Long-lived nearby-template preimages on biometric transformation with genetic algorithm

{ Tanguy Gernot and Patrick Lacharme } Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, Caen, France

Introduction

Biometric transformations prevent biometric data recovery.

A long-lived nearby-template preimage is recovered by performing different attacks, based on genetic algorithm.
The performance is analyzed with different choices of parameters and regarding to an adaptative-plaintext attack.

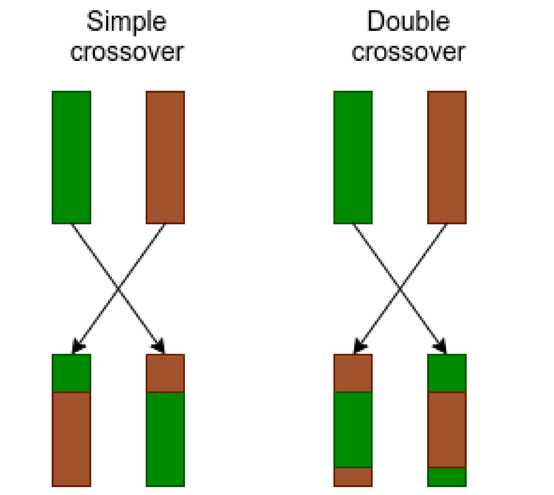
Genetic algorithms

There are four main steps in genetic algorithm.

The generation of the initial population uses two major methods : random generation of each people, or low discrepancy sequence.
The selection step selects a subset of candidates.
The crossover step mixes two vectors.
The mutation step adds randomness with different methods.

Crossover step

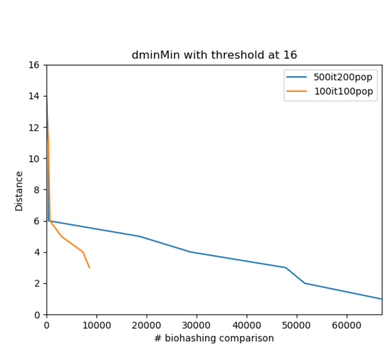
The crossover step combines two good candidates in the hope of seeing a better one emerge.

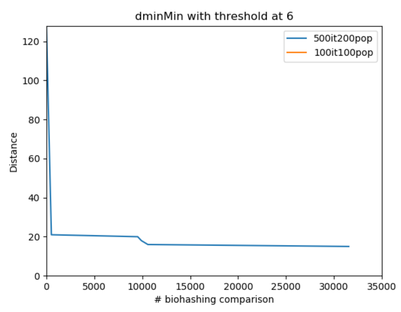


There is two crossover methods : the single point, and the multi point crossover.
There is no efficiency difference between them.

Population & Iteration

Research of the best parameters for genetic algorithm. Difference of efficiency and precision between a population of size 100 with 100 iterations, versus one of size 200 with 500 iterations.





Selection step

There are three selection methods :

Roulette wheel a proportionate reproduction in terms of fitness score

Tournament selection randomly draws 2 individuals and take the most fit with probability p

Rank selection takes the individuals in order of their fitness score

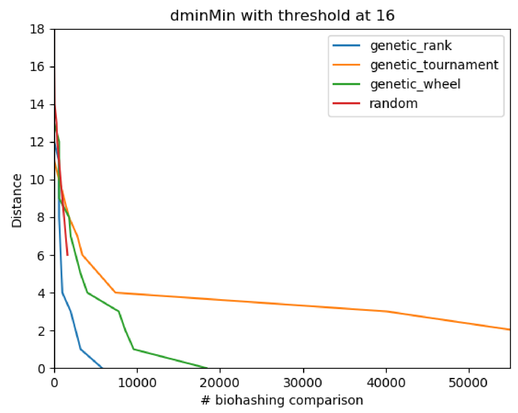


Figure 1: Threshold at 16

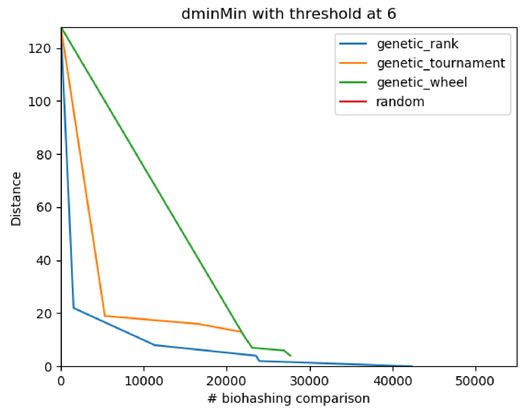


Figure 2: Threshold at 6

The rank selection is the better selection's method. It obtains a minimal distance of 0 from threshold at 6.
The roulette wheel selection has good score, but longer and a little worse.
The tournament selection is the worst : it's clearly longer, and it obtains worse minimal distance.

Conclusion

θ	Rank	Tournament	Wheel	Random
4	-	-	7 (6.9)	-
5	22 (0.15)	20 (3.3)	6 (3.9)	-
6	0 (4.2)	13 (2.1)	4 (2.7)	-
7	0 (2)	13 (2.1)	3 (3.5)	25 (3)

θ	500it200pop	100it100pop
9	3 (63592)	33 (360)
10	3 (61795)	10 (2254)
11	3 (61795)	9 (6577)

Experiments show that a mutation probability at 0.2, a rank selection's method, and a population size of 200 (with 500 iterations) give the best long-lived nearby-template preimage.

Moreover, genetic algorithm is better than the 3 adaptative-plaintext attack tried.

References

[1] P. Lacharme, E. Cherrier, and C. Rosenberger. Preimage Attack on BioHashing. In *SECRYPT*, '13.

[2] X. Dong, Z. Jin, and A. Jin. A Genetic Algorithm Enabled Similarity-Based Attack on Cancellable Biometrics. 2019.

Future Research

- Compute an average vector for the enrollment step
- Generalization to generic transformations and several biometric modalities
- Formalisation of these attacks
- Combination with others attacks on preimages

Contact Information

Web gernot.fr
Email tanguy.gernot@unicaen.fr
Phone +33 2 31 53 81 89