Comparative Study of Three DNA-based information hiding methods

Maimonah Albrahim, NisreenTerkawi, Wafaa Alsaffar
Supervised by: Dr. Amjad Ali Alamar

Introduction & Background

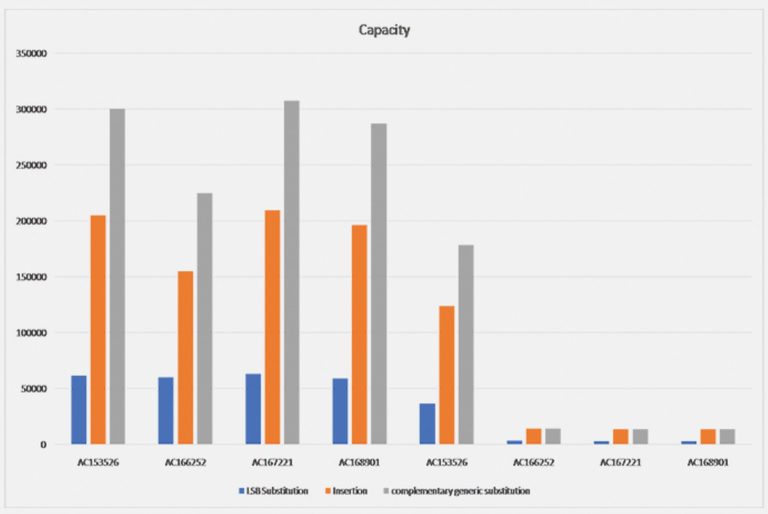
In our real-world exchanging securely for critical information through the internet needs high-security protection. Steganography is one of the security fields that is provide the required protection recently. it is the science of hiding information using different media such as Deoxyribonucleic acid (DNA). The steganography based on DNA provides a high security and more features than others. Therefore, in our project, we compare three DNA-based steganography algorithms [1][2][3] in terms of several properties: capacity, payload, BPN, and the cracking probability.

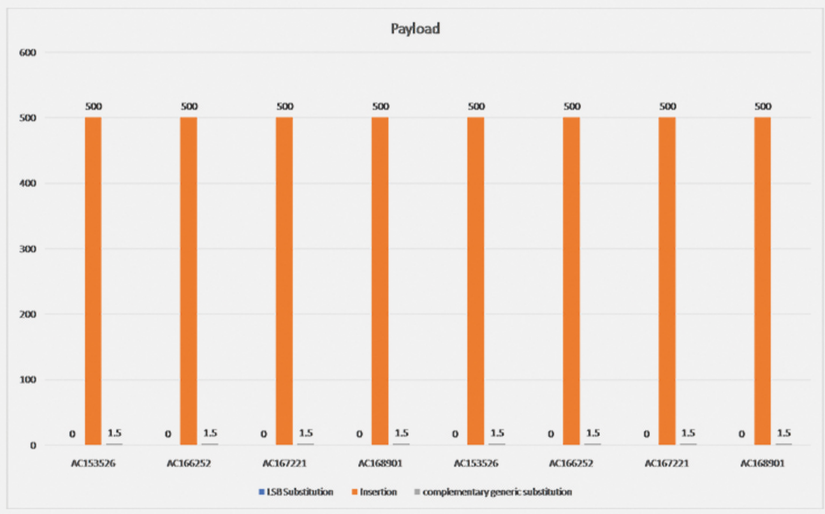
Conclusion & Future work

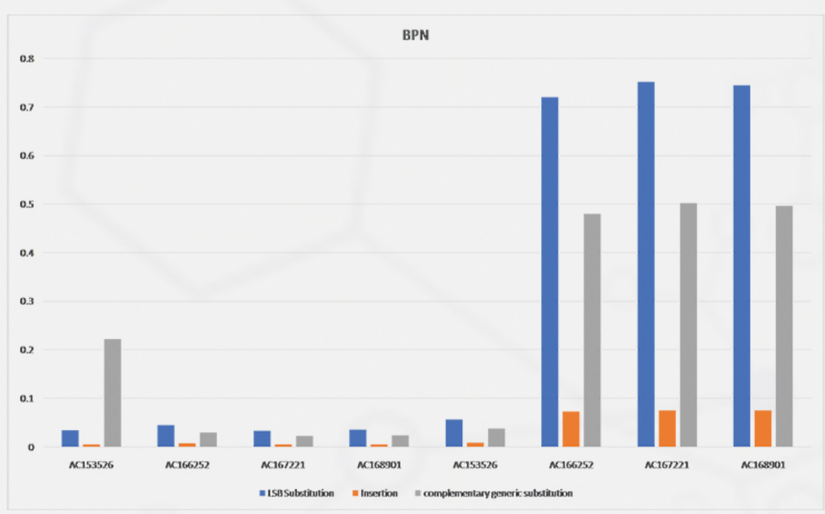
We have concluded from a comparison of algorithms that each algorithm has its strength features and the target system should be consider it when choose the suitable algorithm. For example, the LSB based algorithm is better than the other in term of BPN and payload. While the complementary generic substitution-based algorithm is better in term of capacity. Whereas-the insertion-based algorithm provides low cracking property.In the future, we are thinking about extending this project by creating a new steganography method better than and stronger than others, by combining more than one algorithm, to obtain more secure data at exchanging it. Or, we can improve and overcome some of the limitations we found during our implementation of the selected algorithm.

Results

Algorithms	Cracking property
Based on substitution [1]	$P(SG) = \frac{1}{1.63 * 10^8} + \frac{1}{16!} + \frac{1}{4}$
Based on insertion [2]	$\frac{1}{1.63 * 10\text{^}8} X \frac{1}{24} X \frac{1}{(n-1)} X \frac{1}{(2^m - 1)} X \frac{1}{2s-1} X \frac{1}{2\text{^}8m}$
Based on complementary generic substitution [3]	$\frac{1}{(2^s - 1)^2} X \frac{1}{6} X \frac{1}{24}$







Objectives

Our aim will be achieved by applying the following objectives:

1. Survey existing DNA-based steganography algorithms.
2. Implement selected algorithms.
3. Compare these algorithms based on specified comparison measurements.
4. Analyze the comparison results.
5. Evaluate these results.

Methodology

Algorithm LSB Substitution [1]

Algorithm Insertion [2]

Algorithm Complementary generic substitution [3]

References

[1] G. Hamed, M. Marey, S. A. El-Sayed, and M. F. Tolba, “Hybrid technique for steganography-based on DNA with n-bits binary coding rule,” 2015 7th International Conference of Soft Computing and Pattern Recognition (SoCPaR), 2015.

[2] M. P, M. M, M. R, V. Raghavan, and V. R.e., ‘Highly Improved DNA Based Steganography’, Procedia Comput. Sci., vol. 115, pp. 651–659, Jan. 2017.

[3] A. Khalifa, A. Elhadad, and S. Hamad, “Secure Blind Data Hiding into Pseudo DNA Sequences Using Playfair Ciphering and Generic Complementary Substitution,” Applied Mathematics & Information Sciences, vol. 10, no. 4, pp. 1483–1492, Jan. 2016.

Acknowledgments

First and foremost, we would like to present my deepest gratitude to Almighty Allah for his bounties and blessings and for giving us the ability to finish this project. We would like to express our deep appreciation and our sincere gratitude to our supervisor Dr. Amjad Alamar for her valuable advice guidance throughout this project.