**Technical Report**

**Technical Report**

**Stegnography 1st version**

|  |  |
| --- | --- |
| Prepared by: | Eng. Mohammad Sakka |
|  |  |
| Date: | 26/4/2021 |
|  |  |

**REPORT SENSITIVITY**

Does the report have any of the following sensitivities?

Intended for journal publication YES

Results are incomplete NO

Commercial/IP concerns NO

**pseudocodes**

|  |
| --- |
| % Chromosome fixing pseudocode  Input**:**  Chromosome  trueMessgeBitsNumber  OutPut**:**  fixedChromosome  start**:**  counter **=** 1  subProcedure**:** count the fake bits number  **{**  **for** each chromosome metameric  bitplanesNumber **=** get the number of bits in this metameric bitplane  numberOfPixels **=** numberOfPixels in this metameric  bitsCount**(**counter**)** **=** numberOfPixels **\*** bitplanesNumber  counter **++**  **end**  fakeBitsNumber **=** sum**(**bitsCount**)**  **}**  **while** fakeBitsNumber **~=** trueMessgeBitsNumber  **if** fakeBitsNumber**>**trueMessgeBitsNumber  difference **=** fakeBitsNumber**-**trueMessgeBitsNumber  meta **=** select random metameric  pixelNumber **=** meta**.(**get pixels number**)**  bp **=** meta**.(**get the bitplanes**)**  numberOfBP **=** meta**.(**get the number bitplanes bits**)**  numberOfPixelsToDelete **=** ceil**(**difference**/**numberOfBP**)**  newPixelsNum **=** pixelNumber **-** numberOfPixelsToDelete  **if** newPixelsNum**<**1  newPixelsNum **=** 1  **end**  **else**  difference **=** trueMessgeBitsNumber**-**fakeBitsNumber  meta **=** select random metameric  pixelNumber **=** meta**.(**get pixels number**)**  bp **=** meta**.(**get the bitplanes**)**  numberOfBP **=** meta**.(**get the number bitplanes bits**)**  numberOfPixelsToAdd **=** ceil**(**difference**/**numberOfBP**)**  newPixelsNum **=** pixelNumber **+** numberOfPixelsToAdd  **end** **[**if\_fakeBitsNumber**>**trueMessgeBitsNumber**]**  fakeBitsNumber **=** call subProcedure  **if** fakeBitsNumber still greater than trueMessgeBitsNumber  **if** fakeBitsNumber **-** trueMessgeBitsNumber **==**1  **if** numberOfBP **==** 2  break\_the loop and ignore the last bitplane  **end**  **elseif** fakeBitsNumber **-** trueMessgeBitsNumber **<=**2  **if** numberOfBP **==** 3  break\_the loop and ignore the last bitplane  **end**  **elseif** fakeBitsNumber **-** trueMessgeBitsNumber **<=**3  **if** numberOfBP **==** 4  break\_the loop and ignore the last bitplane  **end**  **end**  **end** **[**if\_fakeBitsNumber still greater than trueMessgeBitsNumber**]**  **end** **while** |

The others pseudocodes are exist in the main approach document

**Execution Parameters**

Metameric Version

1. popSize = 50
2. maxGen = 50
3. mr0 = 0.2 // uniform mutation
4. mr = mr0\*exp(-genr/maxGen)
5. image dims scaling = [512,512]
6. images: first 10 images from brainTumorDataPublic\_1766 dataset
7. QL = 20
8. T\_nbc = 250
9. Selection mode = ‘roulette wheel’
10. Number of seed = 5
11. Fitness value = 1/sum(mse) //maximization

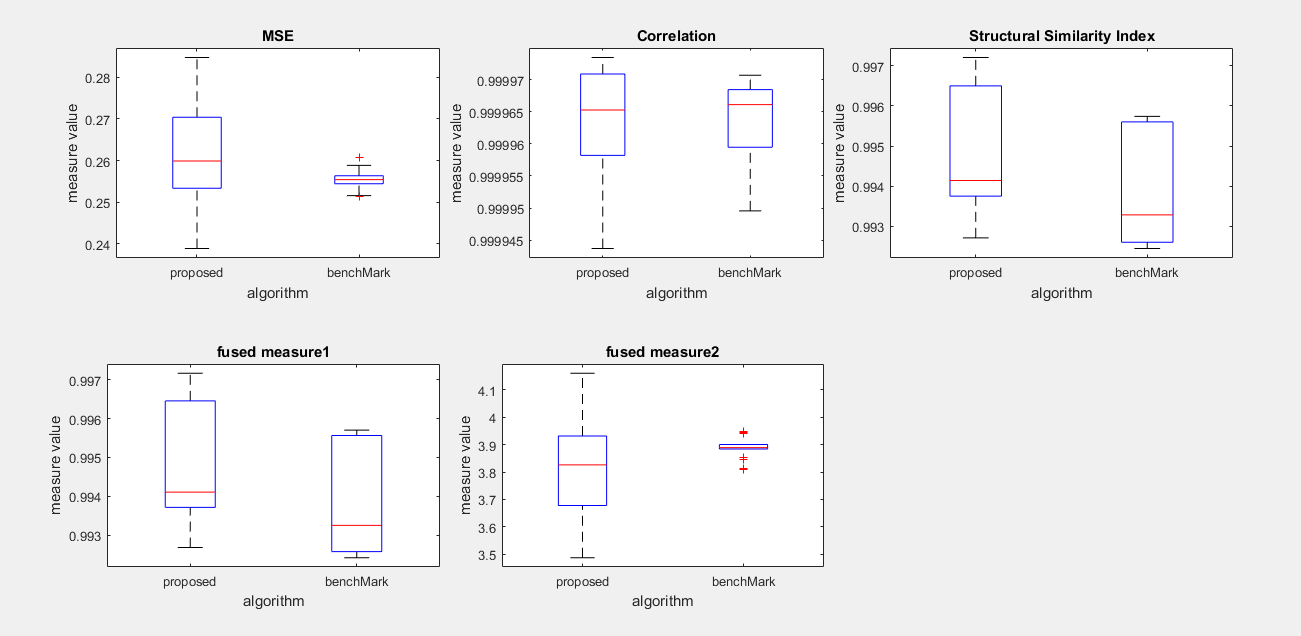
BenchMark Version

1. popSize = 50
2. maxGen = 50
3. gaussian mutation // shrink =1 , fraction = 1
4. mr = mr0\*exp(-genr/maxGen)
5. image dims scaling = [512,512]
6. images: first 10 images from brainTumorDataPublic\_1766 dataset
7. Selection mode = ‘selectionstochunif’
8. Number of seed = 5
9. Fitness value = mse //minimization

Secret Message:

'Steganography is the practice of concealing a message within another message or a physical object. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video. The word steganography comes from Greek steganographia, which combines the words steganَs (????????), meaning "covered or concealed", and -graphia (?????) meaning "writing".The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages appear to be (or to be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography that lack a shared secret are forms of security through obscurity, and key-dependent steganographic schemes adhere to Kerckhoffss principle.The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable they are, arouse interest and may in themselves be incriminating in countries in which encryption'

**Results**



The figure can be generated from visualization/MainFile

Comment:

The fixing pseudocode often leads to make the chromosome blocks unbalanced in terms of number of pixels, and this may make the algorithm worse.

* So we will develop a new version of crossover that reduces the need to fixing and saves the balance