ITERATIVE HAAR-DWT BASED EFFICIENT IMAGE STEGANOGRAPHY

Aditi Singh[*1], K S Venkatesh[2] and Vikas Patidar[3]

Department of Electrical Engineering,
Indian Institute of Technology Kanpur, Kanpur-208016, Uttar Pradesh, India

ABSTRACT

In image steganography, the transfer domain provides better concealment of the secret image in the cover image, and has therefore proved much more reliable than spatial domain. In this paper, we attempt to maximize the retrieved secret PSNR against the original secret, while simultaneously minimizing the cover image degradation. This paper is built upon Discrete-Wavelet Transform to process the image while the Least Significant Bit method to store the information. We follow a principle of priority ordering the wavelet subspaces of both the secret and the cover with a view to make for the most efficient concealment. We propose the product of the secret and cover image PSNR and SSIM measures as the quantities to be maximized as it provides a more comprehensive evaluation of system performance, and study the performance against the choice of the number of levels of wavelet decompositions.

KEYWORDS

Cover; Secret; Stego; Embed; HAAR-DWT; LSB

1. INTRODUCTION

Labeling a message to be of high security will make it a high priority target for attacks. Likewise, enciphered messages always hold the risk of being discovered on route. Moreover, such messages can altogether be destroyed/tampered by a third party, if not decrypted successfully. Thus, the secrecy of transmission of such messages becomes important and here is where steganography takes over cryptography. Steganography, or image hiding, avoids overt declaration of the criticality of a message, by concealing the secret (image) in a mundane cover (image) so that its significance is known only to the intended recipient.

When the cover for embedding secret information is an image, the technique is referred to as Image Steganography. Any kind of signal can be stored into the cover; here, we hide a secret image: The secret image is embedded into the cover image resulting in the so called stego image. The recipient extracts the secret information out of stego image and gets the message. We use the Least Significant Bit (LSB) method to store the information, wherein the secret information is encoded in the least significant bits of the pixels of the cover image. The number of least significant bits used for this purpose varies as per application and the level of fidelity desired. Needless to say, a requirement of higher fidelity conflicts with a requirement of higher capacity.

David C. Wyld et al. (Eds) : IPPR, SOENG, DaMi, CSIT, AIS, CSE, CSIP, CCNET - 2018
pp. 11–24, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.80502

In this paper, we compare two approaches: the first one using only two least significant bits of the cover to store the secret information while the other uses three. While the second provides more capacity, (i.e., more space), the first one leads to a higher cover-stego PSNR as well as SSIM.

In frequency domain approaches, both cover and secret are transferred to the transform domain and the transform coefficients of the secret are embedded in the transform coefficients of the cover to get a transform domain stego. This transform domain stego is converted back to the spatial domain by inverse transforms to get the spatial domain stego image. At the recipient end, to extract the secret information, one has to again perform the respective transform and extract the secret information from LSB of the coefficients. Also, the information of in how many and which coefficients the data is being embedded also needs to be recorded and transmitted. The conversion to the frequency domain helps because the human eye cannot detect changes in the high frequency while changes made in the low frequency can easily be detected. The concealment in the frequency domain spatially spreads the secret data over all the transform coefficients, preventing the retention.

The method used in this paper is a combination of LSB and iterative HAAR-DWT. We prioritize the space (the part where any changes can be least detected) in the cover image and energy in the secret image. Next comes the tradeoff between the amount of secret information being stored and similarity of the stego to the cover image. We observe results in terms of PSNR and SSIM, aiming for the most efficient solution, and state some problems that arise because of using HAAR-DWT.

2. BACKGROUND

The LSB method has been implemented after processing both the cover and secret images in various ways over the decades, for e.g., directly storing the secret image in LSB of cover image in spatial domain itself [1], performing DCT [2] or DWT [3] or DFT [4] on the cover image to convert it into frequency domain and then storing the information is LSB of respective coefficients.

Chandramouli and Memon [5] (2001) devised a method to calculate probability of detection in terms of number of bits hidden for storing information. Morkal, Tayana, et al [6] (2005) stated the applications and suitable uses of different steganographic techniques. Cheddad, Abbas, et al [7] (2010) have mentioned a state-of-the-art review and analysis of then existing steganography techniques. Similar work is done by Singh, Amritpal, et al. [8] (2014). Al-Korbi, Hamad A., et al [9] (2015) developed steganography technique storing information in the wavelet domain (RGB color). Vikas Patidar [3] (2016) developed a technique (monochrome/color) to store information in the HAAR-DDWT domain. We work on this base, performing HAAR-DWT iteratively on the image to better classify its wavelets as per the amount of information stored in them resulting in improved SSIM and PSNR performance. We also show there is a certain degree of permanent loss of information because of using HAAR-DWT with LSB method, making the entire process lossy. We state both the problem and reason of occurrence of this phenomenon.

3. HAAR-DWT

The HAAR wavelet is preferred because of its simple yet efficient decomposition process. It requires only simple addition/subtraction in horizontal and vertical directions to convert images

from spatial to frequency domain. For a 4x4 matrix, the HAAR transform can be evaluated as follows:

$$\begin{bmatrix} a1 & b1 & a2 & b2 \\ c1 & d1 & c2 & d2 \\ a3 & b3 & a4 & b4 \\ c3 & d3 & c4 & d4 \end{bmatrix}$$

$$\begin{bmatrix} a1+b1+c1+d1 & a2+b2+c2+d2 & a1-b1+c1-d1 & a2-b2+c1-d2 \\ a3+b3+c3+d3 & a4+b4+c4+d4 & a3-b3+c3-d3 & a4-b4+c4-d4 \\ a1+b1-c1-d1 & a2+b2-c2-d2 & a1-b1-c1+d1 & a2-b2-c2+d2 \\ a3+b3-c3-d3 & a4+b4-c4-d4 & a3-b3-c3+d3 & a4-b4-c4+d4 \end{bmatrix}$$

Figure 1. Calculation of HAAR-DWT of an image.

Thus, the HAAR transform, applied once, decomposes any image into four frequency regions as $\begin{bmatrix} LL & HL \\ LH & HH \end{bmatrix}$, named low-low, high-low, low-high and high-high, allowing us to make changes in the high frequency region leaving the low frequency region containing the most significant information, untouched. Similar inverse operations can be made on the HAAR-transform to get back our original image.

4. EMBEDDING ALGORITHM

'ns' = number of times HAAR-DWT is desired to be done in secret, 'x' =($size\ of\ cover$)/ ($size\ of\ secret$), where both these are square images and size means any one side, 'nc' =4^($n - (log2x) - 1$), 'm' = number of final level secret image wavelets desired to be stored.

4.1 Hiding All Bits of Secret Information:

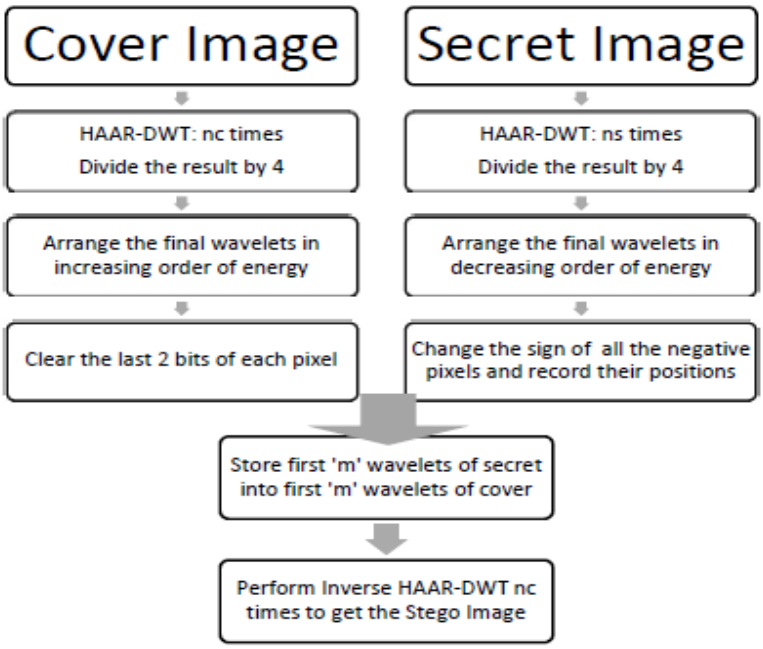

Figure 2. (First) Embedding Algorithm

4.2 Hiding First Six Non-Zero Bits of Secret Information:

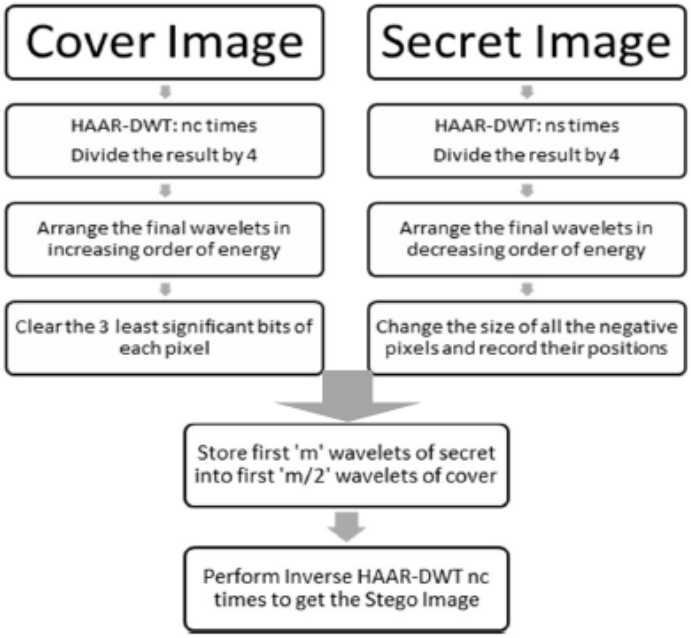

Figure 3. (Second) Embedding Algorithm

5. EXTRACTING ALGORITHM

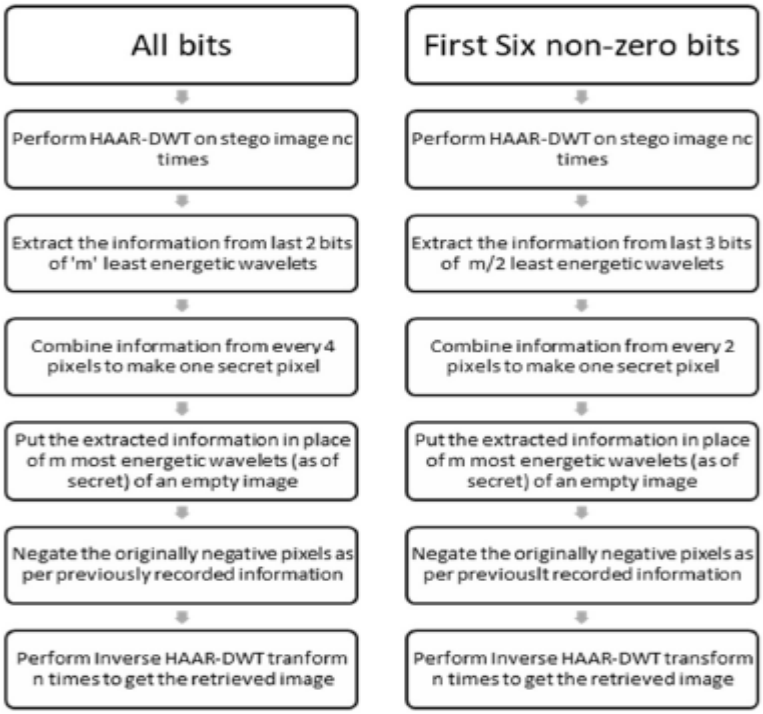

Figure 4. Extracting Algorithm

6. OBSERVATIONS AND RESULTS

To decide the optimum value of 'm' for a given 'n', we study the product of the PSNRs and SSIMs of coverstego pair and secret-retrieved image pair [10][11]. The results are shown for n = 1, 2 *and* 3 (i.e. up to 3 levels of HAAR-DWT) each for both the cases of storing all bits and storing first six non-zero bits.

6.1 First Example

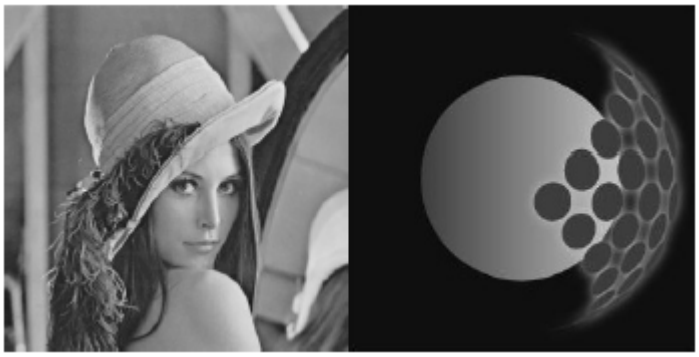

Figure 5. Cover (left) and Secret Image

6.1.1. 'n' = 1

The PSNR and SSIM trend on storing m = 1: 4 wavelets of secret image (on horizontal axis):

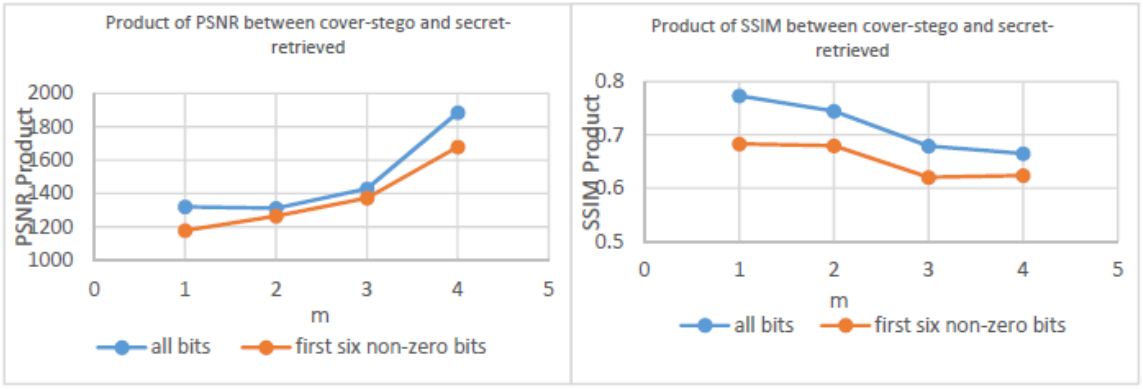

Figure 6. PSNR (left) and SSIM Product for 'n' = 1

6.1.2. 'n' = 2

The PSNR and SSIM trend on storing m = 1: 16 wavelets of secret image (on horizontal axis):

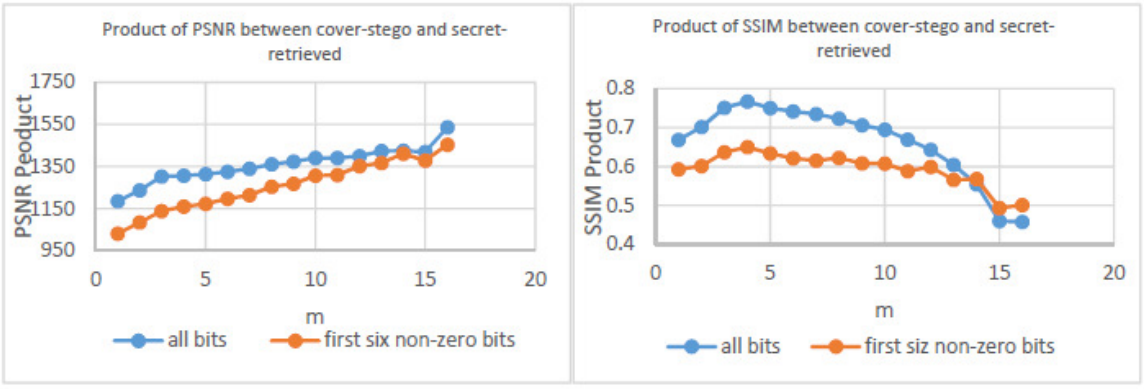

Figure 7. PSNR (left) and SSIM Product for 'n' = 2

Figure 8. Stego (left) and Retrieved Secret Image (m = 4)

6.1.3. 'n' = 3

The PSNR and SSIM trend after storing m=1:64 wavelets of secret image (on horizontal axis):

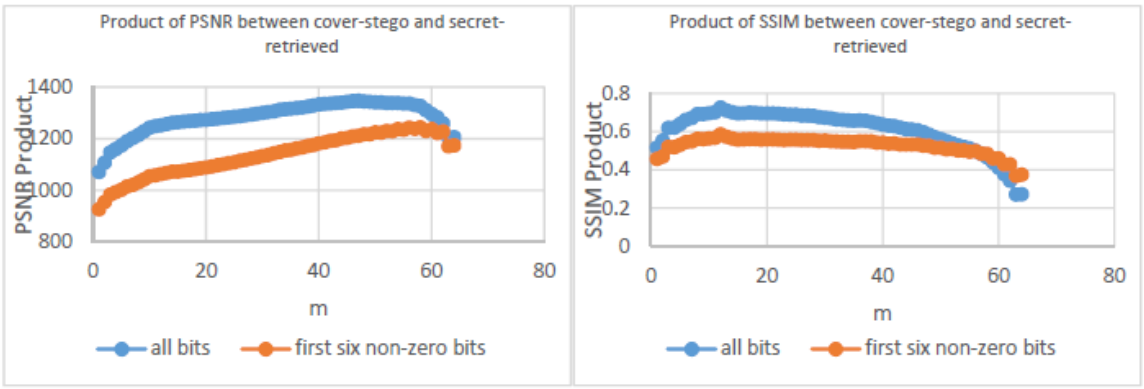

Figure 9. PSNR (left) and SSIM Product for 'n' = 3

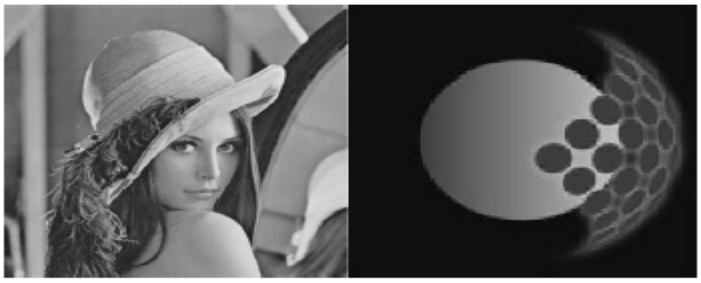

Figure 10. Stego (left) and Retrieved Secret Image (m = 12)

Since the question here is of how similar the retrieved secret image is to the original secret image and how similar the stego image is to the cover image, we will follow the product of SSIM to get our optimum solution. Also, both PSNR and SSIM product are higher when we resort to storing all bits, as compared to storing only the first six non-zero bits in spite of increased storage capacity in the cover image. The results for optimum values of 'm' (as per SSIM) are also shown in each sub-section above.

6.2 Second Example

Figure 11. Cover (left) and Secret Image

6.2.1. 'n' = 1

The PSNR and SSIM trend on storing m = 1: 4 wavelets of secret image (on horizontal axis):

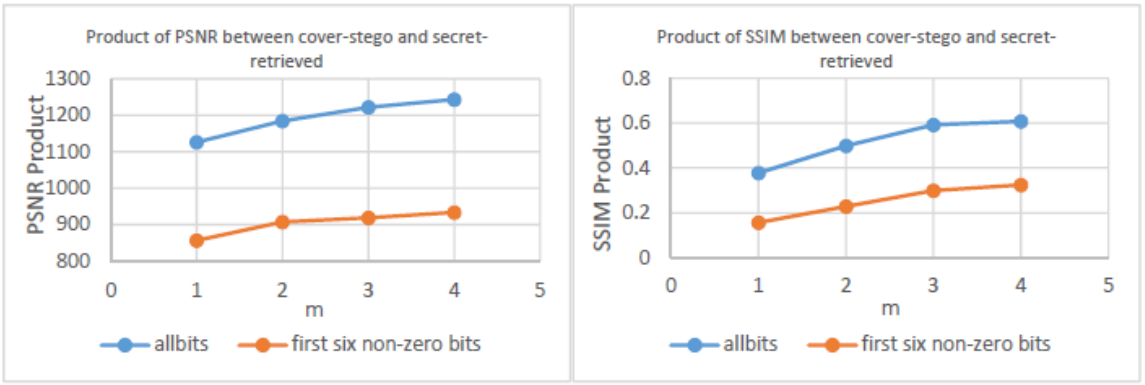

Figure 12. PSNR (left) and SSIM Product for 'n' = 1

6.2.2. 'n' = 2

The PSNR and SSIM trend on storing m = 1: 16 wavelets of secret image (on horizontal axis):

Figure 13. PSNR (left) and SSIM Product for 'n' = 2

Figure 14. Stego (left) and Retrieved Secret Image (m = 8)

6.2.3. 'n' = 3

The PSNR and SSIM trend after storing m=1:64 wavelets of secret image (on horizontal axis):

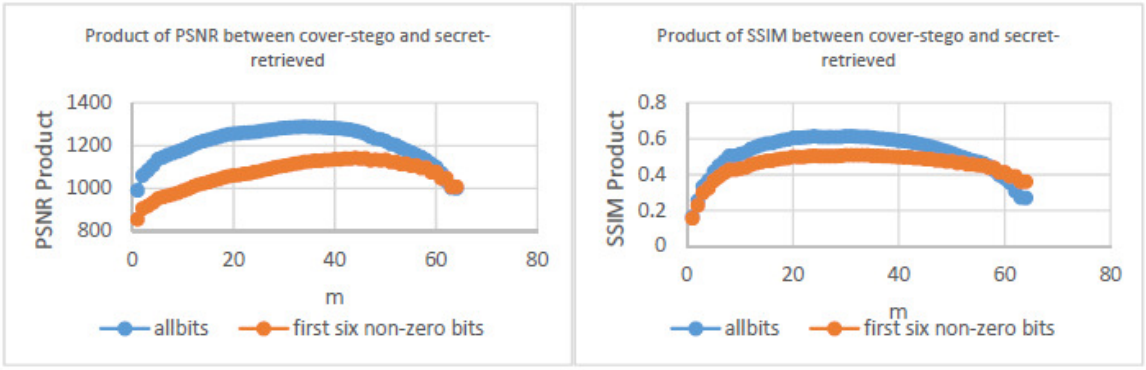

Figure 15. PSNR (left) and SSIM Product for 'n' = 3

Figure 16. Stego (left) and Retrieved Secret Image (m = 28)

6.3 Third Example

Figure 17. Cover (left) and Secret Image

6.3.1 'n' = 1

The PSNR and SSIM trend on storing m = 1: 4 wavelets of secret image (on horizontal axis):

Figure 18. PSNR (left) and SSIM Product for 'n' = 1

6.3.2 'n' = 2

The PSNR and SSIM trend on storing m = 1: 16 wavelets of secret image (on horizontal axis):

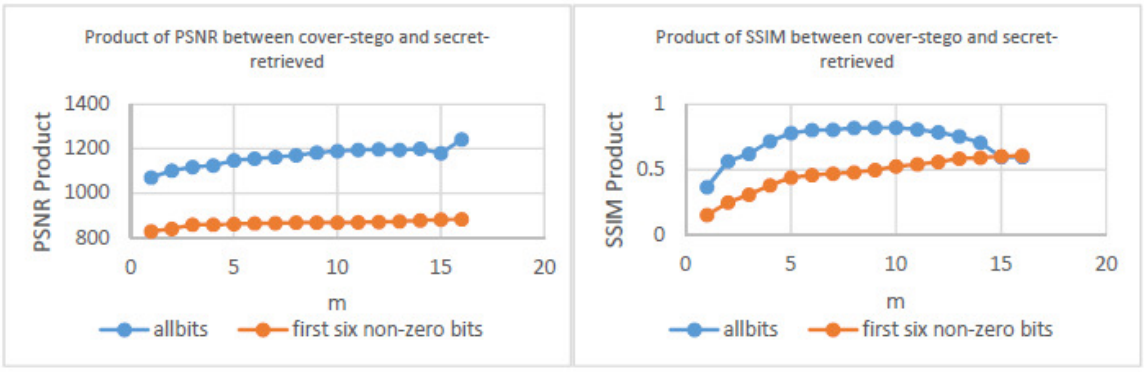

Figure 19. PSNR (left) and SSIM Product for 'n' = 2

Figure 20. Stego (left) and Retrieved Secret Image (m = 10)

6.3.3 'n' = 3

The PSNR and SSIM trend after storing m=1:64 wavelets of secret image (on horizontal axis):

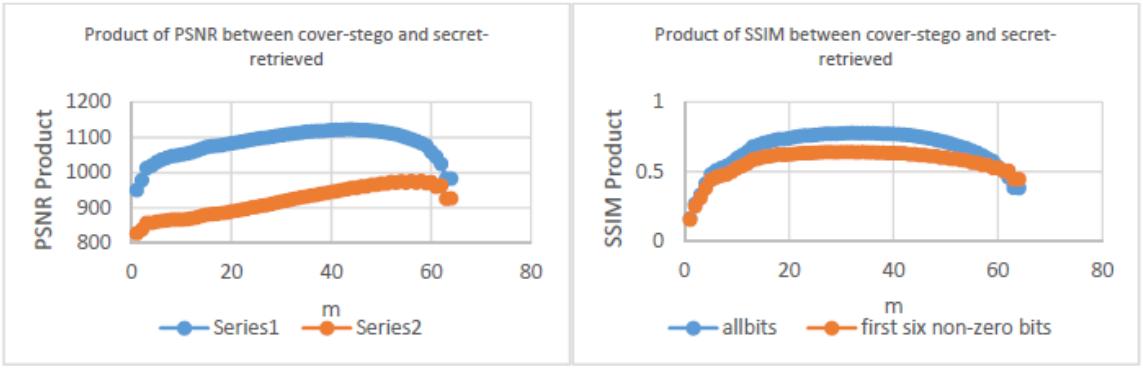

Figure 21. PSNR (left) and SSIM Product for 'n' = 3

Figure 22. Stego (left) and Retrieved Secret Image (m = 35)

6.4 Average Result

We run the algorithm on a total of 10 cover-secret image pairs and plot the average results as follows:

6.4.1. 'n' = 1

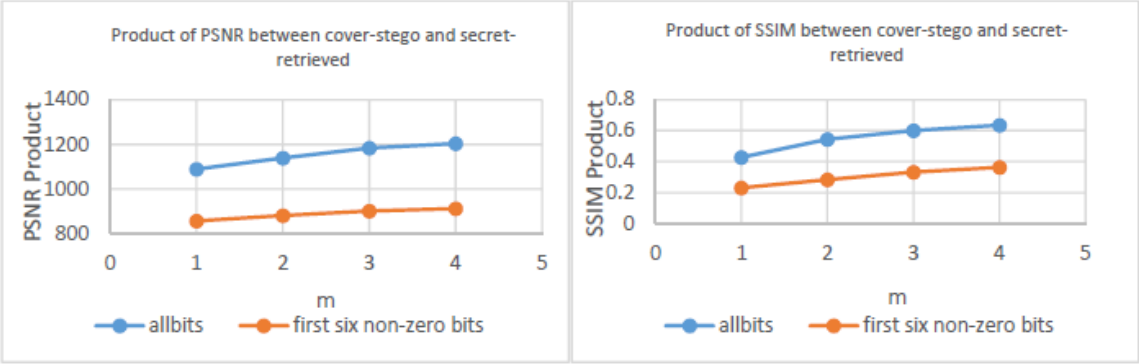

Figure 23. PSNR (left) and SSIM Product for 'n' = 1

6.4.2. 'n' = 2

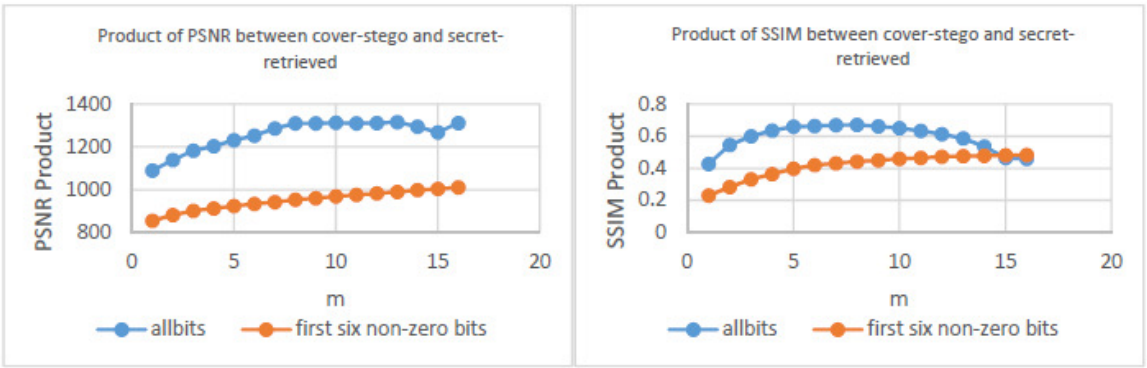

Figure 24. PSNR (left) and SSIM Product for 'n' = 2

6.4.3. 'n' = 3

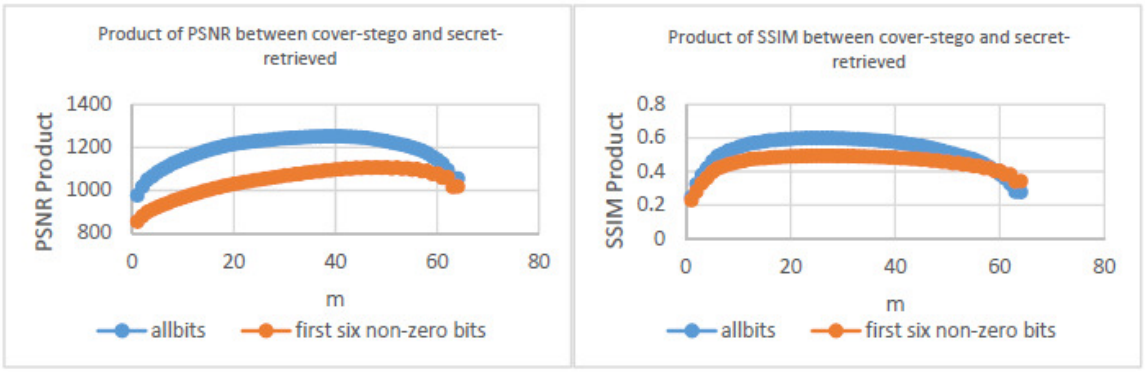

Figure 25. PSNR (left) and SSIM Product for 'n' = 3

7. SHORTCOMINGS

The procedure of evaluating the HAAR transform of an image includes addition as well as subtraction of pixel values as mentioned previously. This subtraction leads to some negative pixel values in the resulting wavelet transform which causes problems in both display of the image, and decimal to binary conversion required for application of the LSB method of embedding. To tackle this, one must record the position of all negative pixels in the transform and then temporarily assign them positive signs before converting them into binary for storing. After extracting the wavelets of the secret image from the stego, the sign of these pixel values should be restored before performing Inverse-HAAR to get the retrieved image.

The LSB method requires the pixel values to be in the range [0,255] for it to be convertible into 8-bit integers for further procedure. Consequently, we need to keep dividing the result by 4 every time we perform HAARDWT. This makes some of the resulting pixel values to be non-integers, which are subsequently rounded off when converted to 8-bits. This rounded-off information is lost forever. Therefore, even on storing the all the wavelets of the secret image, the retrieved secret doesn't show a perfect SSIM of 1 with respect to the original secret. It can also be observed in many cases, but not all, that the PSNR product has started decreasing at the end of the third level which tells us not to go any further in HAAR-DWT levels (since, every time the size of each wavelet is becoming a fourth smaller with increasingly coarser approximation due to quantization error).

8. CONCLUSION

This paper presents a steganography technique using the LSB method. Encoding the secret image in transfer domain, rather than in spatial domain, and that too at different levels (i.e., after iteratively performing HAARDWT) with number of wavelets stored prioritizing their energy, we have found the optimum values of SSIM between cover-stego and secret-retrieved image by seeing the trend on varying the number of wavelets of the secret image being stored. We have also listed the shortcomings of this approach which increases the space complexity of the code, and besides increases the quantization error further. Like every other steganography technique,

ours also has its advantages as well as shortcomings and can be fine-tuned as per the application it is to be used in.

REFERENCES

[1] R. K. Thakur and C. Saravanan, "Analysis of steganography with various bits of LSB for color images," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016

[2] K. Raja, C. Chowdary, K. Venugopal, and L. Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images," 2005 3rd International Conference on Intelligent Sensing and Information Processing, 2005.

[3] Vikas Patidar, "Techniques of Image Concealment," M.Tech Thesis, Indian Institute of Technology Kanpur, Kalyanpur, Uttar Pradesh, India, 2016.

[4] D. Bhattacharyya and T.-H. Kim, "Image Data Hiding Technique Using Discrete Fourier Transformation," Communications in Computer and Information Science Ubiquitous Computing and Multimedia Applications, pp. 315–323, 2011.

[5] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Proceedings 2001 International Conference on Image Processing (Cat. No.01CH37205).

[6] Morkel, T., Eloff, J. H., & Olivier, M. S. 2005, "An overview of image steganography," ISSA, pp. 1-11, 2011.

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

[8] Singh, A., & Singh, S. J. 2014, "An Overview of Image Steganography Techniques," International Journal of Engineering and Computer Science, vol3, (7), 7341-7345, 2014.

[9] H. A. Al-Korbi, A. Al-Ataby, M. A. Al-Taee, and W. Al-Nuaimy, "High-capacity image steganography based on Haar DWT for hiding miscellaneous data," 2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT), 2015.

[10] SIPI Image Database. [Online]. Available: http://sipi.usc.edu/database/. [Accessed: 07-Feb-2018].

[11] "Free high quality photos · Pexels," Free Stock Photos. [Online]. Available: https://www.pexels.com/. [Accessed: 07-Feb-2018].

[12] "Bilinear interpolation Definition from PC Magazine ...", [Online]. Available: https://www.pcmag.com/encyclopedia/term/38607/bilinear-interpolation. [Accessed: 5- Feb- 2018].

[13] "Understanding Digital Image Interpolation", Cambridgeincolour.com, 2018. [Online]. Available: https://www.cambridgeincolour.com/tutorials/image-interpolation.htm. [Accessed: 05- Feb- 2018].

[14] A. Bogomolny, "Equations of a Straight Line from Interactive Mathematics Miscellany and Puzzles", Cutthe-knot.org, 2018. [Online]. Available: https://www.cut-theknot.org/Curriculum/Calculus/StraightLine.shtml. [Accessed: 05- Feb- 2018].

[15] "High-Resolution Antialiasing|NVIDIA", Nvidia.com, 2018. [Online]. Available: http://www.nvidia.com/object/feature_hraa.html. [Accessed: 05- Feb- 2018].

[16] "Hardware Knowledgebase - What is supersampling (antialiasing technique)? - HardwareFAQs: powered by neofaq", Web.archive.org, 2018. [Online]. Available: https://web.archive.org/web/20060325144730/http://www.neoseeker.com/Hardware/faqs/kb/10,72.html. [Accessed: 05- Feb- 2018].

[17] "Supersampling - Everything2.com", Everything2.com, 2018. [Online]. Available: http://www.everything2.com/index.pl?node_id=1028947. [Accessed: 05- Feb- 2018].

[18] P. Getreuer, "Image Interpolation with Contour Stencils", 2018. [Online]. Available: http://www.ipol.im/pub/art/2011/g_iics/. [Accessed: 05- Feb- 2018].

AUTHORS

Aditi Singh – Undergraduate Student, IIT Kanpur; Research Interests - Image and Video Processing, Computer Graphics. Webpage – http://home.iitk.ac.in/~aditisgh/

K S Venkatesh – Professor, IIT Kanpur; Research Interests - Signal, Image and Video Processing with applications in Computer Vision, Machine Vision, Computational Photography and Medical Imaging; Robot Navigation. Webpage - http://home.iitk.ac.in/~venkats/

Vikas Patidar – Former Master's Student, IIT Kanpur