

message from the pixel value. If key=0 we use formula 1 otherwise we use formula 2.

Formula 1: data= (P mod 10)

Formula 2: data=10-(P mod 10). [9]

2.5 Parity Method

The concept of parity checker is used by (Yadav, Rishi, & Batra)[10]. Each pixel value either contains odd parity or even parity. Odd parity means the number of 1's in pixel value is odd, however even parity means the number of 1's in pixel value are even. This method hides 0 bits from secret message into the odd parity bit of the selected pixel. If the selected pixel value does not have an odd parity bit, it adds or subtracts one to make the pixel value an odd parity. However, 1's from secret message are hidden in the selection pixel of even parity, if the selection pixel value is not even one is added or subtracted to make pixel value even. For retrieving, the Stego image and key selection are needed. Using selection location we determine the location of the pixel. 0's are extracted if the parity of the pixel value is odd and 1's if parity of pixel is even. The process of extracting is going through all pixels that are used in hiding process.

2.6 Basic Fibonacci

“The classical Fibonacci numbers introduced in the 13th century by Leonardo of Pisa” .The sequence Fibonacci numbers is defined by the relation $F(N) = F(N-1) + F(N-2)$.

Where $F(0) = 1$ and $F(-) = 0$. [11]

Fibonacci sequence is [1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377,... etc.]. It can be used to represent any numeric value like binary representation. If N is the number of bits allocated to represent any numeric value then it will be easy to distinguish between binary representation and Fibonacci representation because in binary N is 8 bits are used while in Fibonacci N is 12 bits. As a result, this sequence can be used in steganography. It uses Fibonacci sequence to represent the pixel value instead of binary representation. I.e. 12 bits are used to represent the values from (0,255) instead of using 8 bits in binary system. The bit of secret message is written over the bit plan of the cover pixel .i.e. the secret message is converted to binary bit stream. The pixel value of the cover image which is selected for hiding the secret message is converted to Fibonacci representation, and then the bit plan of the pixel value of the cover image is replaced with the secret message. Finally, decompose the Fibonacci representation into the pixel value of the cover image. To retrieve the Stego image, the key of selected pixels are needed. The value of the selected pixel is converted to Fibonacci representation and secret message is reconstructed from the cross pounding bit plan [1],[2]. according to (Zainalabideen,2014)[1],[2] an improving and optimal using of fibonacci LSB method which are applied in image steganography, in this project we will implement a new proposal of fibonacci by using 11 bits representation and set zeros to the both neighbour of bit planes which were separately used in previous works in [1][2].

3. Testing and Conclusion

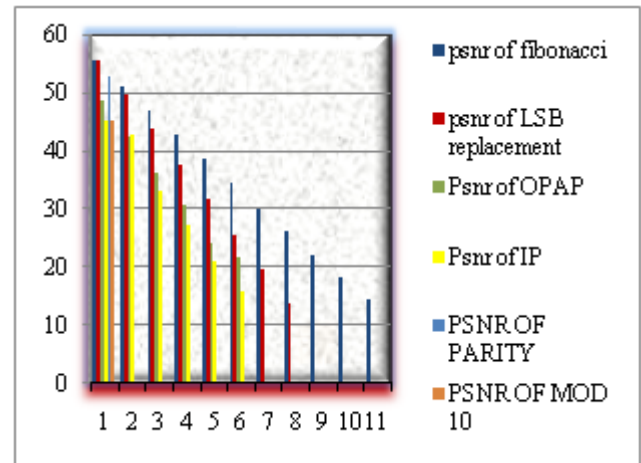


Figure 1: PSNR of all methods

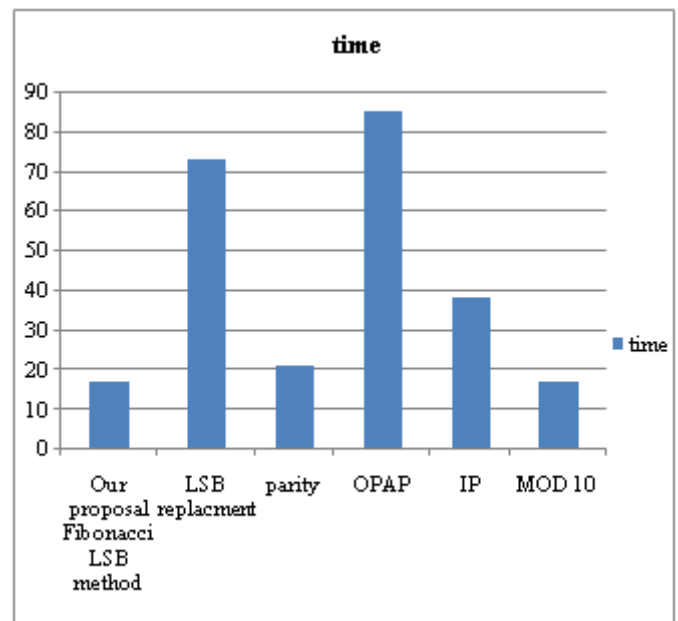


Figure 1: Time of all methods

1. In terms of stego image quality (PSNR) it is clear from figure 1 our proposal Fibonacci method scored better PSNR for all levels of bit plan. However, OPAP and IP methods could also be acceptable. Other applications that check the quality of the stego_image could as well use these methods.
2. In terms of time, figure 2 shows that our proposal, mod 10 and parity methods were better compared with the other methods. This will make it very suitable to be implemented in smart phones.
3. In terms of bit plan, the Fibonacci method is the best because it allows flexible bit plans .i.e. 11 bits while binary representation is 8 bits. For that reason, Fibonacci representation do less change to the pixel value by using the same bit plane with binary representation and Fibonacci means less distortion to the cover image resulting in a high quality stego image.
4. OPAP, IP and mod 10 are the best methods in terms of capacity. However, the long-time and key required make these methods are not so suitable for windows phone.

5. In terms of key necessity, LSB replacement and my proposal Fibonacci LSB is the best since these procedures are practical deprived of a key unlike the other steganography methods where a key is needed for embedding and retrieving. This releases enquiries for in what way a key can be guided to the receiver side.

For all these reasons my proposal, Fibonacci LSB method maybe considered the best choice to develop a steganography application under windows mobile phones in terms of time and quality of stego image and key necessity. For future work the whole apps under windows mobile phone using Fibonacci LSB will be done.

(Baghdad University, Iraq), and MSc (Buckingham university, UK). He has a long experience in teaching various computing practical courses at Baghdad university. At AL Kufa university, Mr. Rasheed teaches different courses like computer organization, operating system and computer architecture. He supervises undergraduate projects. He is interested in data security (steganography and cryptography) and digital image processing (biomedical image and edge detection, de-noising images), Iraq.

References

- [1] Zainalabideen Abdul Samad Rasheed "Steganography Technique for Binary Text Image" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, 2015
- [2] Zainalabideen Abdul Samad Rasheed, Improving Classical Fibonacci in Steganography, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE) ISSN: 2277 128X, 2014
- [3] Zainalabideen Abdul Samad Rasheed, "Comparative study For steganography techniques" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, 2015
- [4] Morkel, T., Eloff, J., & Olivier, M. (2005). An overview of image steganography
- [5] Hong, W., & Chen, T. (2011). A Novel Data Embedding Method Using Adaptive Pixel Pair Matching. *Information Forensics and Security, IEEE Transactions on* (99), 1-1.
- [6] Chan, C., & Cheng, L. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*, 37(3), 469-474.
- [7] Yang, C. (2008). Inverted pattern approach to improve image quality of information hiding by LSB substitution. *Pattern Recognition*, 41(8), 2674-2683.
- [8] Kamal Deep. (2011). Relative Entropy Based Analysis of Image Steganography Techniques. *International Journal of P2P Network Trends and Technology* (99), 1-1.
- [9] Amirtharajan, R., Akila, R., & Deepikachowdavarapu, P. (2010). A Comparative Analysis of Image Steganography. *International Journal of Computer Applications IJCA*, 2(3), 41-47.
- [10] Yadav, R., Rishi, R., & Batra, S. (n.d.). A new Steganography Method for Gray Level Images using Parity Checker. *International Journal of Computer Applications* (0975-8887) Volume.
- [11] Picione, D., Battisti, F., Carli, M., Astola, J., & Egiazarian, K. (2006). A Fibonacci LSB data hiding technique.
- [12] Ker, A. (2005). Steganalysis of LSB matching in grayscale images. *Signal Processing Letters, IEEE*, 12(6), 441-444.

Author Profile



Zainalabideen Abdullasamd Rasheed University of Kufa, Education of College, Najaf /Iraq. Has a BSc

Volume 4 Issue 2, February 2015

www.ijsr.net

Licensed Under Creative Commons Attribution CC BY