ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Novel Image Steganography Technique Implementation Using Edge Detection Process

B.Pravallika
Research Scholar,
Department of ECE,
Teegala Krishna Reddy Engineering College, Hyderabad, India.

B.Jamuna
Assistant Professor,
Department of ECE,
Teegala Krishna Reddy Engineering College, Hyderabad, India.

Dr.P.Ram Mohan Rao
Principal,
Teegala Krishna Reddy Engineering College, Hyderabad, India.

ABSTRACT:

Steganography is that the science of invisible communication. It aims at concealment sensitive data in digital media in very thanks to conceal the existence of knowledge. In this paper, we have a tendency to aim to propose associate improved secured image steganography theme. In this paper we implement Steganography concept with edge detection procedure. This experiment was carried out using Xilinx Platform Studio with implementation on Spartan 3EDK FPGA

Keywords:

Steganography, Edge Detection, FPGA.

I.INTRODUCTION:

Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern inding, patience, determination, and luck. Cryptanalysts are also called attackers.

Cryptology embraces both cryptography and cryptanalysis.First we start with a few definitions. Cryptography can be defined as the processing of information into an unintelligible (encrypted) form for the purposes of secure transmission. Through the use of a "key" the receiver can decode the encrypted message (decrypting) to retrieve the original message.

Stenography improves on this by hiding the fact that a communication even occurred. The message m is imbedded into a harmless message c which is defined as the cover-obect. The message m is then embedded into c, generally with use of a key k that is defined as the stego-key. The resulting message is then embedded into the cover-object c, which results in stego-objects.

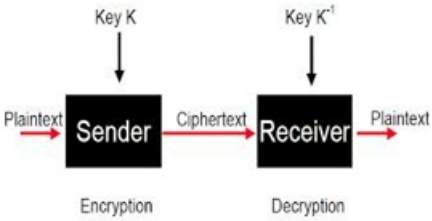


Fig 1: cryptography block diagram

II.STEGANOGRAPHY:

Steganography means to hide secret information into innocent data. Digital images are ideal for hiding secret information. An image containing a secret message is called a cover image. First, the difference of the cover image and the stego image should be visually unnoticeable. The embedding itself should draw no extra attention to the stego image so that no hackers would try to extract the hidden message illegally.

Second, the message hiding method should be reliable. It is impossible for someone to extract the hidden message if she/he does not have a special extracting method and a proper secret key. Third, the maximum length of the secret message that can be hidden should be as long as possible. "Steganography is the art of hiding information in ways that prevent the detection of hidden messages,"

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

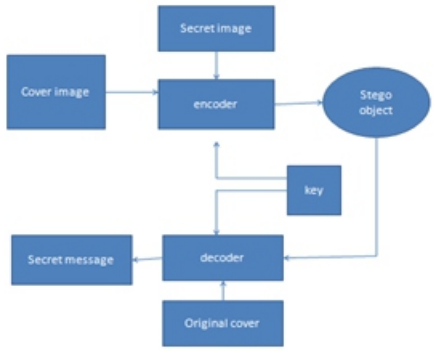


Fig 2: steganography block diagram

III. CRYPTOGRAPHY VS STEGANOGRAPHY:

Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in steganography the existence of data is conceived means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the information is hidden. Information to be hidden + cover object = stego object. To add more security the data to be hidden is encrypted with a key before embedding. To extract the hidden information one should have the key. A stego object is one, which looks exactly same as cover object with an hidden information.

EXISTING METHOD:

- Using Wavelet Transform to decompose original images into proper levels.
- One low-frequency approximate component and three high-frequency detail components will be acquired in each level.
- Lifting Transform of individual acquired low frequency approximate component and high frequency detail components from both of images, neighborhood interpolation method is used and the details of gray can't be changed.
- According to definite standard to fuse images, local area variance is chose to measure definition for low frequency component.
- Inverse Transformation is taken to get Original Image.

PROPOSED METHOD:

- In proposed method steganography presented,
- 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.

IV. Proposed Algorithm:

The proposed algorithm was implemented as Follows

- Reading an Image
- Applying Edge Detection to the Image using Canny Edge Detection
- Identifying the Edge pixel Values
- After Identifying Embedding the Message in the Original Image where the edges are present
- During decryption step applying the same procedure in which the data embedded in that decryption was done.

Block Diagram:

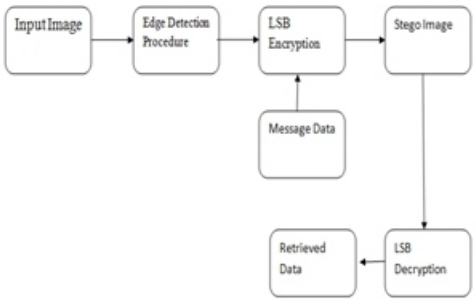


Fig3: Block Diagram

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In this procedure we apply Edge detection and LSB steganography algorithms that are explained below

EDGE DETECTION:

Edge detection is the name for a set of mathematical methods which aim at identifying points in a digital image at which the image brightness changes sharply or, more formally, has discontinuities. The points at which image brightness changes sharply are typically organized into a set of curved line segments termed edges. The same problem of finding discontinuities in 1D signals is known as step detection and the problem of finding signal discontinuities over time is knownas change detection.

CANNY EDGE DETECTION:

John canny considered the mathematical problem of deriving an optimal smoothing filter given the criteria of detection, localization and minimizing multiple responses to a single edge. He showed that the optimal filter given these assumptions is a sum of four exponential terms. He also showed that this filter can be well approximated by first-order derivatives of Gaussians. Canny also introduced the notion of non-maximum suppression, which means that given the pre smoothing filters, edge points are defined as points where the gradient magnitude assumes a local maximum in the gradient directionAlthough his work was done in the early days of computer vision, the canny edge detector (including its variations) is still a state-of-the-art edge detector.[11] Unless the preconditions are particularly suitable, it is hard to find an edge detector that performs significantly better than the Canny edge detector.

The Canny-Deriche detector was derived from similar mathematical criteria as the Canny edge detector, although starting from a discrete viewpoint and then leading to a set of recursive filters for image smoothing instead of Gaussian filters. Different gradient operators can be applied to estimate image gradients from the input image or a smoothed version of it. The simplest approach is to use central differences:

$$L_x(x,y) = -1/2 \cdot L(x-1,y) + 0 \cdot L(x,y) + 1/2 \cdot L(x+1,y)$$
$$L_y(x,y) = -1/2 \cdot L(x,y-1) + 0 \cdot L(x,y) + 1/2 \cdot L(x,y+1),$$

corresponding to the application of the following filter masks to the image data:

$$L_x = \begin{bmatrix} -1/2 & 0 & 1/2 \end{bmatrix} * L \quad \text{and} \quad L_y = \begin{bmatrix} +1/2 \\ 0 \\ -1/2 \end{bmatrix} * L.$$

The well-known and earlier sobel operator is based on the following filters:

$$L_x = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} * L \quad \text{and} \quad L_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} * L.$$

Fig 4: edge detection

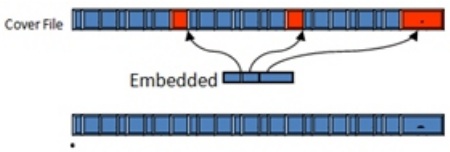
IMAGE EMBEDDING METHODS:

Four steganography methods will be explored:

- Least Significant Bit Insertion
- Algorithms and Transformations
- Redundant Pattern Encoding
- Spread Spectrum Method

LEAST SIGNIFICANT BIT INSERTION (LSB)

The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.



ADVANTAGES OF LSB INSERTION:

A major advantage of the LSB algorithm is it is quick and easy.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

There has also been steganography software developed which work around LSB color alterations via palette manipulation. LSB insertion also works well with gray-scale images.

V. Results and Snapshot:

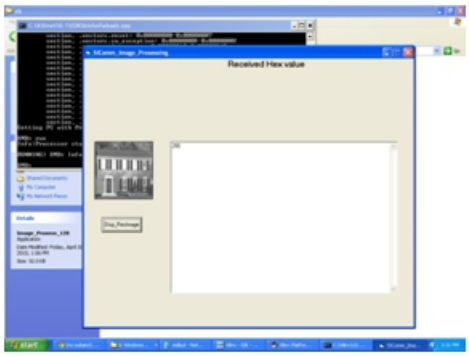


Fig5: Input Image .

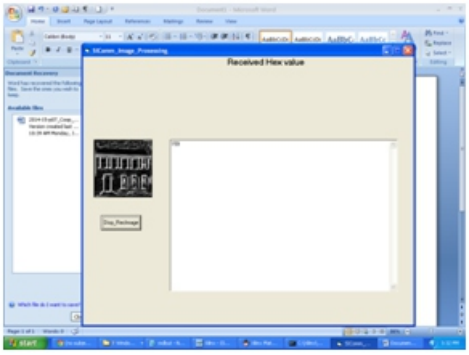


Fig6: Edge Detected Image.

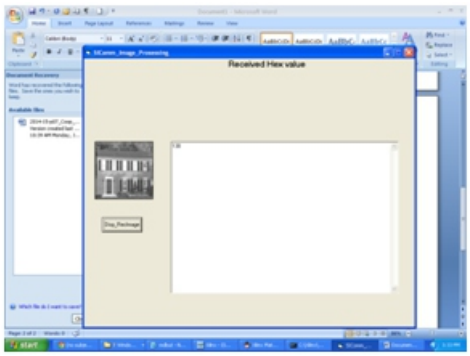


Fig7:Stego Image

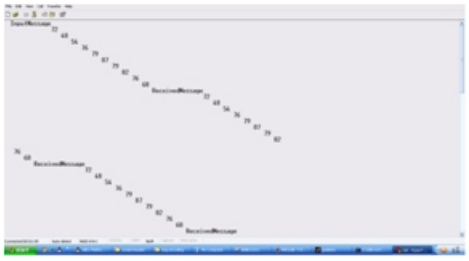


Fig8: Output Data

VII. CONCLUSION:

In this paper we have presented a new method of adaptive steganography with novel embedding. The approach was analyzed and shown to have a very high confidentiality due to thes harpness of information recovery. The New Approach is using Lesser hardware architecture with in a Spartan 3 FPGA with 50MHz Clock Crystal. So We can use it to the steganography technique very easily than other techniques without any problem.

VII. REFERENCES:

[1]W. J. Chen, C. C. Chang, and T. H. N. Le, "High payload steganography mechanism using hybrid edge detector", Expert Systems with Applications, vol. 37, no. 4, pp 3292-3301, 2010.

[2]Z. Nanning, "Computer visualization and pattern recognition", National Defense Industry Press, vol. 2, pp. 1069–1074, 1998.

[3]K. Wang, Z. M. Lu, and Y. J. Hu, "A high capacity lossless data hiding scheme for JPEG images", The Journal of Systems and Software, vol. 86, no. 7, pp. 1965-1975, 2013.

[4]A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, vol. 90, no. 3, pp. 727-752, 2010.

[5]D. L. Hostalot, and D. Megıas, "LSB matching steganalysis based on patterns of pixel differences and random embedding", Computers & Security, vol. 32, pp. 192-206, 2013.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[6]A. Kanso, and H. S. Own, "Steganographic algorithm based on chaotic map", Communication in Nonlinear Science and Numerical Simulations, vol. 17, no. 8, pp. 3287-3302, 2012.

[7]N. H. A. Mahdi, A. Yahya R. B. Ahmad, and O. M. Al-Qershib, "Secured and robust information hiding scheme", Procedia Engineering, vol. 53, pp. 463-471, 2013.

[8]S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A secure and high capacity image steganography technique", Signal and Image Processing: An International Journal, vol. 4, no.1, 2013.

[9]B. Li, J. He, J. Huang, and Y. Q. Shi, "A survey on image steganography and steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, pp. 2073-4212, 2011.

[10]R. M. May, "Simple mathematical model with very complicated dynamics", Nature, vol. 261, pp. 459–467, 1967.