

BIOMEDICAL IMAGE AUGMENTATION AND TRANSMISSION USING STEGANOGRAPHY

CHIRAG SATAPATHY, HRISHIKESH GOKHALE

School of Electrical Engineering (SELECT), Vellore Institute of Technology, Vellore, Tamil Nadu, India. Email: chiragsatapathy@gmail.com, hrishikesh.gokhale04@gmail.com

Received: 14 May 2022, Revised and Accepted: 25 July 2022

ABSTRACT

Objective: The aim of the study was to embed sensitive patient information and image data in a cover image to enable secure transmission of confidential data.

Methods: Image steganography is a process used to embed (hide with encryption) data which includes text, images or audio, and video files inside the main image file. This embedding is done by altering the values of some pixels which are chosen by the encryption algorithm. The algorithm used in this case is the Discrete Wavelet Transformation Algorithm using MATLAB.

Results: Statistical features such as signal to noise ratio (SNR), Peak SNR, and (mean squared error) were extracted from the medical images to test the loss during steganography and transmission.

Conclusion: A technique that enables secure and swift image data transmission using image steganography technique is proposed.

Keywords: Augmentation, Confidential, Image steganography, Discrete wavelet transform, MATLAB.

© 2022 The Authors. Published by Innovare Academic Sciences Pvt Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>) DOI: <http://dx.doi.org/10.22159/ajpcr.2022v15i11.45205>. Journal homepage: <https://innovareacademics.in/journals/index.php/ajpcr>

INTRODUCTION

Biomedical imaging is a power technique that helps in identifying and visualizing internal organs of a living body [1] and also captures images for both therapeutic and diagnostic purposes. It also offers precise tracking of various diseases that the body is affected with and thus can help in accurate, precise, and timely treatment of these diseases. Biomedical images that are generated by the X-rays, computed tomography (CT) scans, or magnetic resonance imaging often help in disease identification and also help doctors to start treatment to cure these diseases as soon as possible.

It sometimes so happens that when the X-ray images are transmitted from one computer to another in the hospitals, it might be under attack by hackers who steal patient information from these medical scans. This potential loss of data is a major threat to the privacy of patients, hospitals staff, corresponding families, and also financial institutions. To prevent loss of data, we have designed a user-to-user software on MATLAB to help in secure transmission of these images using a practiced technique called STEGANOGRAPHY. Steganography is an image hiding technique [2] that helps to hide or conceal secret data in the form of text message, image, or video into another file, message or video. We have concealed image with text and then followed by image with image to make image transmissions as secure as possible.

Every medical scan of a patient is private to the patient itself and also the hospital. With every scan, there is a patient information attached to it, such as patient name, age, gender, family information, doctor assigned, diagnostic given, and treatments specified. To facilitate steganography, we have embedded patients details with their personal profile to these biomedical images using least significant bit (LSB) algorithm and HAAR wavelet transform (HWT) Algorithm.

HWT

In the HWT technique, data are hidden in the frequency domain. This is done because the frequency domain is the most robust area. To avoid the loss of data from the floating point, the embedding is done in the integer part of the transform coefficients. This is done in such a way that it increases both, the imperceptibility and the capacity of hiding [3].

LSB

According to the LSB embedding approach, data can be concealed in the cover picture's LSBs, and the human eye would be unable to detect the hidden image in the cover file. This technique is used for embedding images in 24-bit, 8-bit, or gray-scale format [4].

METHODS

There are two main parts in the process of performing the secure transmission of these biomedical images from one user to another, they are as follows.

Image augmentation

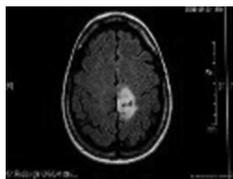
Hence, it considers an image of a CT scan of the human brain. It is found out that there is a tumor in the back of the head causing the person to be unstable while walking. However, to gather multiple angled views of the tumor, image augmentation is performed. The two most common ones being rotation and flips. Rotation and flips performed on biomedical images have helped medical professional to look at the tumors from every angle and side possible so that deducing the type of the tumor and cure for the tumor will be as accurate as possible. Multiple of these rotation and flips are performed taking into consideration various angles and a complete dataset of all these images can be formed which can further help in creating a machine learning or deep learning models to help in more accurate detection of these tumors.

Image steganography

As said earlier, image steganography in simple terms hides secret data or text into another image or text. After image augmentation of patient's medical scans, these personal data are hid inside the image before transmitting it from the imaging room to the doctor. This helps in keeping the patient's privacy by hiding their data using encryption algorithms and also helps to facilitate quick and timely transfer of all relevant medical images. We are using the HWDT to hide data. HWDT aims to decrease the complexity of image steganography technique while providing less image distortion and lesser detectability [5].

All the images before transmission are converted from (red green blue - color images) to GRAY images. To check the quality of the images

Table 1: Tabulated parameter values

Images	Secret text	PSNR	MSE	SNR
 Medical image of the patient (Stegano image)	Patient Mr.Boat, age 65 years, male, has been diagnosed with meningioma stage one. He is advised to start radiation therapy immediately	21.1117	82.4543	19.3319
 Main cover image (hospital logo)	NA	NA	NA	9.8065
Flower.jpeg [10]	NA	47.9688	5.67965e + 04	NA

PSNR: Peak signal-to-noise ratio, MSE: Mean square error, SNR: Signal to noise ratio

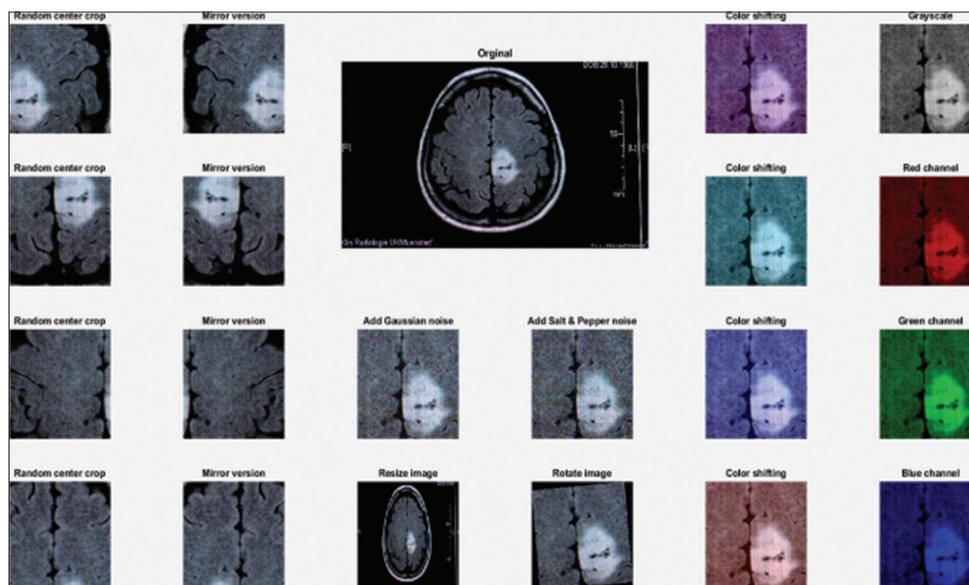


Fig. 1: Image augmentation on brain tumor image

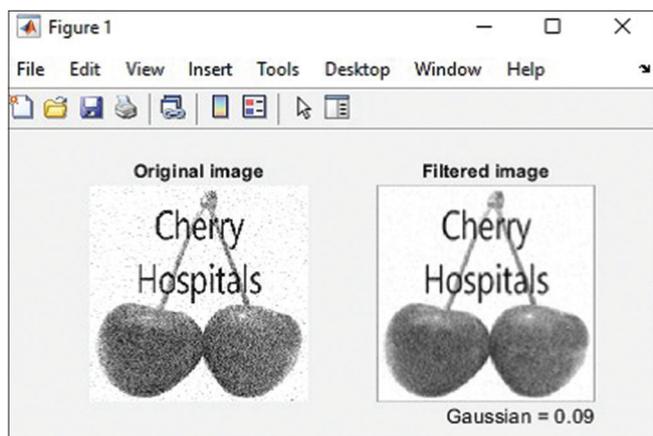


Fig. 2: Original and filtered Gaussian images

obtained at the receiving end, multiple parameters are used to evaluate the strength and accuracy of the algorithm which are peak SNR (PSNR), mean square error (MSE), and signal-to-noise ratio (SNR) of both the main and steganography image.

First, the original image, which is the logo image of the hospital, is taken into consideration. The original image is introduced with Gaussian noise to calculate the PSNR of the noisy image while keeping the original image as a reference. We have used a Gaussian noise of 0.09. This noise will be removed from the original image after obtaining the filtered image. In the first stage, patient's data are embedded into the medical image (X-ray of the patient) using HAAR Wavelets transform which divides the data into packets of wavelets. Then, in the next stage, the medical image of the patient is embedded into the main image (logo of the hospital) using the technique of LSB [6]. This is the second and final stage of securing the image with encryption. All these processes take place at the sender's end.

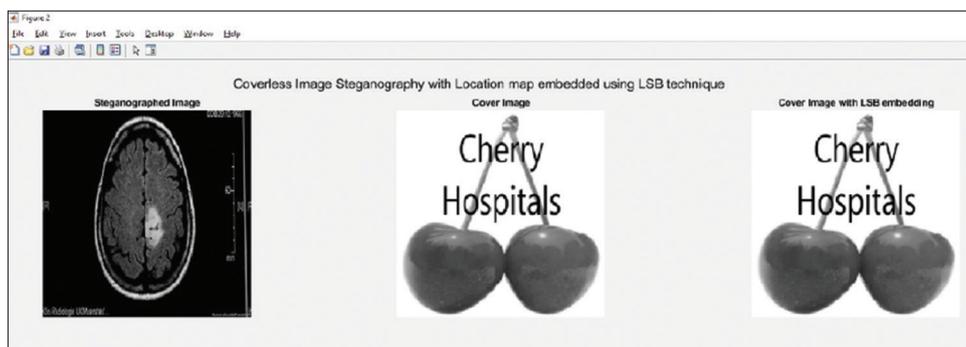


Fig. 3: Image steganography using LSB embedding technique

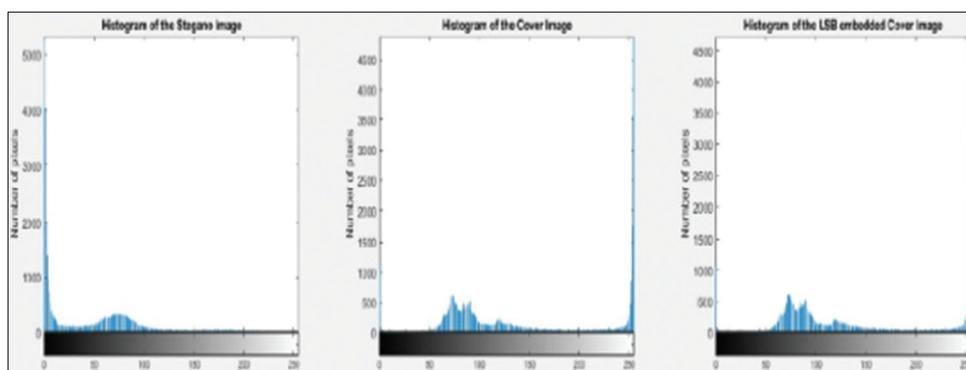


Fig. 4: Histogram statistics of the given images

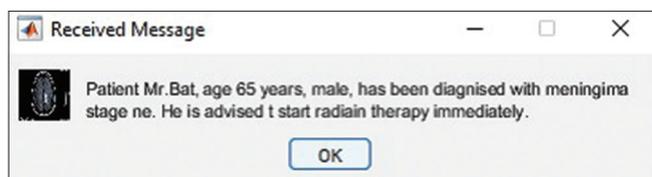


Fig. 5: Recovered image with HAAR WT decoding

Finally, at the receiver’s end, the encrypted images have to be decrypted so that the medical image and patient’s personal information can be recovered. The cover image (X-ray image) embedded with the secret text (patient’s data) can be decoded by the receiver. A dialogue box with the received text will pop up in MATLAB.

RESULTS AND DISCUSSION

Fig. 1 shows the various augmentation techniques applied to the brain tumor scan of a patient [7] such as addition of various noise models (Gaussian, salt and pepper noise), color shifting, cropping, and mirroring the image to create an image dataset to further train machine learning models in the future.

Fig. 2 shows the original image with Gaussian noise of 0.09 and also the filtered image after removing the noise. This helps to calculate the SNR value of the original image.

The performed image steganography snippet of the project using LSB embedding technique is shown in Fig. 3. There are three images that can be seen are – steganographed image which is of brain tumor and is embedded with a text, second is the main or cover image of the hospital’s logo (cherry hospitals), and finally the third image is the cover image with LSB embedding [8,9].

Fig. 4 represents the histogram statics of the three images. From the first histogram, we can deduce that the image obtained is darker in shade, from the second, we deduce that the image is bright with less

contrast and finally from the third histogram, we deduce that the image is a high contrast image. The message recovered using HWT is observed in Fig. 5.

There are few letters that have been lost during transmission but the overall message can be understood by the receiving user. The tabulated results of our proposed technique are shown in Table 1.

From the table, we can see that the PSNR values obtained by our technique are almost half of that obtained by the author Vijay through his proposed technique [10]. Furthermore, the MSE value obtained is extremely less that author Vijay’s obtained value.

CONCLUSION

Using image augmentation and steganography techniques, we have embedded both, a small text message that describes the patient’s condition and possible treatments, and the secret image of the patient’s X-ray which can be only accessed by authorized personnel. To embed the text into the image, we have used HWTs and to embed the text based hidden image into the cover image, we have used LSB embedding.

The application of these techniques facilitates secure storage and transmission of sensitive messages or images in the hospital data storage system. This reduces the risk of cyber criminals accessing and obtaining sensitive patient information.

AUTHOR’S CONTRIBUTION

All the authors have contributed equally to the article.

CONFLICTS OF INTEREST

No conflicts of interests.

AUTHOR’S FUNDING

Nil.

REFERENCES

1. Weissleder R, Nahrendorf M. Advancing biomedical imaging. *Proc Natl Acad Sci U S A* 2015;112:14424-8. doi: 10.1073/pnas.1508524112, PMID 26598657
2. Johnson NF, Jajodia S. Exploring steganography: Seeing the unseen. *Computer* 1998;31:26-34. doi: 10.1109/MC.1998.4655281
3. Taouil Y, Ameur EB, Belghiti MT. New image steganography method based on haar discrete wavelet transform. *Adv Intell Syst Comput* 2017;287-97. doi: 10.1007/978-3-319-46568-5_30
4. Neeta D, Snehal K, Jacobs D. Implementation of LSB Steganography and its Evaluation for Various Bits. In: 1st International Conference on Digital Information Management. Vol. 2006. New Jersey: Institute of Electrical and Electronics Engineers; 2007.
5. Houssein EH, Ali MA, Hassanien AE. An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System. In: Federated Conference on Computer Science and Information Systems (FedCSIS). Vol. 2016; 2016. p. 641-4.
6. Dumitrescu S, Wu X, Memon N. On Steganalysis of Random LSB Embedding in Continuous-tone Images. In: Proceedings International Conference on Image Processing. New Jersey: Institute of Electrical and Electronics Engineers; 2022.
7. Brain Tumor Image. Available from: <https://www.dw.com/en/brain-tumors-in-children-when-all-that-matters-is-now/a-53725741>
8. Lu P, Luo X, Tang Q, Shen L. An improved sample pairs method for detection of LSB embedding. *Inf Hiding* 2004;116-27. doi: 10.1007/978-3-540-30114-1_9
9. Fridrich J, Long M. Steganalysis of LSB Encoding in Color Images. Latest Advances in the Fast Changing World of Multimedia IEEE International Conference on Multimedia and Expo ICME2000. Proceedings; 2000 (Cat. No. 00TH8532). New Jersey: Institute of Electrical and Electronics Engineers.
10. Sharma VK, Srivastava DK. Comprehensive data hiding technique for discrete wavelet transform-based image steganography using advance encryption standard. In: Lecture Notes in Networks and Systems. Singapore: Springer; 2017. p. 353-60.