Project Description

SOFE 3770U: Design and Analysis of Algorithms, Fall 2018

Instructor: Dr. Sukhwant Kaur

Comparative Study (Brute Force vs. PSO)

Submission deadline: Sunday, Nov. 25, 2018 11:59 PM

Class project presentation: Nov. 27 and 29, 2018 (9:40am - 11:00 am)

Title of the project: Comparison of Brute Force and Particle Swarm Optimization in cryptanalysis of Vigenere Cipher

Instructions for the project

1. This course project is a group project. The group can have maximum of 4 students. While making groups, please make sure that you have two students who are good in programming in any environment and the other two students needs to have inclination towards research and analysis part of the project. This combination will definitely bring success to the project.
2. The basic goal of the project is for you as a group to apply some of the advanced algorithmic thinking you have been developing in this class. The course project involves a combination of goals-encountering and absorbing new material, doing some thinking about it, and presenting what you have done.

3. Each of the groups are required to be registered with the instructor latest by 16th October, 2018. Beyond that date, no student is permitted to change to any other group.

4. The project submission (pdf document-using full APA document writing style and references) should have include- a, c, d points and the marking scheme is also listed here:

a) The title page containing the course title, course code, team information (Banner id, student name), Project Title and date of submission.

b) The entire team has to defend the project in front of jury. All the team members are required to present the project as the marks are based on individual effort too. Failure to attend the demonstration will have zero marks for the student: Presentation skills: (20 marks)

c) Introduction about the project (based on your research after understanding project title), System requirements of the project, Methodology used, Detailed codes, screenshots of the execution of important steps of your project. (50 marks)

d) Experimental Results, Discussion on the results achieved along with Big O analysis and Conclusion of the project (30 marks)

Project Description

Vigenere cipher is a polyalphabetic substitution cipher with a very large key space. In this project, you are required to investigate the use of Brute Force and PSO for the cryptanalysis of vigenere cipher.

An English plain text file from various text books and articles needs to be formed. After removing all the punctuations, numerals and structure (sentences/paragraphs marks, space characters, and newline characters) a sample text file consisting of 480526 (it's just some value, but you will be needing bigger values like this number) characters is to be created. All plaintexts of varying size, used in this project are required to be taken from this file. Keywords of varying lengths up to twenty-five (as mentioned down in the document) are to be used and the plain texts should be converted into cipher texts using Vigenère method. First Brute force is required to be used to deduce plaintext from cipher text. Findings are to be reported.

Then, PSO is to be applied and the global minima in each character is required to be intimated to other members in the swarm. The individual moved towards the global minima if necessary and finds its local best solution. This process is to be repeated till the overall fitness of swarm reached a tolerance value or 100 iterations whichever was earlier.

You need to include in your project report:

- A table (for keyword length =5,10,15,20,25) to compare Brute Force and PSO in terms of average number of key characters recovered correctly, minimum

number of key characters recovered correctly, maximum number of key characters recovered correctly, standard deviation of the collected errors between 50-100 runs.

- You need to report Minimum size of cipher text required for different keyword lengths. You can start at 200 characters of cipher text and can gradually increase in multiples of 100
- You need to report the best solution (and its fitness function) between 50-100 runs.
- You need to have Big-O analysis for Brute Force and PSO algorithms.
- You need to compare Brute Force and PSO and conclude that which one performs better under what conditions.

Control Parameter Settings and sketch of procedure(Hint):

1. ***Initialization of PSO search algorithm parameters***

- Self-confidence C_1= 2.05,
- Swarm confidence C_2 = 2.05
- inertia weight w = 0.9
- r1, r2 are the uniformly generated random numbers in the range of [0, 1].
- Number of Particles Np=100
- Size of the key N_d =5,10,15,20,25

2. ***Initialization of discrete birds or population***

- For cryptanalysis of Vigenere cipher: the initial positions of the particles are determined by randomly choosing the permutations of size N_d, sampled uniformly at random from integers 0 to 25.
- Initialize velocity of each particle using: $v_i = v_{min} + (v_{max} - v_{min}) \times rand$

where:

v_i is velocity of *ith* particle,
v_{max} is maximum velocity,
v_{min} is minimum velocity,
rand is a random number between 0 and 1.

3. ***Calculate fitness function value***

For each particle

- Decrypt the cipher text using the position of the particle as the key.
- Find the fitness function value of the text obtained in step 3 (a).

4. ***Update velocity and position of the particles***

$$v_i^{t+1} = w.v_i^t + C_1.rand_1 \times (pbest_i - x_i^t) + C_2.rand_2 \times (gbest_i - x_i^t)$$

$$x_i^{t+1} = x_i^t + v_i^{t+1}$$

Calculate the fitness function value of each particle as discussed in step 3.

5. ***Termination criterion***

Repeat steps 3 and 4 until termination criterion is satisfied. The maximum number of iterations or the saturation of fitness value of the *gbest* particle is considered as termination criterion of the algorithm.

More details will be provided during the lectures or tutorials.

Note: During your presentation in class, you will explain the comparison of Brute Force and PSO for Cryptanalysis of Vignere Cipher on certain ciphertexts of varied lengths.

****

Good Luck

****