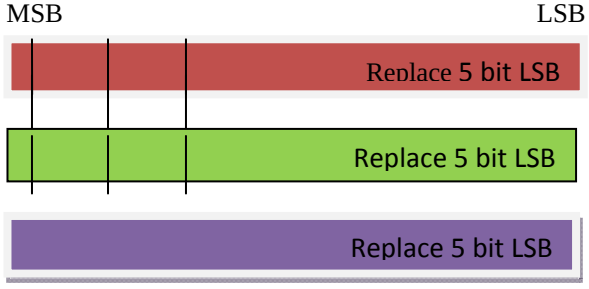
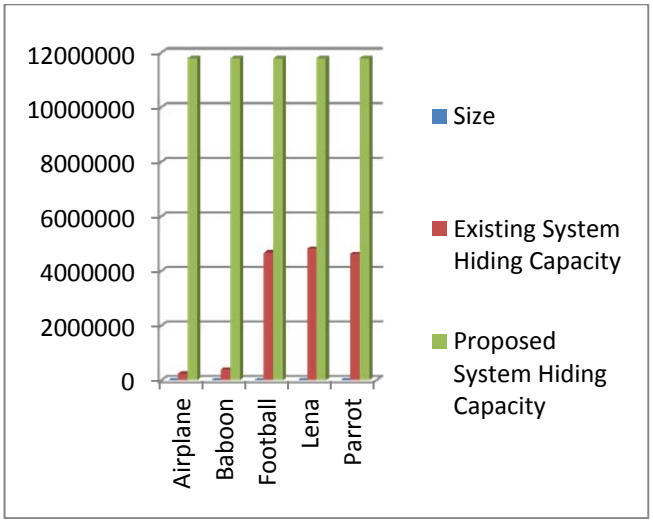


Fig:Replacement of 5 bit from LSB side

Table: Hiding Capacity Comparison with Existing System

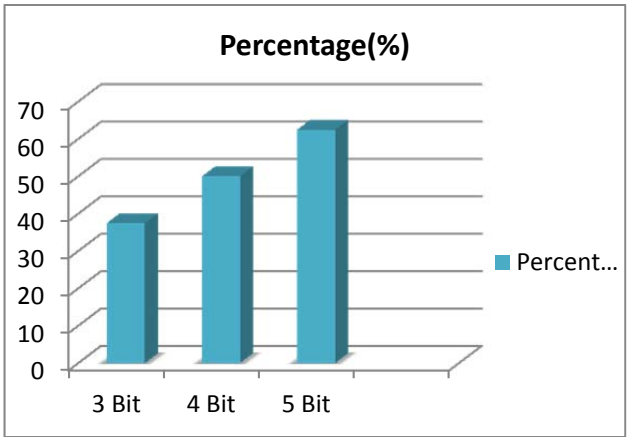
Image	Size	Existing System Hiding Capacity	Proposed System Hiding Capacity
Airplane	512*512	249608	11796480
Baboon	512*512	396496	11796480
Football	512*512	4675856	11796480
Lena	512*512	4815936	11796480
Parrot	512*512	4625160	11796480



Graph: Hiding Capacity Comparison with Existing System

Table: Hiding Capacity in percentage

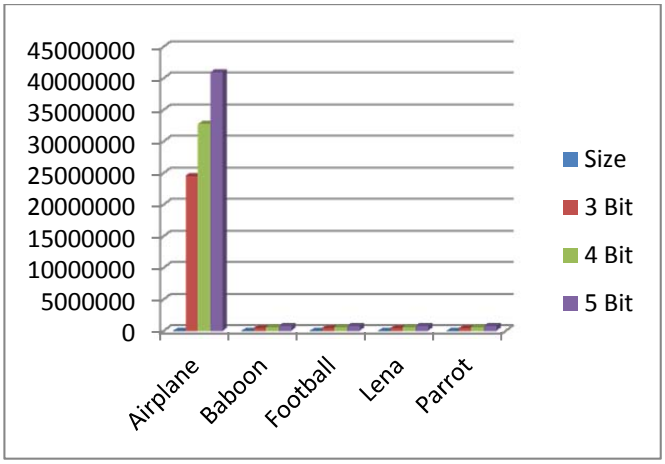
Bit	Percentage(%)
3 bit	37.50
4 bit	50.00
5 bit	62.5



Graph: Hiding Capacity in percentage

Table : Hiding Capacity of different bit

Image	size	3 bit	4 bit	5 bit
Airplane	2022*1349	24549102	32732136	40915170
Baboon	257*196	453348	604464	755580
Football	259*194	452214	602952	753690
Lena	225*225	455625	607500	759375
Parrot	275*183	452925	603900	754875



Graph: Hiding Capacity of different bit

4. CONCLUSION

It is conclude that the Steganography scheme is used for better transmission of data. This paper used that, data is hidden in RGB component of pixels with LSB 5 bit Replacement..A secured LSB (5 bit) for image steganography has been presented in this paper. The experimental results demonstrate that the proposed method not only has an acceptable image quality but also can provide a large embedded secrete data capacity.

REFERENCE

[1] Ms. Archana A. Athawale "Information Hiding in Image and Audio Files". SVKM's NMIMS University Vile Parle (W), Mumbai-56 ,2010.

[2] Ravi Kumar. B #1, Murti. P.R.K.*2 ,"Data Security and Authentication Using Steganography" 1,2 Department of Computer and Information Sciences, University of Hyderabad, (P.O) Central University, Gachibowli, Hyderabad 500046, India.

[3] Images With four-pixel Differencing and LSB Substitution "IEEE 2010

[4] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012

[5] Moni Naor, Adi Shamir" Visual Cryptography".

[6] Smita Patil1, Jyoti Rao2" Survey of Cheating Prevention Techniques in Visual Cryptography" Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri, Pune-18, India.

[7] Tung-Hsiang Liu and Long-Wen Chang, "An Adaptive Data Hiding Technique for Binary Images", Proc.IEEE 17th Int.Conf. On Pattern Recognition (ICPR'04) 2004.

[8] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.

[9] Beenish Mehboob and Rashid Aziz Faruqui," A stegnographyimplementation", IEEE 2008

[10] M.B. Ould MEDENI, El Mamoun SOUIDI," A Novel Steganographic Method for Gray-Level Images With four-pixel Differencing and LSB Substitution "IEEE 2010

[11] Tasnuva Mahjabin, Syed Monowar Hossain, Md. Shariful Haque," A Block Based Data Hiding Method in Images Using Pixel Value Differencing and LSB Substitution Method", IEEE 2012.

[12] Ming Li, Michel K. Kulhandjian, Dimitris A. Pados, Stella N. Batalama, and Michael J. Medley," Extracting Spread-Spectrum Hidden Data From Digital Media", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013.

[13] Shuo-Fang Hsu ; Yu-Jie Chang ; Ran-Zan Wang ; Yeuan-Kuen Lee ; Shih-Yu Huang, "Verifiable Visual Cryptography" Sixth International Conference on Genetic and Evolutionary Computing (ICGEC), 2012, 464 – 467

[14] Jana, B. ; Mondal, S.K. ; Jana, S. ; Giri, D., "Cheating prevention in Visual Cryptographic Schemes using message embedding: A hardware based practical approach" International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014, 319 – 324

[15] Bin YU, Jin-Yuan LU, Li-Guo FANG," A Co-cheating Prevention Visual Cryptography Scheme", Third International Conference on Information and Computing, 2010.