International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

New Approach for Image Hiding By Using Block Transformation

Khushboo Dhoke[1], Shubhangi Dhengre[2]

[1]Electronics and Communication Department/ Abha Gaikwad Patil College of Engineering/ Nagpur University, India

[2]Professor, Electronics and Communication Department/ Abha Gaikwad Patil College of Engineering/ Nagpur University, India

Abstract: ***The network provides a method of communication to distribute information to the multitude. With the growth of data communication over computer network, the security of information has become a major issue. Cryptography and steganography are two different data hiding techniques. The science of securing a data by encryption is Cryptography whereas the method of hiding secret messages in other messages is Steganography, so that the secret's very existence is hidden. The term 'Steganography' describes the method of hiding cognitive content in another medium to avoid detection by the intruders. Steganography hides messages inside some other digital media. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using LSB insertion method. The combination of these two methods will enhance the security of the data embedded. A comparative analysis is made to demonstrate the effectiveness of the proposed method by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). We analyzed the data hiding technique using the image performance parameters like Mean, Entropy and Standard Deviation. The main objective in this paper is to provide resistance against statistical attacks and visual as well as high capacity.***

Keywords: Steganography, Mean Square Error, Peak Signal to Noise Ratio

1. Introduction

As the world changes technology is also changing rapidly. In advancement of network technology domain, large amount of multimedia information is transmitted over the Internet conveniently. Various confidential data such as Banking, Military, Government, Banking and other space, secured data and geographical images taken from satellite and commercial important document are transmitted over the Internet. While using secret information we need more secure information hiding techniques. Steganography is the art or practice of concealing a image, message or file within another image, message, or file. The word steganography combines the Ancient Greek words steganos. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganography coding inside of a transport layer, such as a image file, document file, protocol or program. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an unobjectionable image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages—no matter how unbreakable—will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

2. Least Significant Bit Technique

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M‟s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Bit) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size.

3. Stream Cipher Method

Stream ciphers are an important class of symmetric encryption algorithms. Their basic design philosophy is inspired by the Vernam (One-Time-Pad) cipher, which encrypts by XOR'ing the plaintext with a random key. The drawback of the Vernam cipher is the requirement that key must be a true random sequence, shared by the sender and the receiver, and can only be used once[14]. This poses a practical problem in terms of key generation and distribution. Instead, stream ciphers expand a given short random key into a pseudo-random key stream, which is then XOR'ed with the plaintext to generate the cipher text. The basic form of a stream cipher involves the generation of a pseudorandom sequence of bits that is XOR'ed bit by bit with the plaintext to generate the cipher text at the transmitter. At the receiver, the plain text is recovered by generating the identical pseudorandom sequence of bits such that it is exactly synchronized with the received cipher text stream. Stream encryption systems are categorized into synchronous and

self-synchronous. In the former, the key stream is generated independently of the message, so that a lost character during transmission necessitates a resynchronization of the transmission and receiver key generators. The block diagram of synchronous stream encryption is as shown in Figure. The starting state of the key generator is initialized with a known input, Io. The cipher text is obtained by modulo addition of the ith message character, mi. Such synchronous ciphers are generally designed to utilize confusion but not diffusion. That is, the encryption of a character is not diffused over some block length of message. For this reason, Synchronous stream ciphers do not exhibit error propagation.

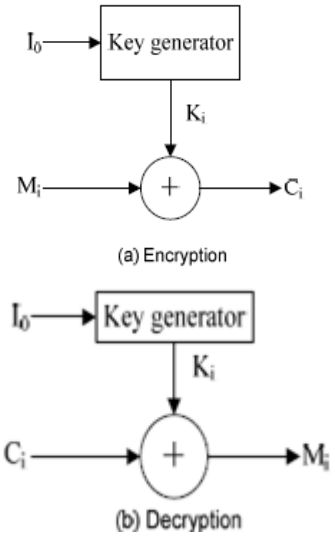
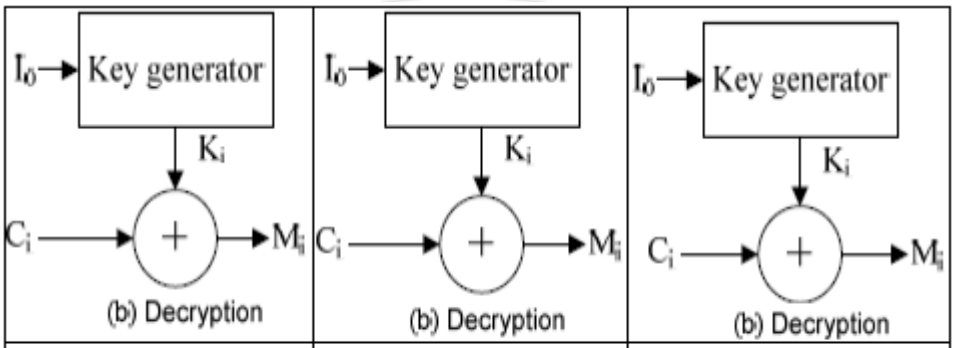


Figure: Block Diagram of Synchronous Stream Encryption



Font size	9 pt	
Font	Times New Roman	
Line Spacing	1.0	
Heading	Bold	Center

4. Literature Survey

Junhwan Kim [1] "Jigsaw Image Mosaics" deals with This paper introduces a new kind of mosaic, called Jigsaw Image Mosaic (JIM), where image tiles of arbitrary shape are used to compose the final picture. The generation of a Jigsaw Image Mosaic is a solution to the following problem: given an arbitrarily-shaped container image and a set of arbitrarily-shaped image tiles, fill the container as compactly as possible with tiles of similar color to the container taken from the input set while optionally deforming them slightly to achieve a more visually pleasing effect. We approach the problem by defining a mosaic as the tile configuration that minimizes a mosaicking energy function. We introduce a general energy-based framework for mosaicking problems that extends some of the existing algorithms such as Photo mosaics and Simulated Decorative Mosaics. We also present a fast algorithm to solve the mosaicking problem at an acceptable computational cost. We demonstrate the use of our method by applying it to a wide range of container images and tiles. [1]

Gianpiero Di Blasi [2] "PUZZLE IMAGE MOSAIC" proposes a new technique to produce composite images called Puzzle Image Mosaic (PIM). The method is inspired by Jigsaw Image Mosaic (JIM), where image tiles of arbitrary shape are used to compose the final picture. The JIM approach leads to impressive results, but the required computation time is high. We propose an algorithm that produces good results in lower time. The technique takes advantage from recent results about data structures aimed to optimize proximity queries. Experimental results prove the soundness of our method. [2]

Yu Liu, Olga Veksler and all [3] "Simulating Classic Mosaics with Graph Cuts" deals with Classic mosaic is one of the oldest and most durable art forms. There has been a growing interest in simulating classic mosaics from digital images recently. To be visually pleasing, a mosaic should satisfy the following constraints: tiles should be non-overlapping, tiles should align to the perceptually important edges in the underlying digital image, and orientation of the neighboring tiles should vary smoothly across the mosaic. Most of the existing approaches operate in two steps: first they generate tile orientation field and then pack the tiles according to this field. However, previous methods perform these two steps based on heuristics or local optimization which, in some cases, is not guaranteed to converge. Some other major disadvantages of previous approaches are: (i) either substantial user interaction or hard decision making such as edge detection is required before mosaicking starts (ii) the number of tiles per mosaic must be fixed beforehand, which may cause either undesired overlap or gap space between the tiles. Author propose a novel approach by

formulating the mosaic simulating problem in a global energy optimization framework. Our algorithm also follows the two-step approach, but each step is performed with global optimization.

For the first step, we observe that the tile orientation constraints can be naturally formulated in an energy function that can be optimized with the _-expansion algorithm. For the second step of tightly packing the tiles, we develop a novel graph cuts based algorithm. Our approach does not require user interaction, explicit edge detection, or fixing the number of tiles, while producing results that are visually pleasing. [3]

Mohammad Sajid [4] "Image Encryption using Different Techniques for High Security Transmission over a Network" focus on Digital image is a collection of the pixel with different intensity values, and each image is in the form of n*m, no of pixel (where n,m is no of Rows and Column) when we transfer a digital image from source to destination through a network, it need to be encrypted at the source side and decrypted at the destination side. Encryption is process of hiding the information, when the information is transferred through a network and decryption is the process of extracting the information from an encrypted information. For this encryption and decryption, we need some encryption and decryption algorithm. Security of a data or information is very important now a day in this world. And everybody want a secure network, for transmission of his information, being a well secure network there is also a chance of hacking a data.So we need a more secure data with high security environment. Generally, we do high secure working environment and data is also secure with an encryption and decryption method or technique, but that techniques uses only one encryption and decryption keys.[4]

5. Research Methodology

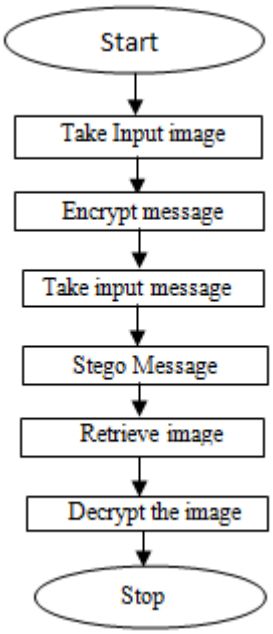


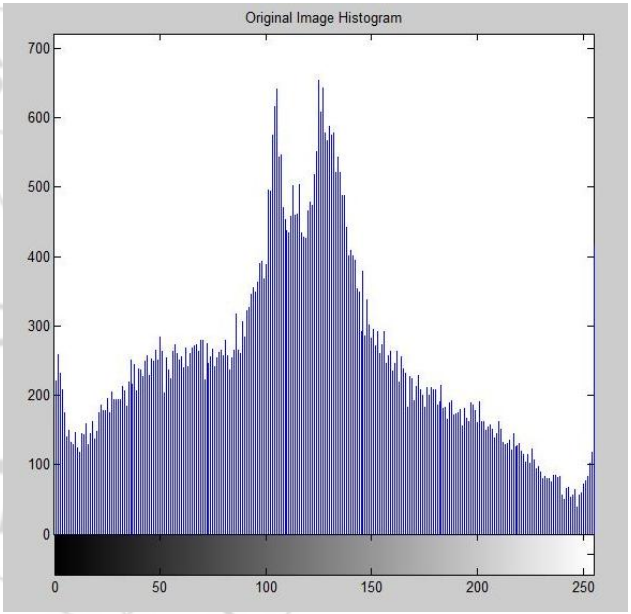
Figure: Flow of the project

The flow of project is as follows:

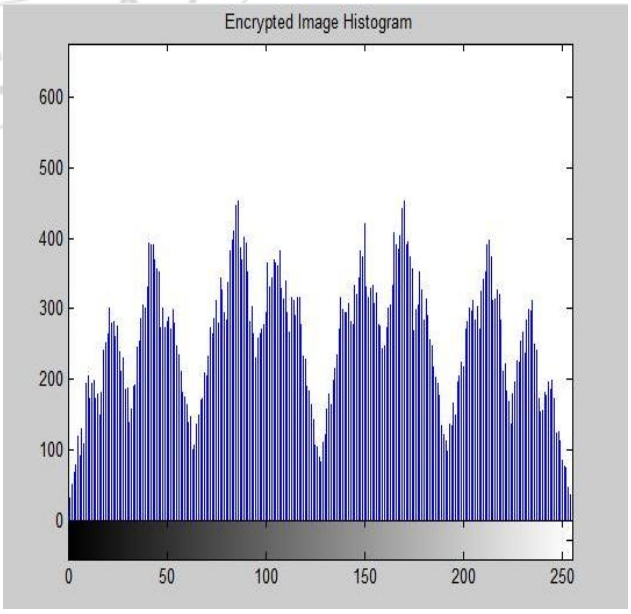
a) firstly take an input image.
b) Encrypt image using stream cipher method
c) and then take input message.
d) After that Message is hidden using improve LSB (Block Transformation).
e) Then retrieve message and image.
f) Then decrypt the image.

6. Experimental Result

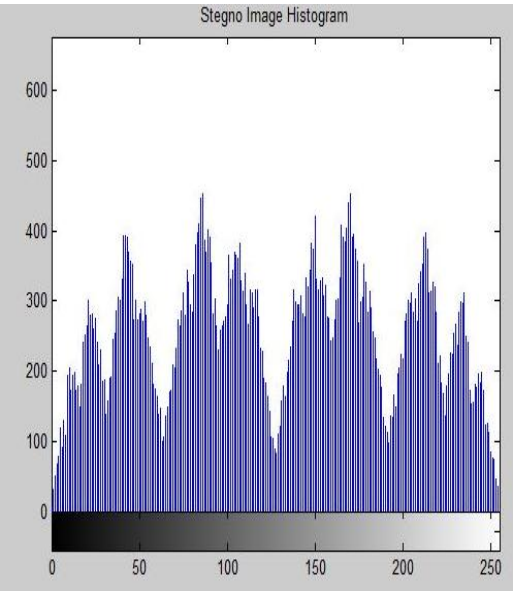
Now give an attention on both images original and Encoded image we can clearly see the difference between the original image and encoded image. Encoded image is that image which has the secret data by performing the LSB technique. The resolution of the encoded image is burst from the original image. The difference between the original image and encoded image can also see from the following histograms of the both original image and encoded image by using LSB technique in Gray and RGB formats



Histogram of Original Image



Histogram of Encrypted Image



Histogram of STEGO IMAGE

7. Conclusions

In this paper the existing Least Significant Bit Algorithm has been analyzed and found to have a more amount of distortion, so a new method has been proposed "Enhanced Least Significant Bit (ELSB)". It improves the performance of the LSB method. The main objective of my project is to maintain the quality of the secrete image that we are hiding. And again maintaining the quality of target image after hiding the secrete image so nobody can see that a image is hiding in that image.

8. Acknowledgment

I acknowledge the sincere and long lasting support of my project guide Prof. Parag Jawarkar and other professors of Electronics and Communication Department, who gave me healthy suggestion and had helpful discussion.

References

[1] Junhwan Kim, Fabio Pellacini "Jigsaw Image Mosaics" IEEE Trans. on PAMI, Vol. 12, no 9, pp. 855-867, Sept. 20069.
[2] Gianpiero Di Blasi,Giovanni Gallo "PUZZLE IMAGE MOSAIC" TX, 2002, 657-664
[3] Yu Liu, Olga Veksler, and Olivier Juan "Simulating Classic Mosaics with Graph Cuts" ACM Transactions on Graphics, SIGGRAPH 2003 22(3) (2003) 277–286
[4] Mohammad Sajid Qamruddin Khizrai "Image Encryption using Different Techniques for High Security Transmission over a Network" International Journal of Engineering Research and General Science Volume 2, Issue 4, June-July, 2014
[5] I-Jen Lai and Wen-Hsiang Tsai "Secret-Fragment-Visible Mosaic Image–A New Computer Art and Its Application to Information Hiding" IEEE 2011 [6] G. Elber and G. Wolberg, "Rendering traditional mosaics," Vis. Comput., vol. 19, pp. 67–78, 2003.
[6] J.Kimand F. Pellacini, "Jigsaw image mosaics," in Proc. SIGGRAPH, San Antonio, TX, Jul. 2002, pp. 657–664.
[7] G.Di Blasi, G. Gallo, andM. Petralia, "Puzzle image mosaic," in Proc. IASTED/VIIP, Benidorm, Spain, Sep. 2005, pp. 33–37.
[8] G. Di Blasi and G. Gallo, "Artificial mosaics," Vis. Comput., vol. 21, pp. 373–383, 2005.
[9] S. Battiato, C. Guarnera, G. Di Blasi, G. Gallo, and G. Puglisi, M. Bubak, Ed. et al., "A novel artificial mosaic generation technique driven by local gradient analysis," in Proc. ICCS, Crakov, Poland, Jun. 2008, vol. 5102, pp. 76–85.

Author Profile

Khushboo Dhoke received degree in Electronics Engineering from G.H. Raisoni College of Engineering & Technology for Womens in 2013.

Shubhangi Dhengre received master degree in Electronics Engineering from Yashwantrao Chauhan College of Engineering.