ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Reconfigurable Processor for Image Steganography using DCT with Morphological Operations

Achsah Elizabeth Varghese

M. Tech Student (VLSI & Embedded Systems), Dept. of ECE, , IIET, M. G. University, Kottayam, Kerala, India

ABSTRACT: Image processing is a powerful tool in many image and video applications**.** A reconfigurable processor is presented for image processing in this paper. Steganography is the art of hiding the fact that communication is taking consign, by hiding data in other information. Many different carrier file formats could be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret data in images, there exists a large variety of steganography techniques, some are more complex than others and all of them have respective strong and weak points. Various applications have different requirements of the steganography method used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden. This work intends to give a method of image steganography, based on Discrete Cosine Transform with morphological operations. This method employed the efficient steganography as well as the noise reduction in the recovering stego images (secret information). The DCT method is used to transform into DCT domain i.e. frequency domain. Then the secret images is embedded into layers of images in transform domain itself after embedding this image is again converted back into image domain and that is the image called stego image. The quality of steganography method could be compared with the no visual difference in the original and stego image. The visual difference easily caught by anyone who have seen original image before so the visual difference should be negligible in the stego image.

KEYWORDS*:* DCT; Morphological Operation; Steganography and LSB.

I. INTRODUCTION

Image processing is extremely useful in various areas, such as object recognition, tracking, motion detection and machine intelligence [1]-[6], image analysis and understanding [7], [8], video processing [9], computer vision [10], [11], and identification and authentication systems [12]-[15] . Application-specific chips and hardware have been reported for various applications. The major drawback of application-specific chips is the lack of flexibility. With the continuous CMOS technology scaling, the importance of flexibility exceeds that of silicon area, especially in vision chips. The reconfigurable technique can bridge the gap between application-specific integrated circuits and flexibility. Chips were presented to perform basic binary morphological operations, such as dilation, erosion, opening, and closing. Hiding Capacity plays a vital role for efficient covert communication. This is achieved by Steganography. Steganography is the science of hiding the information into the other information so that the hidden information appears to be nothing to the human eyes. There are many ways to hide information inside an image, audio/video, document etc. But Image Steganography has its own advantages and is most popular among the others. This paper gives a review of various methods such as image domain and transformation domain algorithms available for implementing Image Steganography. In this paper, a high capacity Image Steganography schemes are discussed for different file formats. Covert communication is taking place by encrypting the password for information to be protected. The intended receiver will decrypt the information using that password.

Since the rise of the Internet one of the most important factors of data technology and communication has been the security of information. Steganography is the art and science of invisible communication. The strength of steganography could thus be amplified by combining it with cryptography. Two different technologies that are closely related to steganography are watermarking and fingerprinting [17]. These technologies are mainly concerned with the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

protection of intellectual property, thus the algorithms have other requirements than steganography. These requirements of good steganographic algorithm will be discussed below. Watermarking all of the instances of an object are "marked" in the same way. The kind of data hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection [18]. With fingerprinting alternatively, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties [17]. A successful attack on a steganographic system consists of an adversary observing that there is data hidden inside a file, while a successful attack on watermarking or fingerprinting system would not be to detect the mark, but to remove it [16].

A lot of governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether [19], forcing people to study other methods of secure data transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. This reflection is based on a set of criteria that we have identified for image steganography. Steganography is the art of hiding the fact that communication is taking consign, by hiding data in other information. Many different carrier file formats could be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret data in images, there exists a large variety of steganography techniques, some are more complex than others and all of them have respective strong and weak points. Various applications have different requirements of the steganography method used. For example, some applications may require absolute invisibility of the secret information, while others require a larger secret message to be hidden**.**

II. LITERATURE SURVEY

In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), [20] Investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR in both domain (time and frequency) but DFrFT gives an advantage of additional stego key.

In the year of 2013 Akhtar, N.; Johri, P.; Khan, S., [21] implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stegoimage. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality.

In the year of 2013 Prabakaran, G.; Bhavani, R. and Rajeswari P.S. [22] Investigated on Medical records are extremely sensitive patient information a multi secure and robustness of medical image based steganography scheme is proposed. This methodology provides an efficient and storage security mechanism for the protection of digital medical images. Authors proposed a viable steganography method using Integer Wavelet Transform to protect the MRI medical image into a single container image. The patient's medical diagnosis image has been taken as secret image and Arnold transform was applied and scrambled secret image was obtained. In this case, the scrambled secret image was embedded into the dummy container image and Inverse IWT was taken to get a dummy secret image. It has been observed that the quality parameters are improved with acceptable PSNR compared to the existing algorithms.

In the year of 2012 Thenmozhi, S. and Chandrasekaran, M., [23] presented the novel scheme embeds data in integer wavelet transform coefficients by using a cropping function in an 8×8 block on the cover image. The optimal pixel change process has been applied after embedding the message. Authors employed the frequency domain to increase the robustness of our steganography method. Integer wavelet transform avoid the floating point precision problems of the wavelet filter. Result shows that the method outperforms adaptive steganography technique based on integer wavelet transform in terms of peak signal to noise ratio and capacity.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

In the year of 2012 Das, R. and Tuithung, T. [24] proposed a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. The size of Huffman encoded bit stream and Huffman Table are also embedded inside the cover image, in order that the Stego-Image becomes standalone information to the receiver. Results show that the algorithm has a high capacity and a good invisibility. Moreover Peak Signal to Noise Ratio (PSNR) of stego image with cover image shows better result in comparison with other existing steganography approaches. The satisfactory security is maintained in this research.

III. MORPHOLOGICAL OPERATIONS

In this section, binary image processing operations in the proposed processor are discussed, including binary mathematical morphology operations. Mathematical morphology is a powerful tool for image processing and analysis in a wide range of applications, including shape recognition, image processing, video processing, document authentication and computer vision. The basic binary morphological operations are dilation and erosion [25]. Either of the two operations have two operands: the input signal, which is usually an image, and the structuring element characterized by its shape, size, and center location. The other binary morphological operations such as opening, closing, and hit-and-miss operation are based on various combinations of the two basic operations, dilation, and erosion.

Dilation is one of the basic operations in mathematical morphology. The dilation operation usually uses a structuring element for probing and expanding the shapes contained in the input image. To compute the dilation of a binary input image by this structuring element, we consider each of the background pixels in the input image in turn. For each background pixel (which we will call the input pixel*)* we superimpose the structuring element on top of the input image so that the origin of the structuring element coincides with the input pixel position. If at least one pixel in the structuring element coincides with a foreground pixel in the image underneath, then the input pixel is set to the foreground value. If all the corresponding pixels in the image are background, however, the input pixel is left at the background value.

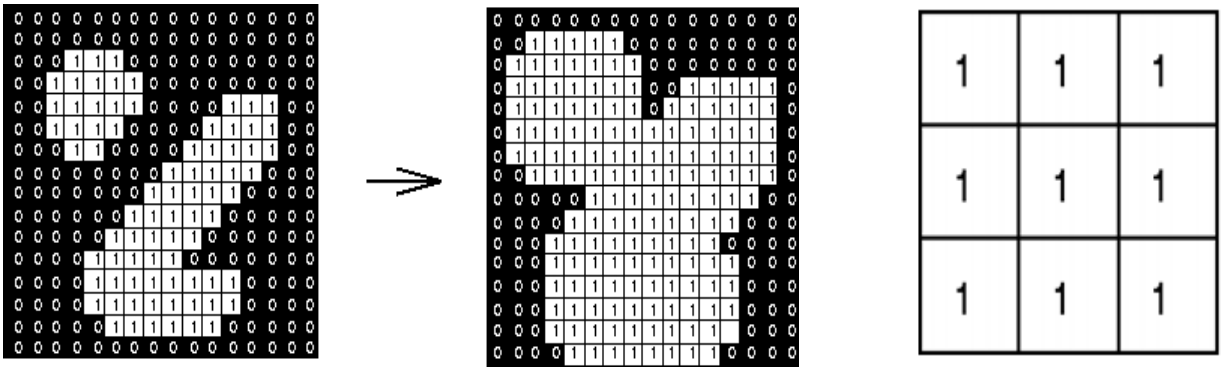

Fig. 1. Effect of dilation using a 3×3 square structuring element

Erosion is one of two fundamental operations (the other being dilation) in morphological image processing from which all other morphological operations are based. It was originally defined for binary images, later being extended to grayscale images, and subsequently to complete lattices. To compute the erosion of a binary input image by this structuring element, we consider each of the foreground pixels in the input image in turn. For each foreground pixel (which we will call the input pixel) we superimpose the structuring element on top of the input image so that the origin of the structuring element coincides with the input pixel coordinates. If for *every* pixel in the structuring element, the corresponding pixel in the image underneath is a foreground pixel, then the input pixel is left as it is. If any of the corresponding pixels in the image are background, however, the input pixel is also set to background value.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

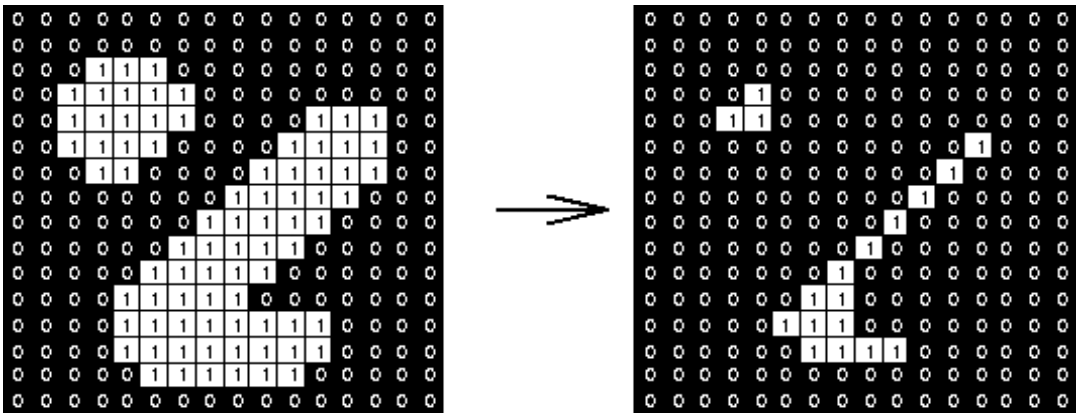

Fig. 2. Effect of dilation using a 3×3 square structuring element

IV. PROPOSED METHODOLOGY

Here the method of image steganography, based on Discrete Cosine Transform with morphological operations. This method provide the efficient steganography as well as the noise reduction in the recovering stego images (secret information). The DCT method is used to transform into DCT domain i.e. frequency domain. The cover image is separated in to three different layers and the secret images is embedded into layers of images in transform domain itself after embedding this image is again converted back into image domain and that is the image called stego image. The quality of steganography method could be compared with the no visual difference in the original and stego image. The visual difference easily caught by anyone who have seen original image before so the visual difference should be negligible in the stego image**.** Least significant bit i1nsertion is a common, simple approach to embedding data in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret data. When using a 24-bit image, a bit of each of the red, green and blue colour components could be used, since they are each represented by a byte. In other words, one could store 3 bits in each pixel.

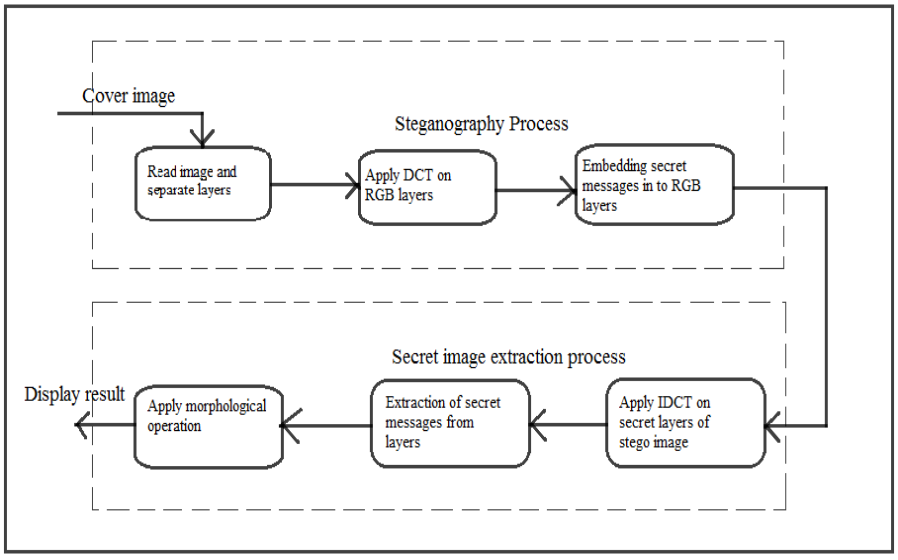

Fig. .3 . Block diagram of proposed methodology

Block diagram of proposed methodology is shown in figure. 3. The first block reading images given as input to the system i.e. cover image which is a colour image. After loading into simulation environment the colour image is then separated into Red, Green and Blue layers for embedding process. Each secret message is then embedding in layers of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

colour image in discrete cosine transform. After embedding process the red green and blue layers are combined and stored on the pc and this image is called as stego image which contains the all three secret messages. In the recovery process, the stego image is then again separated into layers for extraction of secret message for which we need to apply DCT on red, green and blue layers. The recovered secret messages contain error due to transform domain. Now to reduce these errors we are applying morphological operation and we will finally get the secret images. Table.1 shows the comparison of different image steganography algorithms.

	LSB in BMP	LSB in GIF	JPEG compression	Patchwork	Spread spectrum
Invisibility	High*	Medium*	High	High	High
Payload capacity	High	Medium	Medium		Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious files	Low	Low	High	High	High

Table 1: Comparison of image steganography algorithms

V. SIMULATION AND IMPLEMENTATION RESULTS

Model Sim and Mat lab are the softwares used for the simulation. After simulation all the designed systems were implemented on the Xilinx Spartan 3E FPGA. The FPGA kit used for the implementation is Xilinx Spartan 3E (family), XC3S50 (device), ft 256 (Package), -4 (speed grade).

MATLAB is a tool for doing numerical computations with matrices and vectors. It can also display information graphically. MATLAB is matrix-oriented, so what would take several statements in C or Fortran can usually be accomplished in just a few lines using MATLAB's built-in matrix and vector operations.

Model Sim is a well-known HDL simulator in Xilinx. Model Sim is a digital simulator for both Verilog and VHDL hardware description languages. It doesn‟t create any hardware, even on the monitor. Model Sim just compiles the code, checks syntax and provides the waveform of the design behaviour according to the inputs values defined at the Test Bench file.

For simulation model we have used the colour image to utilize the all the three channels i.e. Red, Green and Blue for hiding separate data in each of the channel.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

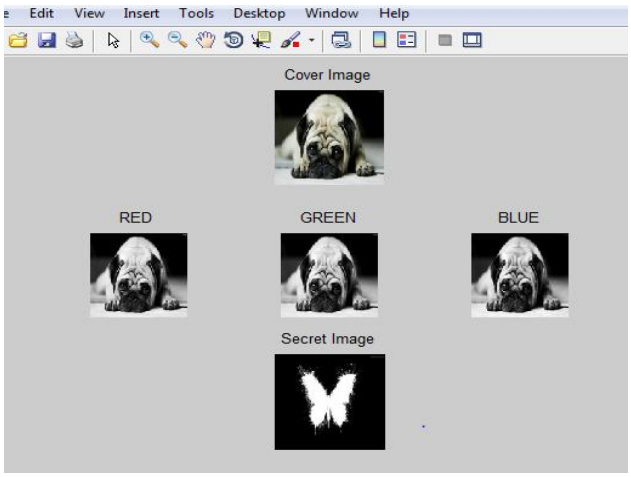

Fig. .4. Cover Image And Red, Green, Blue Channel Of Cover Image And Secret Image

The cover image then separated into different channels for hiding process of secret message behind them. The DCT method is used to transform into DCT domain i.e. frequency domain. Then the secret images is embedded into layers of images in transform domain itself after embedding this image is again converted back into image domain and that is the image called stego image. Least significant bit (LSB) insertion is a common, simple approach to embedding data in a cover image. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret data. When using a 24-bit image, a bit of each of the red, green and blue colour components could be used, since they are each represented by a byte.

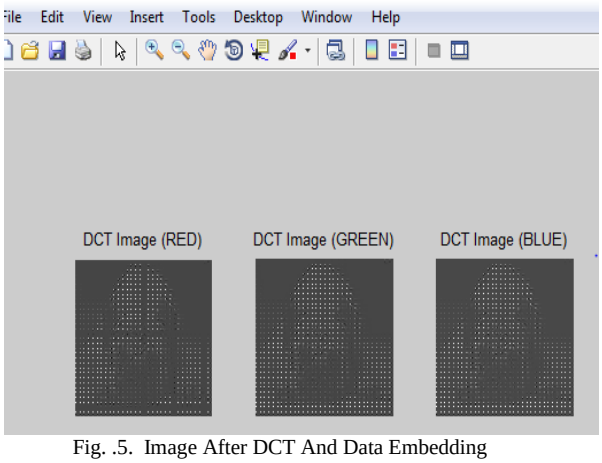

Fig. .5. Image After DCT And Data Embedding

The recovery process is then performed and the results are compared with the original secret message and the recovered secret message.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

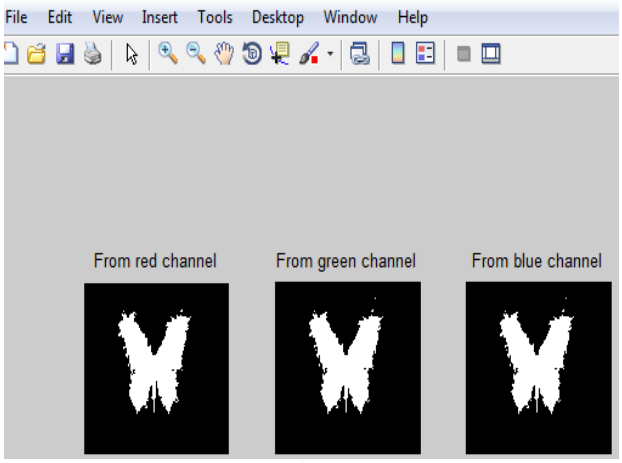

Fig. 6. Recovered Image After Morphological Operations

Then the recovered secret message are then passed through morphological operation which enhances the recovered secret message and remove noises to appear correctly.

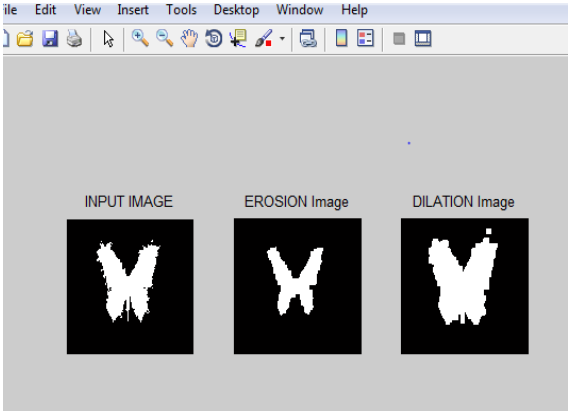

Fig.. 7. Recovered Secret Image From Three Channels

Morphological operations are affecting the form, structure or shape of an object. Applied on binary images .The two principal morphological operations are dilation and erosion. Dilation allows objects to expand, thus potentially filling in little holes and connecting disjoint objects. Erosion shrinks objects by etching away their boundaries. These operations could be customized for an application by the proper selection of the structuring element, which determine exactly how the objects will be dilated or eroded. After these morphological operations, noise reduction in the recovering stego images (secret information) observed by calculating the PSNR(peak signal to noise ratio) Value.

Peak signal-to-noise ratio, often abbreviated PSNR, is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codecs. The signal is the original data, and the noise is the error introduced by compression. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

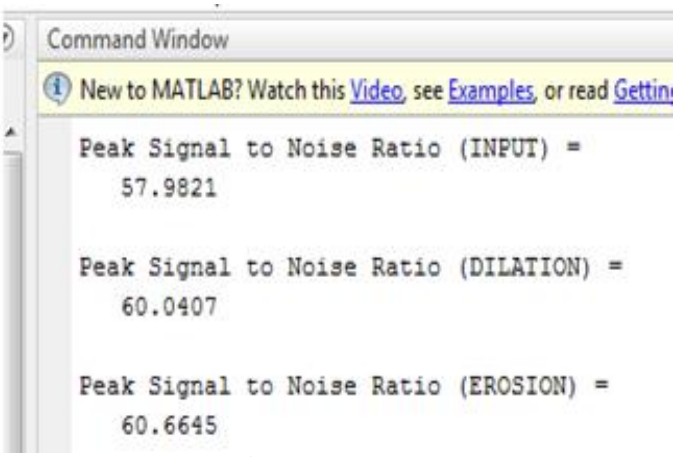

Fig.. 8. PSNR Value After Morphological Operations

VI. CONCLUSION

In this work a new method of steganography which has some effective work done in the form of data embedding capacity using available resources. The results shows that the proposed methodology is best for less noisy system, because from robustness test it is clear that the White Gaussian Noise, Resizing, Poisson Noise and Compression may damage the secret data, which partly unrecognizable. The future of this method is the improvement against the possible attacks occurs during transmission of information, and to secure using any encryption method so that intruder can't get hidden data easily. In the future enhancement of steganographic method is to make more robust recovery process so that the secret massage could be recovered correctly. Here we have used the morphological process to enhance the recovered message but in the future if apply method that is more efficient then it will be helpful for robust system. Morphological operations for binary images provide a basic techniques and those operations for gray scale images requires more sophisticated mathematical concepts for extracting image components that are useful in the representation and description of regions.

REFERENCES

1. Y. Liu and C. Pomalaza-Raez, "A low-complexity algorithm for the on-chip moment computation of binary images," in *Proc. Int. Conf. Mechatron. Autom.*, 2009, pp. 1871–1876.
2. E. C. Pedrino, O. Morandin, Jr., and V. O. Roda, "Intelligent FPGA based system for shape recognition," in *Proc. 7th Southern Conf. Programmable Logic*, 2011, pp. 197–202.
3. M. F. Talu and I. Turkoglu, "A novel object recognition method based on improved edge tracing for binary images," in *Proc. Int. Conf. Appl. Inform. Commun. Technol.*, 2009, pp. 1–5.
4. A. J. Lipton, H. Fujiyoshi, and R. S. Patil, "Moving target classification and tracking from real-time video," in *Proc. Workshop Appl. Comput. Vision*, 1998, pp. 8–14.
5. J. Kim, J. Park, K. Lee *et al.*, "A portable surveillance camera architecture using one-bit motion detection," *IEEE Trans. Consumer Electron.*, vol. 53, no. 4, pp. 1254–1259, Nov. 2007.
6. D. J. Dailey, F. W. Cathey, and S. Pumrin, "An algorithm to estimate mean traffic speed using uncalibrated cameras," *IEEE Trans. Intell. Transportation Syst.*, vol. 1, no. 2, pp. 98–107, Jun. 2000.
7. T. Ikenaga and T. Ogura, "A fully parallel 1-Mb CAM LSI for real-time pixel-parallel image processing," *IEEE J. Solid-State Circuits*, vol. 35, no. 4, pp. 536–544, Apr. 2000.
8. E. C. Pedrino, J. H. Saito, and V. O. Roda, "Architecture for binary mathematical morphology reconfigurable by genetic programming," in *Proc. 6th Southern Programmable Logic Conf.*, 2010, pp. 93–98.
9. M. R. Lyu, J. Song, and M. Cai, "A comprehensive method for multilingual video text detection, localization, and extraction," *IEEE Trans. Circuit Syst. Video Technol.*, vol. 15, no. 2, pp. 243–255, Feb. 2005.
10. W. Miao, Q. Lin, W. Zhang *et al.*, "A programmable SIMD vision chip for real-time vision applications," *IEEE J. Solid-State Circuits*, vol. 43, no. 6, pp. 1470–1479, Jun. 2008.
11. A. Lopich and P. Dudek, "A SIMD cellular processor array vision chip with asynchronous processing capabilities," *IEEE Trans. Circuits Syst. I*, vol. 58, no. 10, pp. 2420–2431, Oct. 2011.
12. H. Yang and A. C. Kot, "Binary image authentication with tampering localization by embedding cryptographic signature and block identifier," *IEEE Signal Process. Lett.*, vol. 13, no. 12, pp. 741–744, Dec. 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

13. M. Wu and B. Liu, "Data hiding in binary image for authentication and annotation," *IEEE Trans. Multimedia*, vol. 6, no. 4, pp. 528–538, Aug. 2004.
14. H. Yang, A. C. Kot, and S. Rahardja, "Orthogonal data embedding for binary images in morphological transform domain: A high-capacity approach," *IEEE Trans. Multimedia*, vol. 10, no. 3, pp. 339–351, Apr. 2008.
15. H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," *IEEE Trans. Multimedia*, vol. 9, no. 3, pp. 475–486, Apr. 2007.
16. Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.
17. Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.
18. Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999.
19. Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002..
20. Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," *Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on* , vol., no., pp.97,100, 1-2 March 2013.
21. Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on* , vol., no., pp.385,390, 27-29 Sept. 2013.
22. Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based steganography scheme," *Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on* , vol., no., pp.1188,1193, 20-21 March 2013.
23. Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image stenography based on integer wavelet transform," *Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on* , vol., no., pp.1,5, 18-20 Dec. 2012.
24. Das, R.; Tuithung, T., "A novel steganography method for image based on Huffman Encoding," *Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on* , vol., no., pp.14,18, 30-31 March 2012
25. Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf

BIOGRAPHY

Achsah Elizabeth Varghese is an M Tech scholar in VLSI and Embedded Systems in the Electronics and Communication Department, IIET, MG University. She received B Tech degree in 2013 from M.G. University, Kottayam, Kerala. Her research interests are VLSI and HDL languages etc.