

Comparison and Implementation of Biometric Inspired Digital Image Steganography

¹Rupa Maan, ²Lovneesh Bansal

^{1,2}Dept. of Computer Science, Bhai Maha Singh College of Engineering, Mukatsar, Punjab, India

Abstract

The recent progress in the digital multimedia technologies has offered many facilities in the transmission, reproduction and manipulation of data. However, this advancement has also brought the challenge such as copyright protection for content providers. In the present work, two techniques namely LSB and Biometric pattern (Skin tone) based steganography have been compared and result were evaluated on the basis of comparison of quality of image after embedding of data and change in PSNR value of the image.

This project is developed for hiding and store information in any image file by using biometric pattern. Biometric Steganography is presented that uses skin region of images in DWT domain for embedding secret data. This work also showed the results for skin detection which performed pretty well in this case for identifying the skin regions from the given image. By embedding data in only certain region (here skin region) and not in whole image security is enhanced. To evaluate quality of stego image after embedding the secret message, Peak Signal to Noise Ratio (PSNR) has been used. The performance in terms of capacity and PSNR (in dB) is demonstrated for this method.

From above results it is observed that this preserves histogram of DWT coefficients after embedding also. That is the main reason why there is not much visual difference between the cover image and embedded image. Performing biometric steganography offers respectable level of security. By adopting embedding algorithm that preserves histogram of DWT coefficients after embedding, prevents histogram based attacks.

Keywords

Biometric, LSB, Skin Tone, DWT

I. Introduction

Digital image watermarking provides copyright protection to image by hiding appropriate information in original image to declare rightful ownership [1]. In spatial domain, LSB modification algorithm has been implemented and the results have been produced for grayscale, RGB and YCbCr color domains. For DCT domain, block based approach and for wavelet domain, multi-level wavelet transformation technique and CDMA based approaches is implemented. There are four essential factors those are commonly used to determine quality of watermarking scheme. They are robustness, imperceptibility, capacity, and blindness.

A. Robustness

Watermark should be difficult to remove or destroy. Robust is a measure of immunity of watermark against attempts to image modification and manipulation like compression, filtering, rotation, scaling, collision attacks, resizing, cropping etc.

B. Imperceptibility

Means quality of host image should not be destroyed by presence of watermark.

C. Capacity

It includes techniques that make it possible to embed majority of information.

D. Blind Watermarking

Extraction of watermark from watermarked image without original

II. Steganography

Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. What steganography essentially does is exploit human perception, human senses are not trained to look for files that have information inside of them, although this software is available that can do what is called Steganography. The most common use of steganography is to hide a file inside another file [2].

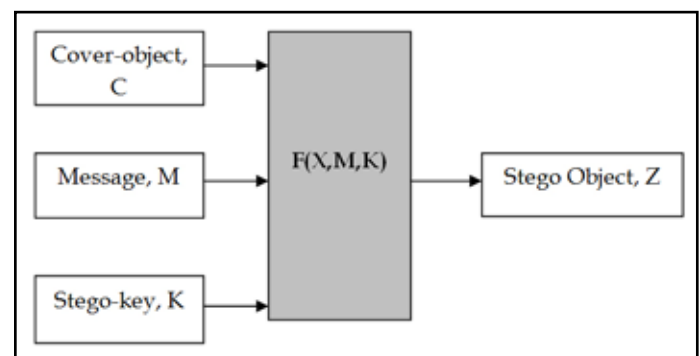


Fig. 1: Basic Model for Steganography

A. Problem Statement

Security and capacity of watermark data are very important issues to be considered. A lot of research is going on to increase security and capacity. This method increases the security and capacity of robust watermark. To increase capacity the concept of nesting is used. Means one watermark in other is embedded. And to increase security of watermark steganography is used.

In the present work, two techniques namely LSB and Biometric pattern (Skin tone) based steganography has been compared and result are evaluated on the basis of comparison of quality of image after embedding of data and change in PSNR value of the image

B. Least Significant Bit Replacement Technique (LSB)

In image steganography almost all data hiding techniques try to alter insignificant information in the cover image. Least Significant Bit (LSB) insertion is a common, simple approach to embedding information in a cover image. For instance, a simple scheme

proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image. The altered image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc. we emphasized more on this technique for the various image formats [3]. The least significant bit i.e. the eighth bit inside an image is changed to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue colour components, since they are each represented by a byte. An 800×600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [4].

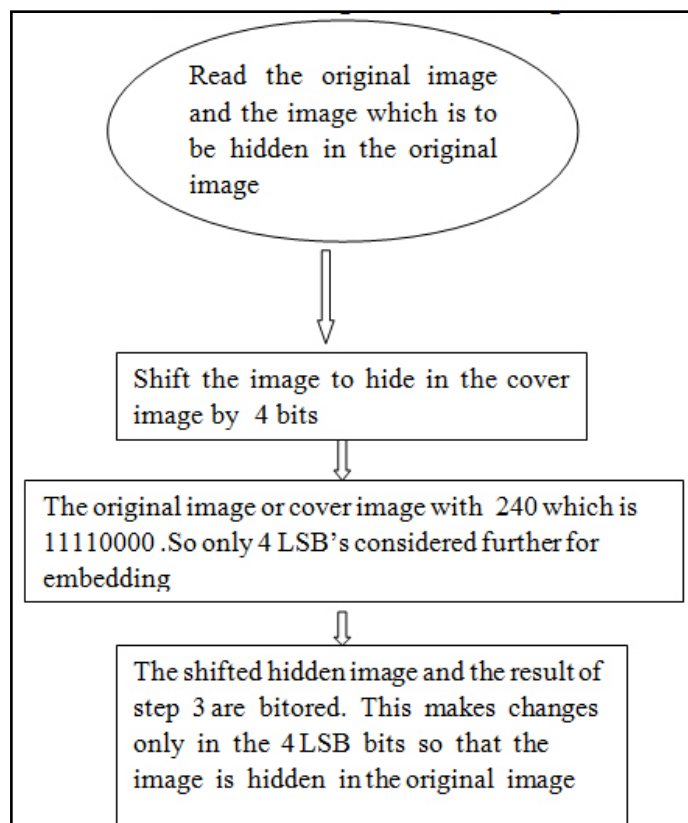


Fig. 2: Algorithm for Hiding Data in LSB

First of all, since it is a so vulnerable technique even for simple processing, LSB insertion is almost useless for digital watermarking, where it must face malicious attempts at its destruction, plus normal transformations like compression/decompression, conversion to analog or conversion to digital.

Its comparatively high data rate can point it as a good technique for steganography, where robustness is not such an important constraint. The major drawback of this technique being ease of extraction.

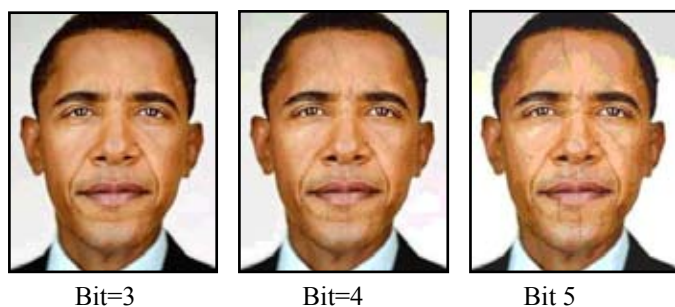


Fig. 3: Shows the Embedded Image Using LSB Insertion by

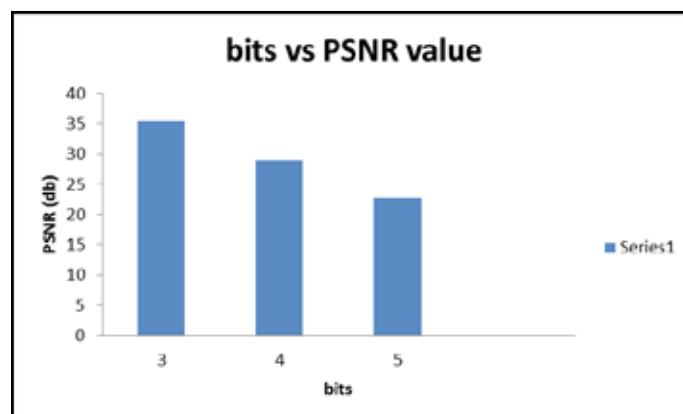
Varying Number of LSB Message Bits Inserted

Fig. 3 showed the effect of variation in number of LSB message bits being inserted in the cover image. It is clearly observe that as number of LSB bits inserted increases the visual quality of the cover image also goes down. On the other side when less number of bits are inserted, the quality of image restore but at the cost of partial message. An optimal bit value is to be chosen so that most of the message is embedded and also the quality of the image is maintained with high PSNR.

Table 1: Showing PSNR value at different bits in LSB

Number of Bits inserted	PSNR VALUE LSB Embedded Image
3	35.5
4	28.98
5	22.75

The above table shows the value of PSNR changes as the number of LSB to be inserted is vary in the cover image. Undoubtedly with decreasing number of bits the SNR value is increasing but it is also to be mentioned that the amount of message being inserted is also reducing so eventually when message is recovered, it may be unreadable too. Using biometric steganography we are able to get visually better quality images with high SNR values.



Graph 1: Graph showing comparison of PSNR value of LSB at different bits

C. Skin Tone Based Steganography

We proposed method of embedding secret data within skin region as it is not that much sensitive to HVS (Human Visual System). This takes advantage of biometrics features such as skin tone, instead of embedding data anywhere in image, data will be embedded in selected regions. Overview of method is briefly introduced as follows. At first skin tone detection is performed on input image using HSV (Hue, saturation, value) color space. Secondly, cover image is transformed in frequency domain [5].

D. Skin Detection

The goal of skin color detection is to build decision rule that will discriminate between skin and non-skin pixels. A skin detector typically transforms a given pixel into an appropriate color space and then uses a skin classifier to label the pixel whether it is a skin or a non-skin pixel.

The skin detection algorithm produces a mask, which is simply a black and white image. The black pixel values are 0 (false) and the white pixel values are 1 (true). This mask of ones and zeros acts as a logic map for skin detection. The simplest way to decide whether a pixel is skin color or not, is to explicitly define a boundary. RGB (Red, Green, Blue) matrix of the given

color image can be converted into different color spaces to yield distinguishable regions of skin or near skin tone. Mainly two kinds of color spaces are available HSV (Hue, Saturation and Value) and YCbCr (Yellow, Chromatic Blue, Chromatic red) spaces. For this work HSV color space is chosen. It is experimentally found and theoretically proven that the distribution of human skin color constantly resides in a certain range within the color space [6]. Embedding is performed in G-plane and B-plane but strictly not in R-plane as contribution of R plane in skin color is more than G or B plane. So if i modify R plane pixel values, decoder side doesn't retrieve data at all as skin detection at decoder side gives different mask than encoder side.

This embedding algorithm attempts to preserve histogram of DWT coefficients after embedding. This protects from histogram based first order statistics attacks. Ultimately it is observed that both the cases provide enough security. Embedding process affects only certain Regions of Interest (ROI) rather than the entire image. So utilizing objects within images can be more advantageous. This is also called as Object Oriented steganography. Next sub-sections describe encoding, decoding process in detail and briefly introduce skin tone detection and DWT.

This is performed by applying Haar-DWT, the simplest DWT on image leading to four sub-bands. Finally, secret data embedding is performed in one of the high frequency sub-band by tracing skin pixels in that band [7].

DWT is used as it performs better than the DCT. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact. This drawback of DCT is eliminated using DWT. DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as

- LL – Horizontally and vertically low pass
- LH – Horizontally low pass and vertically high pass
- HL - Horizontally high pass and vertically low pass
- HH - Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL sub-band) we can hide secret message in other three parts without making any alteration in LL sub-band. As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much. Simplest DWT, Haar-DWT, have been used to transform images into frequency domain [8].

Some of the advantage of Haar wavelets

- High performance in terms of computation time
- Simplicity
- Computation Speed is high

It performs two steps, row and column transformation respectively. Entire row of an image matrix is taken, then do the averaging, differencing is done. After i treated entire row of an image matrix, then do the averaging and differencing process for the entire each column of images.

In this matrix of skin pixels, start from first pixel and using pseudorandom sequence its corresponding pixel for pair is found. In the same way other skin pixel pairs are formed. To create a pseudo random sequence Lehmer's Congruential generator is used that generates non overlapping random sequence [9]. Lehmer invented the multiplicative congruential algorithm, which is the basis for many of the random number generators in use today. Lehmer's generators involve three integer parameters, a, c, and m, and an initial value, x₀, called the seed. A sequence of integers is shown in Equation

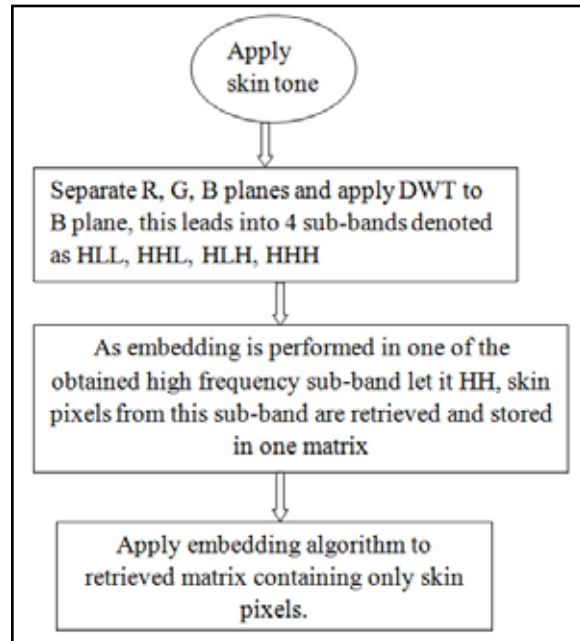


Fig. 4: Flow Chart for Skin Tone Detection

$$x_{k+1} = ax_k + c \bmod m$$

Once pairs are formed secret message bits are embedded based on values of pixel pairs. Each message bit is related with one pair. For embedding 0, check if the first pixel of pair is less than other pixel, if it is then don't change anything otherwise swap gray level values. Similarly pixel value of 1 can be embedded by making the value of first pixel greater than the second pixel. All skin pixels pairs chosen are skin pixels as i have to hide data in only skin pixels. Note that values of pixels are altered but in this way that total count of gray vales in image should remain same. As pixel gray values are not modified, count will remain same leading to an unchanged histogram.

E. Encoding Algorithm

Input- matrix of only skin pixels, let it is S and secret message bits of size M Output- Modified matrix of only skin pixels

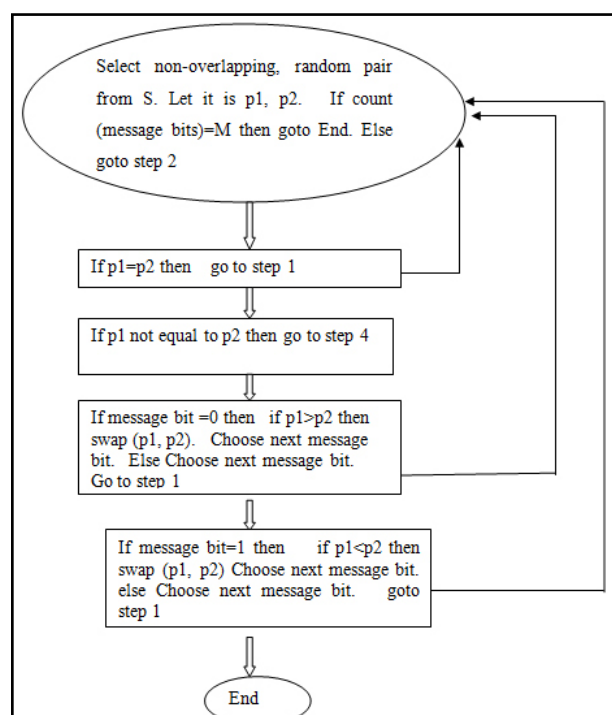


Fig. 5: Flow Chart Encoding Algorithm

Similarly for decoding this i simply store the matrix of swapped values and based on comparison against the HH coefficients of embedded image. I fetch the message bits. So this matrix acts as the key for retrieving messages.

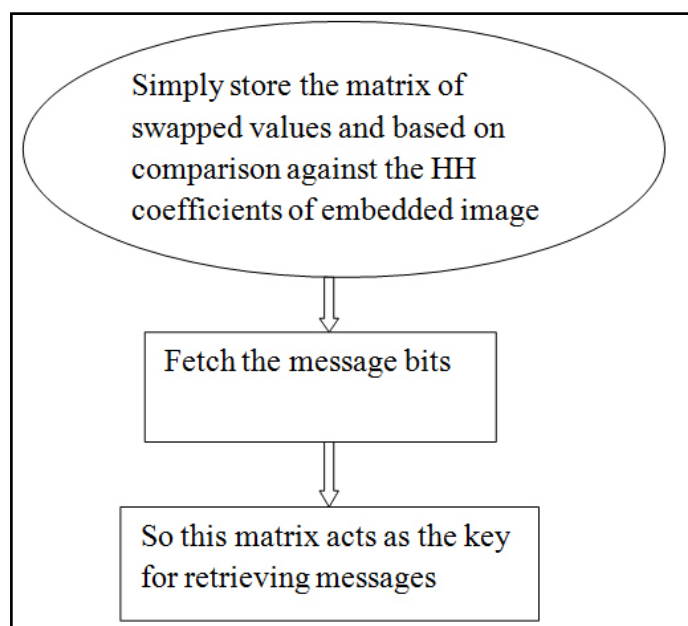


Fig. 6: Flow Chart Decoding Algorithm

Even if the key is leaked it will not be possible for the intruder to decode the image since i have used biometric feature along with DWT.

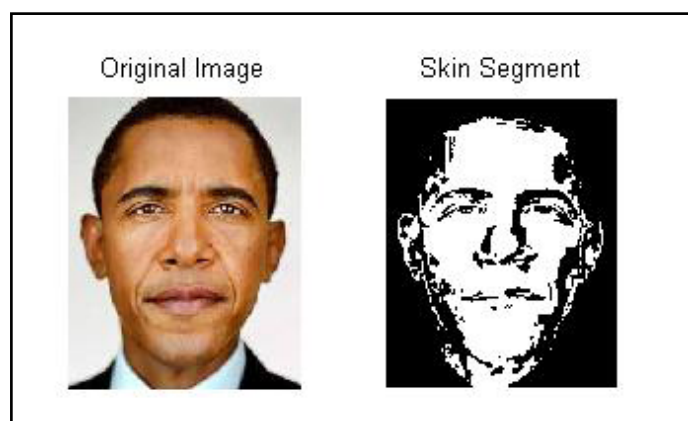


Fig. 7: Show's the Result of Skin Tone Detection on the Cover Image

The above figure shows the result for skin tone detection. As mentioned we change color space of from RGB to HSV in order to identify skin regions in the given image. The results we obtained were clearly able to segregate the skin pixels from the non-skin pixels.

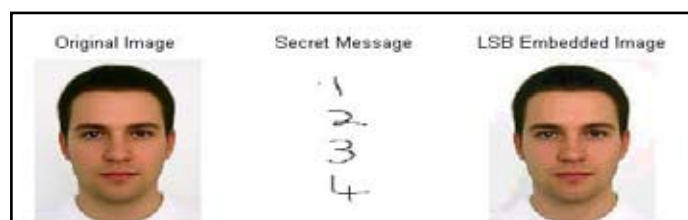


Fig. 8: Comparison Original Image, Biometric Image & LSB Embedded Image (A)

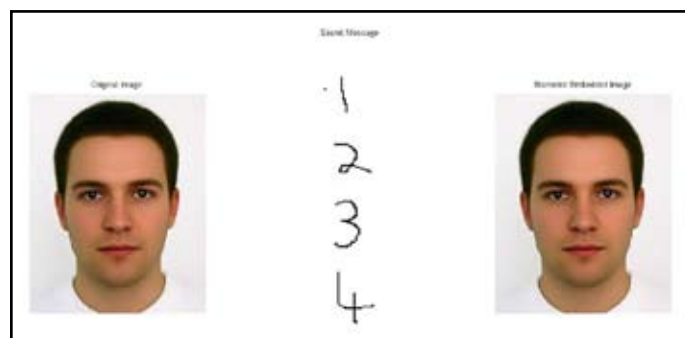


Fig. 8 showed comparison between original image, Biometric image and LSB embedded image. After seeing the figure it is clearly seen that quality of LSB image diminish when data is hidden. And after seeing the image it can be encoded message is seen with visible eye. While in biometric image data is completely unseen and cannot be perceived by eye and quality of image remain unchanged which can be further confirm by comparing the PSNR value of LSB & Biometric image.

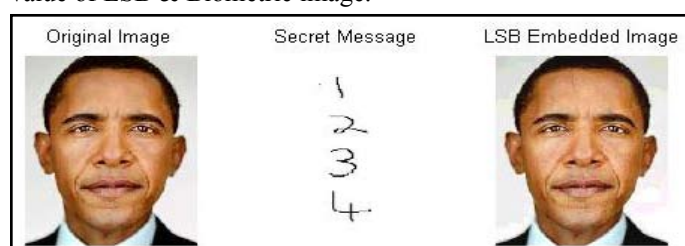
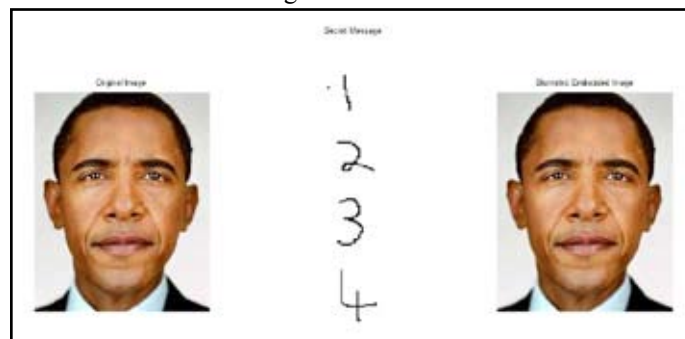
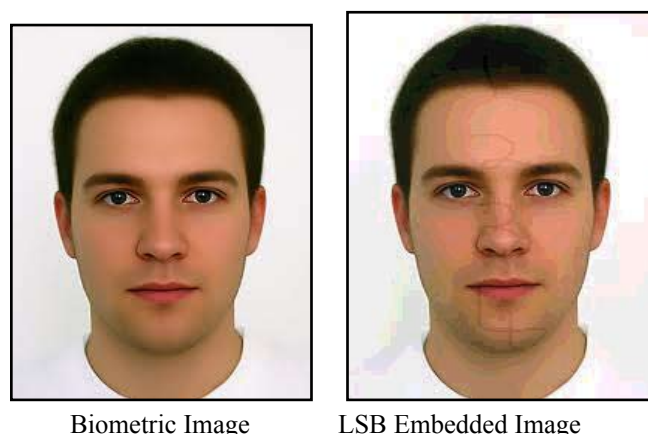


Fig. 9: Comparison Original image, Biometric Image & LSB Embedded Image (B)
LSB embedded image

Biometric Embedded image



The fig. 9 shows the original and embedded image. It can be noticed that the image quality is maintained since I manipulate the cover image in frequency domain and also only the high frequency coefficients in order the hide the message information from the visible eye.



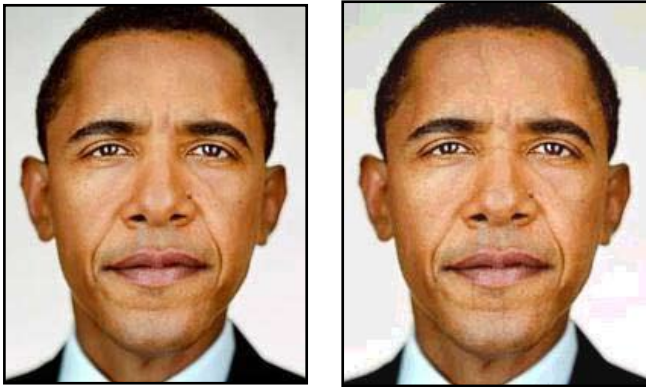
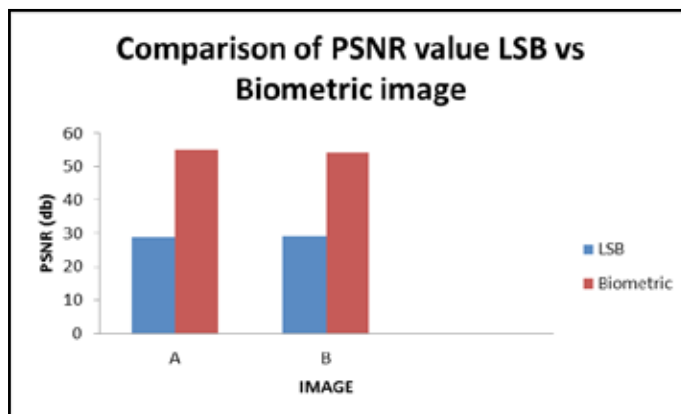


Fig. 10: Comparison of Biometric embedded & LSB Embedded Image A & B

Table 2: Comparison of PSNR Value of LSB & Biometric Images

Image	PSNR (db) value LSB Embedded Image	PSNR (db) value Biometric Image
A	28.7264	54.9165
B	28.9858	54.1070



Graph 2: Graph showing comparison of PSNR value of LSB & Biometric embedded image

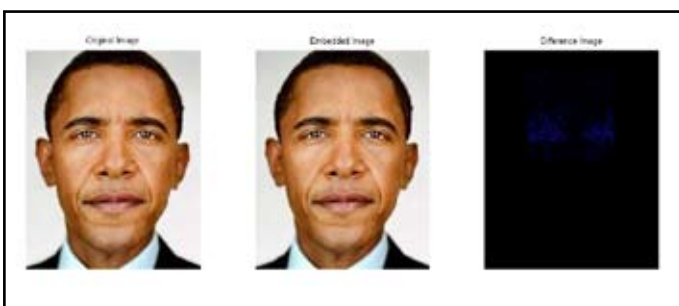


Fig. 11: Difference Image Between the Cover and Embedded Image

Fig. 11 showed the difference image between the cover and embedded image. We have generated the below image by the expression given below

$$\text{Diff} = (\text{Cover} - \text{Embedded}) * 80$$

The factor of 80 is just to highlight the difference in the image. We can see only the skin region is manipulated during embedding.

IV. Conclusion

Digital Steganography is a fascinating scientific area which falls under security systems. The main emphasis in mine results will be on visual image quality being preserved and also the PSNR value which is a measure of quality of embedding. In present work two techniques LSB and Biometric technique have been compared using DWT and LCG. Working in frequency domain it is easy to manipulate the high frequency coefficients. only high frequency coefficients manipulated.

Biometric Steganography is presented that uses skin region of images in DWT domain for embedding secret data. By embedding data in only certain region (here skin region) and not in whole image security is enhanced.

From above results it is observed that this preserves histogram of DWT coefficients after embedding also. That is the main reason why there is not much visual difference between the cover image and embedded image. Performing biometric steganography offers respectable level of security. By adopting embedding algorithm that preserves histogram of DWT coefficients after embedding, prevents histogram based attacks.

V. Future Scope

Steganography has a wide array of uses. For example, it can be used for digital watermarking, e-commerce, and the transport of sensitive data. Digital watermarking involves embedding hidden watermarks, or identification tokens, into an image or file to show ownership. This is useful for copyrighting digital files that E-commerce allows for an interesting use of steganography.

Steganography can also employ in following areas:

- Encoding Secret Messages in Text
- Encoding Secret Messages in Images
- Encoding Secret Messages in Audio

References

- [1] S Kasmani, A. Naghsh-Nilchi, "A New Robust Digital Image Watermarking Technique Based on Joint DWT-DCT Transformation", Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference, Vol. 2, pp. 539-544, 11-13 Nov. 2008.
- [2] R. Popa, "An Analysis of Steganographic System", The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.
- [3] J. Fridrich, M. Goljan, R. Du, "Reliable Detection of LSB Steganography in Grayscale and Color Images", Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, pp. 27- 30, October 5, 2001.
- [4] Po-Yueh Chen, Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, Vol. 4 , No. 3, pp. 275-290, 2006.
- [5] E. Ahmed, M. Crystal, H. Dunxu, "Skin Detection-a short Tutorial", Encyclopedia of Biometrics by Springer-Verlag Berlin Heidelberg 2009.
- [6] J. Yang, A. Waibel, "A real-time face tracker", Proceedings of the 3th IEEE Workshop on Applications of Computer Vision, Sarasota, Florida, 142-147, 1998.
- [7] K. Sobottka, I. Pitas, "Extraction of facial regions and features using color and shape information", Proc. IEEE International Conference on Image Processing, pp. 483-486, 1996.

- [8] P. Chen, E. C. Liao, "A new Algorithm for Haar Wavelet Transform", IEEE International Symposium on Intelligent Signal Processing and Communication System, pp. 453-457, 2002.
- [9] W.H. Press, S. A. Teukolsky, W. T. Vetterling, B. P. Flannery, "Section 7.1.1. Some History", Numerical Recipes: The Art of Scientific Computing (3rd ed.), New York: Cambridge University Press, 2007.



Mrs. Rupa Maan is working as research scholar as M. Tech. Student at Dept. of Computer Science, Bhai Maha Singh College of Engineering, Mukatsar, Punjab, India.