Grenze International Journal of Engineering and Technology, Jan Issue

LSB based Variable Capacity Data Hiding Approach and Enhanced AES Security with Seam Carving

Juhi Singh[1] and Mukesh Singla[2]
[1-2]Department of computer Science and Engineering, BMU Rohtak, Haryana
Email: Juhisingh17@gmail.com, Mukesh27singla@yahoo.co.in

***Abstract*—Steganography is a technology in 'information hiding' that allows us to hide a message (text, document, image, audio, video, etc.) in an image or video.LSB technique is very simple and popular data hiding method in which cover image holds on bit secret data in each pixel. So no of data bit in cover image depends on no of pixels in cover image. In this study we are going to discuss that the capacity of the cover image can be increased via incorporating two mathematical tools in it. One is compressing secret message using DCT compression and second using Seam Carving for increasing the resolution of the cover image.**

***Index Terms*— Steganography, DCT Compression, Seam craving.**

I. INTRODUCTION

Now these days the data is being send over the internet so safety of data becomes very important. Because of the rapid rise of the technological era, all documents, audio, and video have been digitized. This has raised the need to ensure the security and trustworthiness of any document, audio, or video in order to protect personal information and prevent piracy and mass reproduction. This criterion differs from one person to the next. Cryptography and steganography is modern tool to secure the data over the internet. Cryptography and steganography are the methods employed to ensure this, with the former being detectable as noise and the latter being invisible to the naked eye [1]. The use of both tools in proposed data hiding method offer more benefits as compared to other technique.

Steganography earliest usage was in ancient era around 440 B.C. American Revolution saw the usage of invisible ink which could glow in heat, used by the British and Americans for secret communication. In world war II, German spies used invisible dots in letters and changed heights of letter-strokes to hide messages (Petitcolas et al. 1999)[3]. In first World War, prisoners of war hide messages in Morse code by using dots and dashes on alphabets [2].

Even though the objective of the cryptography and steganography are the same, which is to provide secure end-to-end data communication, their definitions of robustness to attack are different. A cryptographic system is regarded as broken when the third party gains access to the original data, whereas the steganography system is regarded as broken when the third party gets the presence of secret data [7].

In modern digital 2-D steganography we are limited to a certain size of message for a particular cover image. [4][5] Our objective for the study is to show that a secret message of a large size can be embedded in a similarly sized cover image. We plan to leverage the use of two techniques namely seam carving and DCT compression for image resizing and messagecompression respectively.

Grenze ID: 01.GIJET.9.1.532

We plan to use seam craving for image resizing as it a content-aware method to resize image to any aspect ratio. Resizing an image increases or decreases it resolution and increases the size of the overall file. Greater the resolution means greater thesize and more bits to manipulate [12][20].
We plan to use DCT compression algorithm as it is simple and convenient to implement in programming language. It provides an average compression ratio of around 64:5 in our testing and demonstration [13][166] . It can be replace by a lossless compression method like LSZ compression but the only challenge being the implementation and integrity of the model.
We can modify the aspect ratio of an image by continually carving out or introducing seams in one direction. We can retarget the image to a different size by using these operations in both directions. The order and selection of seams safeguard the image's content, as defined by the image's content.

II. Literature Review

Kadhim et al. (2018) In their comprehensive examination of steganography: methodology, evaluations, and trends in future research, they explore the implementation of digital image steganography. The basic challenge in developing a Steganographic system, is to maintaining a fair trade-off between robustness, security, imperceptibility, and high embedding rate as claimed. The research examines existing varieties of image steganography as well as recent innovations in each category across a variety of modalities. They also presented a comprehensive review of image steganography, including its general operation, requirements, various characteristics, types, and performance assessments. They also go over the many types of steganography techniques and their reversibility. Each approach has its own set of applications.
Avidan et al. (2018) [9] According to their research study on seam cutting for content-aware scaling, a good resizing algorithm should not only impose physical restrictions, but also consider image content. Seam searching is a content-aware scaling technique that can be applied to both reduction and expansion. On a single image, a seam is an ideal 8-connected path of pixels from top to bottom, or left to right, whose optimality is specified by an image energy function, techniques, as well as their reversibility. Each approach has its own set of applications.
Anitha (2011) [11] Discrete cosine transform and wavelet transform are used in the proposed technique. According to her research on discrete cosine transformation and discrete wavelet transformation, picture compression is an important aspect of digital image processing. The need for image compression becomes clear when the amount of bits per image is estimated using typical sampling rates and quantization methods.

III. Methodology

The process starts by selecting the message to be hidden and selecting the cover image. The cover image is our host image that will store the secret message.[12][14][18] If the message is 4 bits long and the cover image is 8 bits in resolution then embedding the message may lead to drastic change in the cover image. This can be overcome using 2 techniques statedbelow.

A. Image Resizing

The image can be resized to greater resolution to allow more bits in the cover image. Say if we decide on doubling theresolution on the original image the 8 bit image becomes a 9 bit image. More MSB means lesser is the impact of the LSB bits manipulation meaning grater volume of message can be embedded in the cover image.[10][11]
We decided to use Seam craving as it is an content aware image resizing technique that allows resizing of image irrespective of aspect ratio and maintains the original nature of the image.[15][16]

i. The top image is the original image and bottomimage is the resized image. The overall size of the image is increased.
ii. Since the technique uses content aware scaling toresize the image the final image looks the sameas the original image with all the featuresretained.
iii. We can along adjust the aspect ratio using this technique.
iv. Since the final image is almost double in size the number of bits is increased by 1.

Now we work on the message that is to be hidden.

B. DCT Compression

The Message that is needed to be embedded is compressed so that the message when embedded in the cover image it alterthe cover image to the least [22][23].

Figure 1: Size comparison before and after Image resizing

DCT is a lossy compression technique that offers an average compression ratio (64:5). It is easy to implement and can be programmed in matlab [19][20]

i. DCT compresses the large message into a smaller form.
ii. Files are compressed to such a limit that the message isn't alter.
iii. The integrity of the message can be checked using MD5 algorithm.
iv. DCT can be implemented in python as well a java.
v. After the compression the message can be embedded in the cover image using the LSB technique.
vi. Since the size of the image is now greater (two or four times the original resolution) we can embedded a larger message than the original image would have allowed.

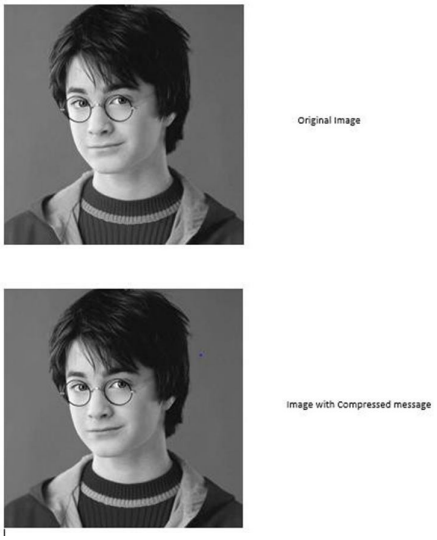
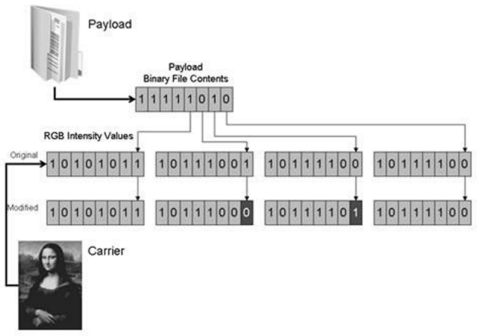


Figure 2: Bottom image is embedded with large compressed message

C. LSB Steganography

It is a type of steganography where the message bits are embedded in the lower order bits of the image. This is doneas the lower bits have the least impact on the features of the image thus allowing us to store our message without significant loss of details[5][6].

If more bits of higher order are tampered during embedding processes the image will start to lose its features and thus making it obvious that the image was tampered [22].



IV. Enhancement in Security

The security can be further enhanced by encrypting the stego image using AES so that only the receiver can access the message.
AES is a secure cryptographic technique that allows us to share the file safely. It is a symmetric cryptographic technique that uses a secret key for encryption and decryption.

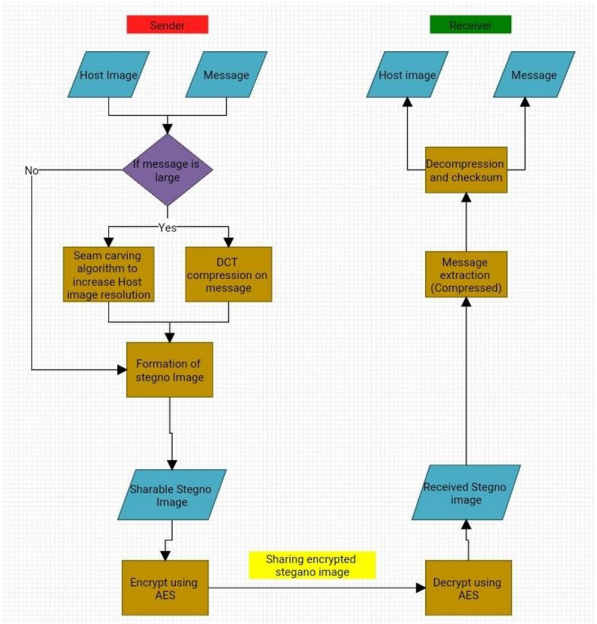


Figure 3: Complete Steganographic Procedure

V. Result & Discussion

We can see that using a compression algorithm and a resizing algorithm can vastly impact our Steganographic system. Not only we can store a larger amount of data in the same image but also we can retain maximum features of the original image after the embedding process.

VI. Conclusion

It is clear that steganography is a viable solution in the world of data hiding. Our model is capable of up scaling the cover image resolution and compressing the message to enable data of a larger size to be hidden in the cover image.
Seam craving is a content aware technique for image up scaling that allows us to resize the image up to n times the original resolution while DCT compression is an easy to implement compression technique to allow message to compress at an average compression ratio.

Our Model allows us to select the cover image and message to form a stego image and share it using AES. Without knowing the key the receiver or the intermediate person wouldn't be able to open the hidden message.

REFERENCES

[1] Deepthi K Prasad , Vibha , Venugopal K R, Early Detection of Diabetic Retinopathy from Digital Retinal Fundus Images, 2015.

[2] Darshit Doshi ,Aniket Shenoy ,Deep Sidhpura Diabetic Retinopathy Detection using Deep Convolutional Neural Networks, 2016.

[3] S.D. Shirbahadurkar, V. M. Mane , D. V. Jadhav. A Modern, 2017.

[4] Approach to Detection of Diabetic Retinopathy. Avula Benzamin , Chandan Chakraborty. Detectionof Retinal Fundus Images using Deep Learning,2018.

[5] Xianglong Zeng, Haiquan Chen, Yuan Luo & Wenbin Ye. Automated Diabetic Retinopathy Detection Based on Binocular Siamese, 2019

[6] S. Choudhury, S. Bandyopadhyay, S. K. Latib, D. K. Kole, C. Giri. "Fuzzy C means based feature extraction and classification of diabetic retinopathy using supportvector machines", 2016 International Conference onCommunication and Signal Processing (ICCSP), 2016

[7] R. Casanova, S. Saldana, E. Y. Chew, R. P. Danis, C. M. Greven, and W. T. Ambrosius, "Application of random forests methods to diabetic retinopathy classification analyses," Plos One, vol. 9, no. 6, p. e98587, 2014.

[8] Kaggle, "Diabetic retinopathy detection," https://www.kaggle.com/c/diabetic-retinopathy-detection/, July 27, 2015, accessed May 7, 2018.

[9] V. Gulshan, L. Peng, M. Coram, M. C. Stumpe, D. Wu, A. Narayanaswamy, S. Venugopalan, Widner, T. Madams, and J. Cuadros, "Development and validation of a deep learning algorithm for detection of diabetic retinopathy in retinal fundus photographs." Jama, vol. 316, no. 22, p. 2402, 2016.

[10] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, The Journal of Machine Learning Research, vol. 15, no. 1, pp. 1929–1958, 2014.

[11] S. Chopra, R. Hadsell, and Y. LeCun, "Learning a similarity metric discriminatively, with application to face verification," in Computer Vision and PatternRecognition, vol. 1, pp. 539–546,2015.

[12] S. R. Flaxman, R. R. Bourne, S. Resnikoff, P. Ackland, T. Braithwaite, M. V. Cicinelli, A. Das, J. B. Jonas, J. Keeffe, J. H. Kempen et al., "Global causes of blindness and distance vision impairment 1990–2020: a systematic review and meta-analysis," The Lancet Global Health, vol. 5, no. 12, pp. e1221–e1234, 2017.

[13] G. Quellec, K. Charria"Re, Y. Boudi, B. Cochener, and M. Lamard, "Deep image mining for diabetic retinopathy screening," Medical Image Analysis, vol. 39, pp. 178– 193, 2017.

[14] O. Hosam, N. Ben Halima, Adaptive block-based pixel value differencing steganography, Secur. Commun. Scheme. Networks 9 (2016) 5036–5050, doi: 10.1002/ sec.1676.

[15] Bentley, J. L., Sleator, D. D., Tarjan, R. E.,and Wei, V. K. 1986. A Locally Adaptive Data Compression Commun. ACM 29, 4 (Apr.), 320-330.

[16] A. Cheddad, J. Condell, K. Curran, P. Mc Kevtt, "Digital image steganography: survey and analysis of current methods", Signal Processing 90 (2010) 727–752, doi: 10.1016/j.sigpro.2009.08.010 .

[17] Anitha S," Image Compression Using Discrete Cosine Transform & Discrete Wavelet Transform", Volume 2 Issue 8 August 2011.

[18] Assaf Zomet, Anat Levin, Shmuel Peleg, andYair," Seamless Image Stitching by MinimizingFalse Edges", Volume 15 Number 4 April 2006.

[19] Swagota Bera , , Dr. Monisha Sharma ," Feature Weiss Feature Extraction and Analysis using Gabor Filter and Higher Order Statistics for the JPEG Steganography",Volume 13, Number 5 (2018) pp.2945-2954.

[20] Sumit Kumar Moudgil, Dr. Amit Kumar Goel,Dr.Manish Sharma,"Steganography on Audio Wave Tenth Layer by Using Signal to Noise RatioTest and Spectrogram Analyses",Volume 13 , November 4.

[21] Singh, Arun Kumar, Juhi Singh, and Harsh Vikram Singh. "Steganography in images using lsb technique." *International Journal of Latest Trends in Engineering and Technology (IJLTET)* 5.1 (2015): 426-430.

[22] Kumar, Singh Arun, Singh Juhi, and Singh Harsh Vikram. "DCT-and DWT-Based Intellectual Property Right Protection in Digital Images." *First International Conference on Artificial Intelligence and Cognitive Computing*. Springer, Singapore, 2019.

[23] Singh, Arun Kumar, Harsh Vikram Singh, and Juhi Singh. "Highly Impartible Spatial Domain Steganography in Double Precision Images." *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE, 2018.

[24] V. K. 1986. A Locally Adaptive Data Compression Scheme. Networks 9 (2016) 5036–5050, doi: 10.1002/ sec.1676 Commun. ACM 29, 4 (Apr.), 320-330.