**Technical Report**

**Technical Report**

**Stegnography final version**

|  |  |
| --- | --- |
| Prepared by: | Eng. Mohammad Sakka |
|  |  |
| Date: | 9/2/2022 |
|  |  |

**REPORT SENSITIVITY**

Does the report have any of the following sensitivities?

Intended for journal publication YES

Results are incomplete NO

Commercial/IP concerns NO

Project Workflow:

* After that matameric approaches have not given good approaches, we have introduced decompsition technique, in wich we decompose the secret message to n sub-messages and hiding them in distributed areas of the image.
* To approve the benefit of hiding the secret bits in a distributed areas of the image, we returned back to the GA benchMark algorithm that is already superior over all other algorithms, and make it decompose the secret bits to n part and then hide them in non-continous areas of the image.
* Decomposition Pseudocode:

Input:

imCover, secretMessage, n

Output:

stegno

Start:

1. subMsgs = decompose(secretMessage,n)
2. old\_hiding\_pixels = [ ]
3. finalChrom = [ ]
4. for subMsg in subMsgs
5. [bestChrom,stegno,hidingPixels] = benchMarkAlgo(imCover, subMsg)
6. old\_hiding\_pixels = [old\_hiding\_pixels hidingPixels]
7. imCover = stegno
8. finalChrom = [finalChrom bestChrom]
9. End for

End

* Modified cost function pseudocdoe

|  |
| --- |
| Input:  imCover,stegno,oldHidignPixels,hidingPixels  Output:  Cost  Start:   1. If any(ismember(hidingPixels, oldHidignPixels)) 2. Cost = inf 3. Else 4. Cost = MSE(imCover,stegno) 5. End if   End |

By implementing the above approach, we solve the problem of hyper search space that appears in the metameric approach, and the continuity problem that appears in the benchMark approach.

Execution:

Execution parameters:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Population size | maxIter | Mutation rate/mutation ratio |
| All algorithm | 50 | 50 | Gaussian mutation with default matlab ga values for scale and shrink that are modified adaptivally using the generation number , default initial scale/shrink = 1/1 |

Other uniform params:

1. image dims scaling = [512,512]
2. Fitness function = -MSE

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 steganos , 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 encryptionis illegal.Whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent and its contents. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer such as a document file image file program or protocol. Media files are ideal for steganographic transmission because of their large size. For example a sender might start with an innocuous image file and adjust the color of every hundredth pixel to correspond to a letter in the alphabet. The change is so subtle that someone who is not specifically looking for it is unlikely to notice the change.The first recorded uses of steganography can be traced back to 440 BC in Greece, when Herodotus mentions two examples in his Histories. Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, "marking" the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, "When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon." Additionally, Demaratus sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand.In his work Polygraphiae, Johannes Trithemius developed his so-called "Ave-Maria-Cipher" that can hide information in a Latin praise of God. "Auctor Sapientissimus Conseruans Angelica Deferat Nobis Charitas Potentissimi Creatoris for example contains the concealed word VICIPEDIA.Modern steganography entered the world in 1985 with the advent of personal computers being applied to classical steganography problems.[7] Development following that was very slow, but has since taken off, going by a large number of steganography software availableAn image or a text can be converted into a soundfile, which is then analysed with a spectrogram to reveal the image. Various artists have used this method to conceal hidden pictures in their songs, such as Aphex Twin in "Windowlicker" or Nine Inch Nails in their album Year ZeroIn communities with social or government taboos or censorship, people use cultural steganographyhiding messages in idiom, pop culture references, and other messages they share publicly and assume are monitored. This relies on social context to make the underlying messages visible only to certain readers.

BenchMark Decomposed specific parameters:

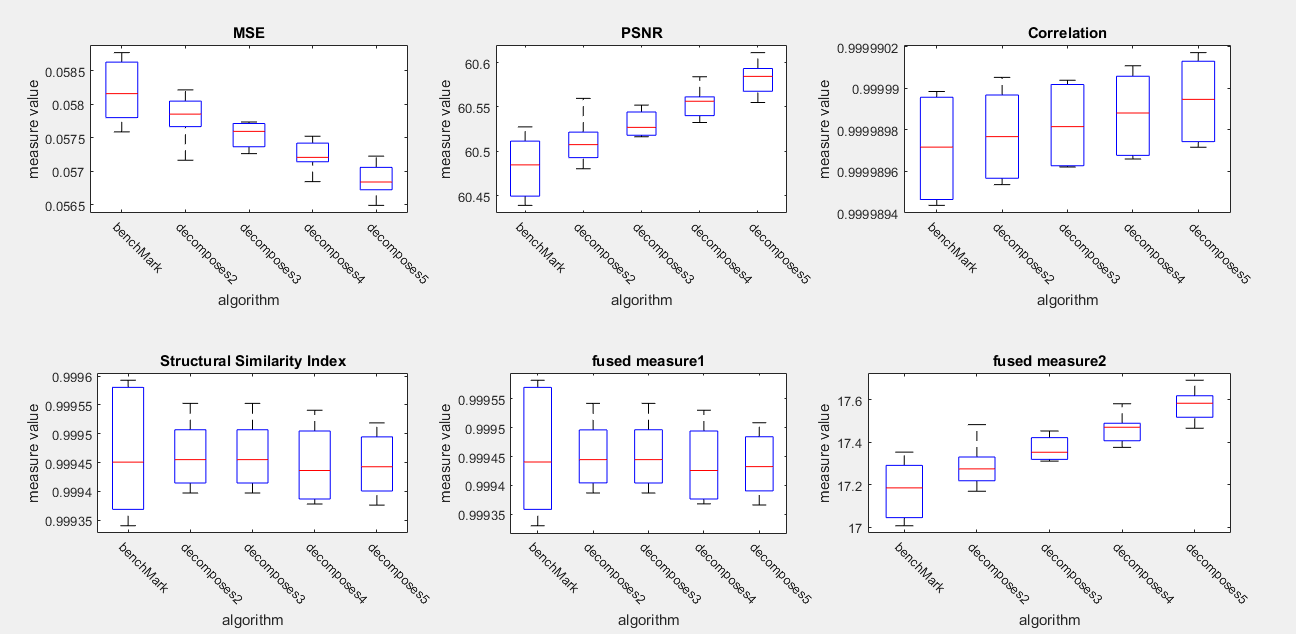
We have executed the previous approach using n=2 ,n=3,n=4 and n=5, this means that the message was decomposed to 2 and 3 subMsgs respectively

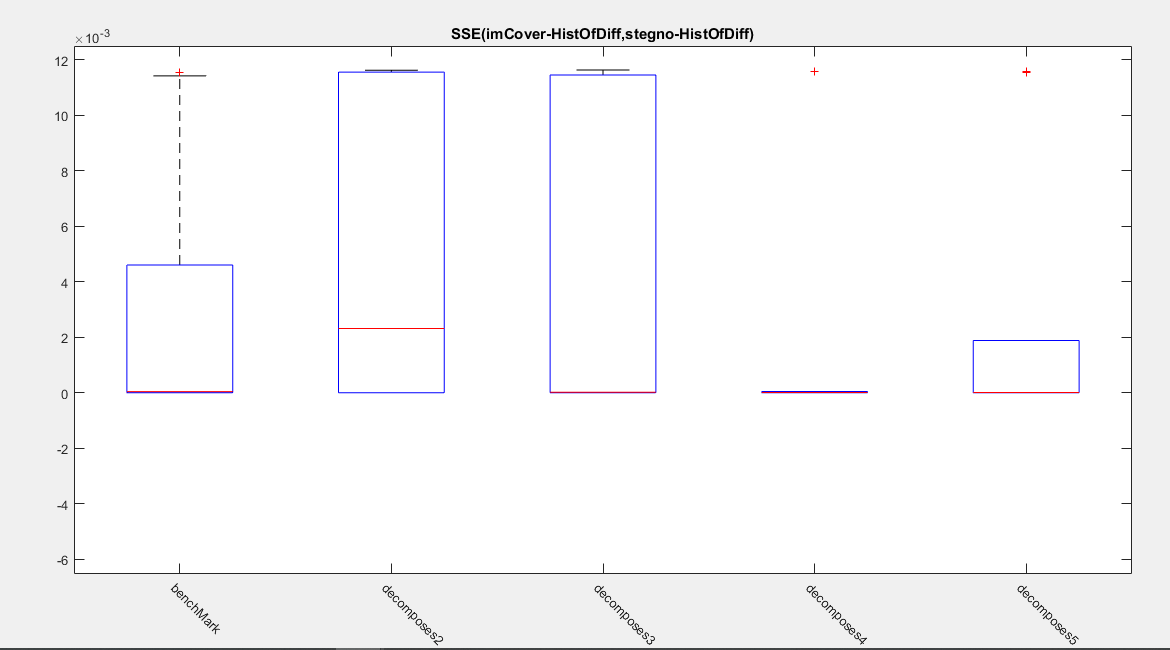
Used Measures:

1. MSE: mean of squared errors
2. PSNR
3. Correlation
4. Structural similiarity
5. Fused Measure1 = correlation \* structural similiarity
6. Fused Measure2 = Fused Measure1 / MSE

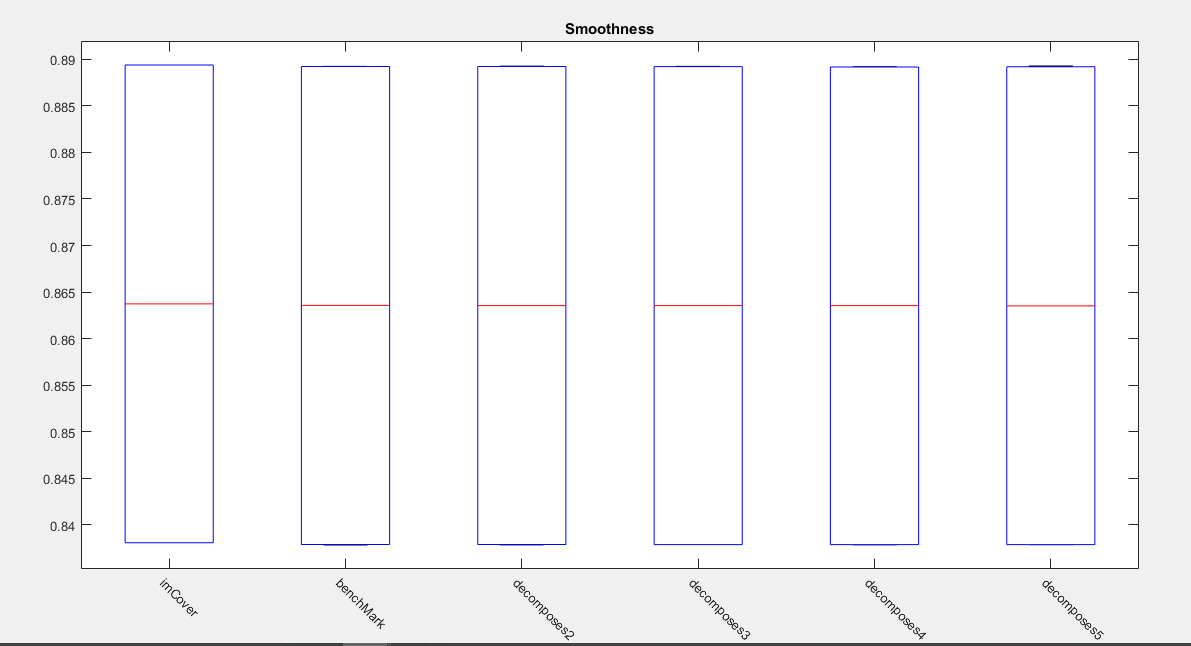
Results:

1-Chest Dataset within 2 images and 5 seeds for each image



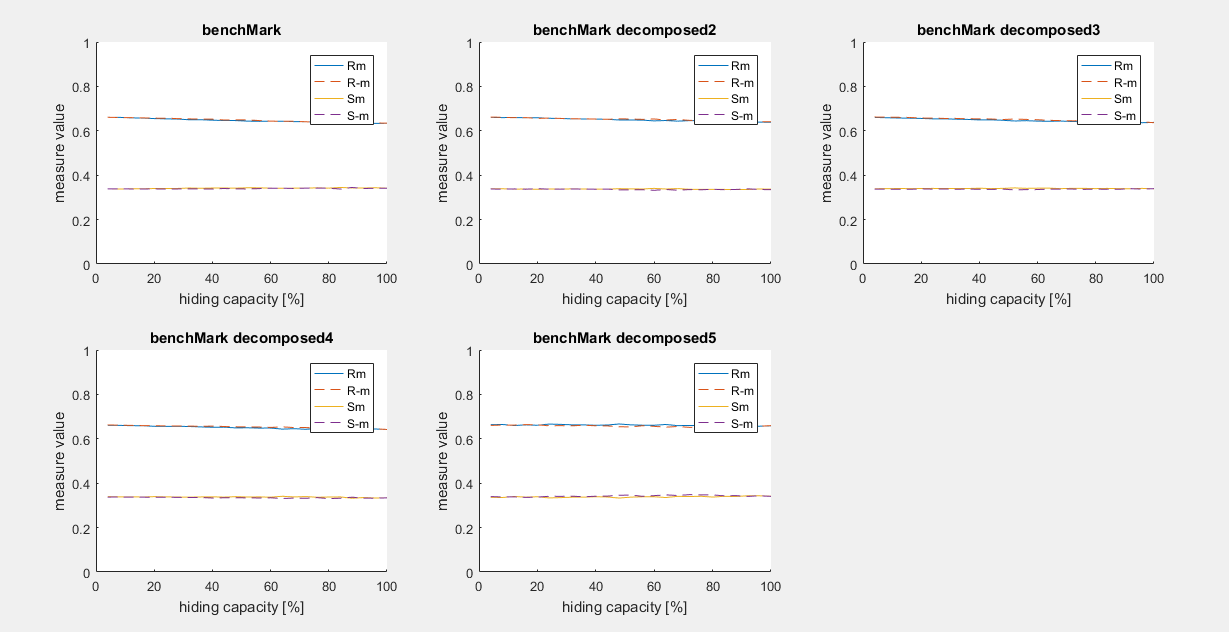


We notice that decomposed approaches have lower SSE, thus they are more secure

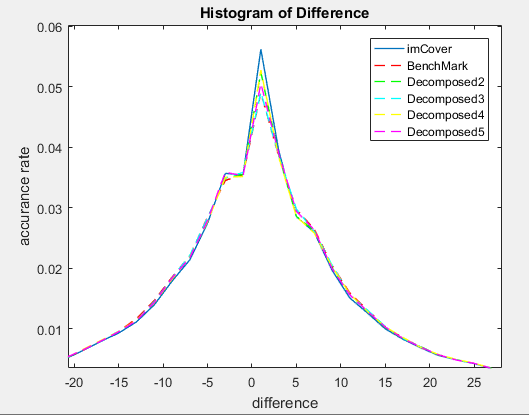


we notice that the MSE gets smaller as n (decomposition degree) gets higher

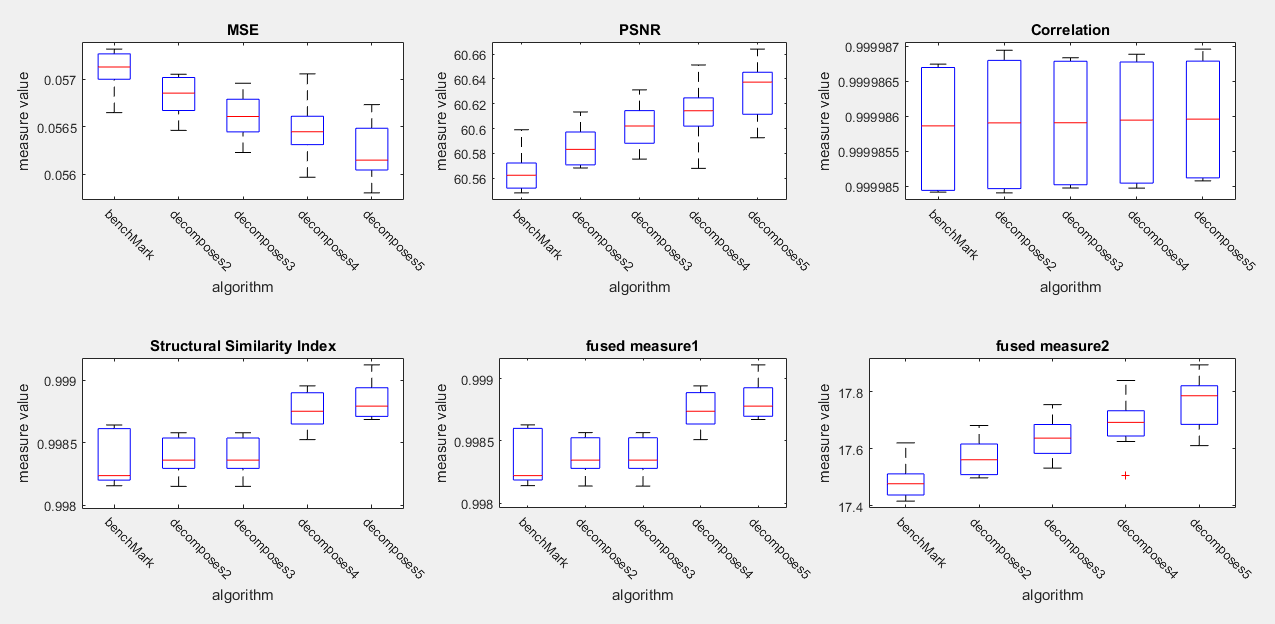
RS analysis

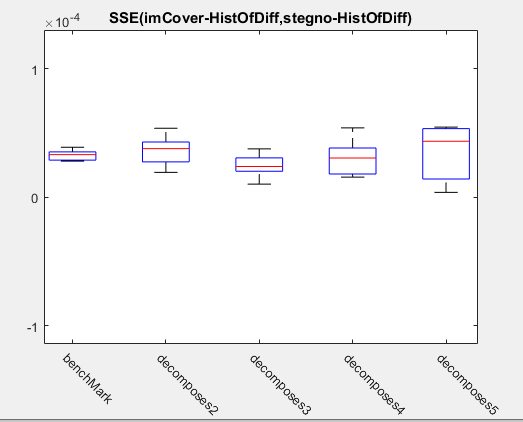


We notice that all algorithms are secure

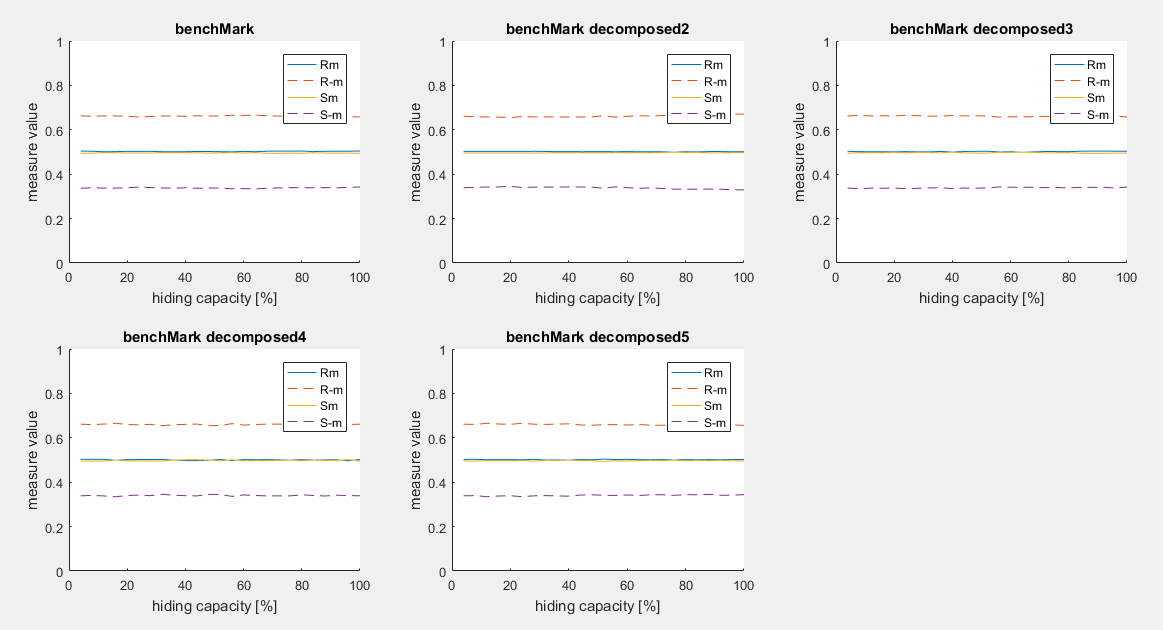


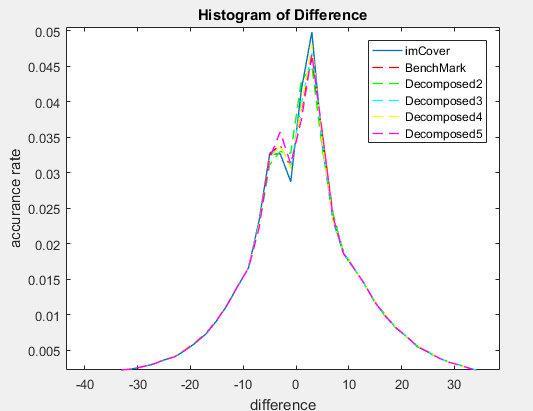
2-Rentina dataset



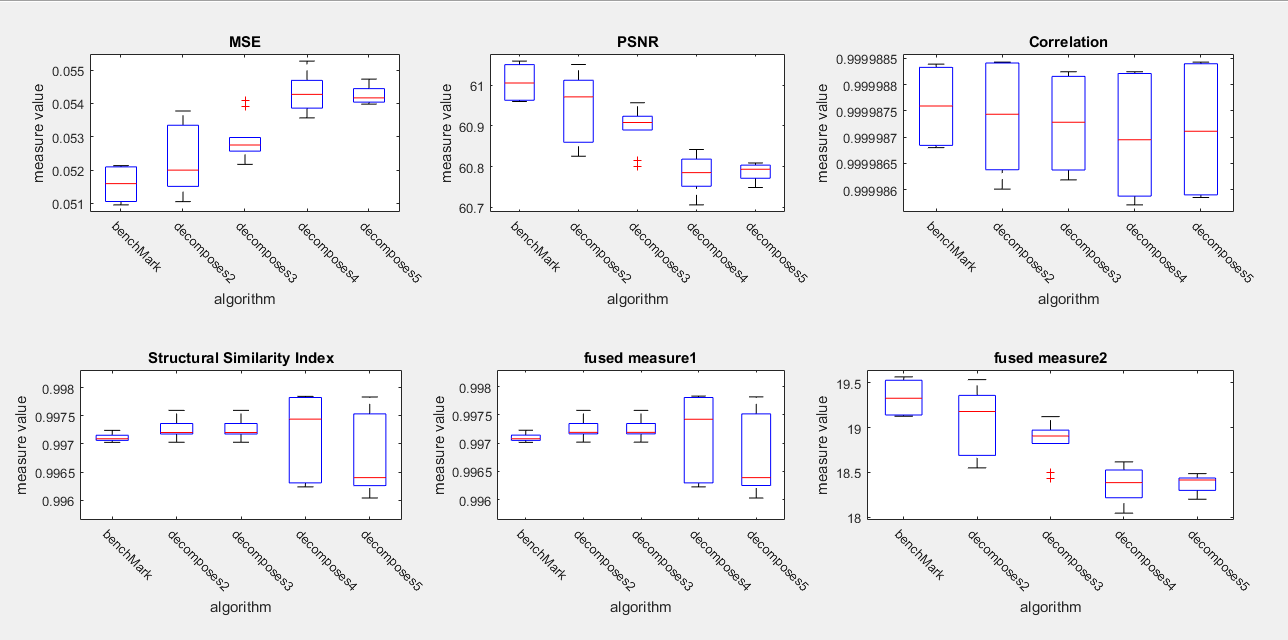




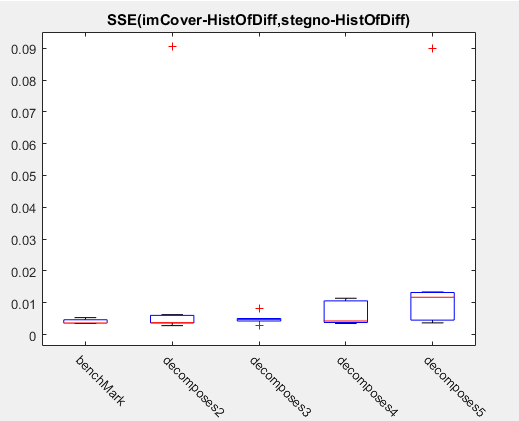


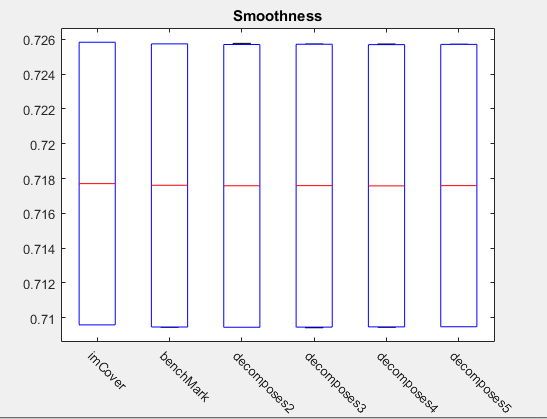


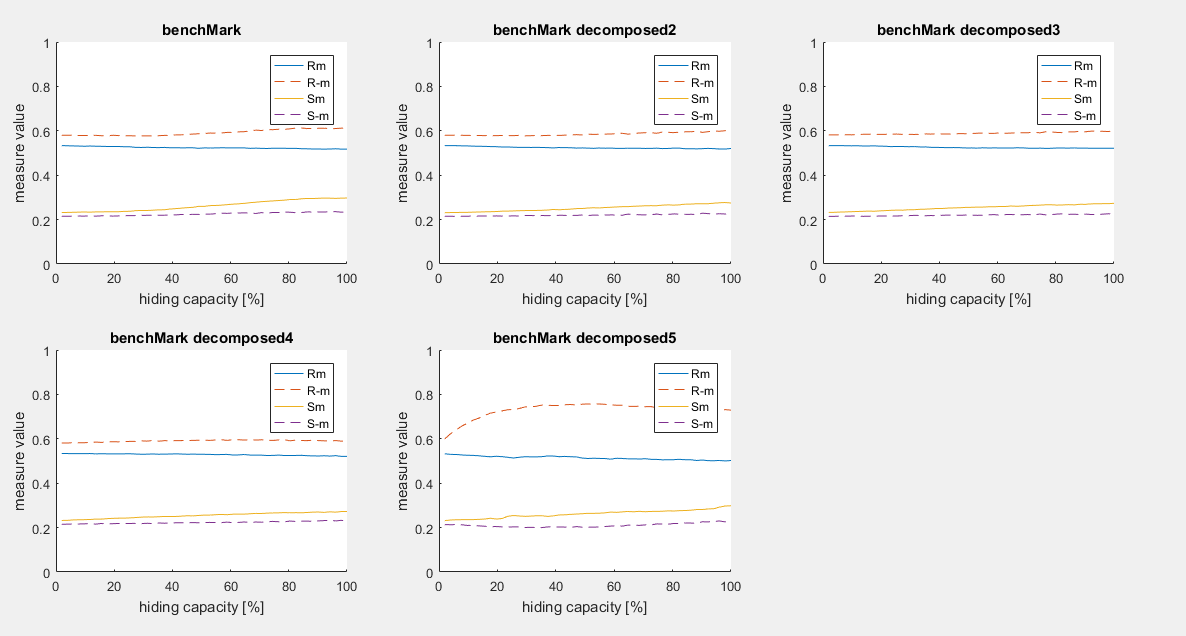
3-Brain dataset



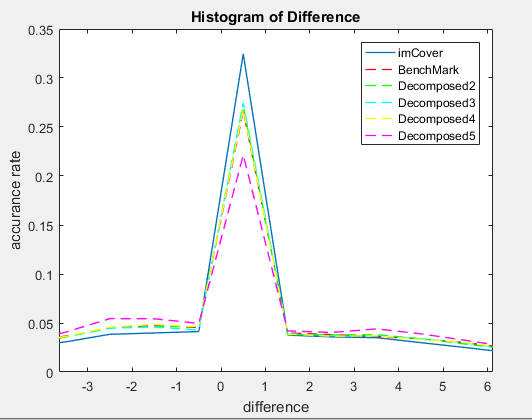
We notice that the MSE is higher in decomposed algorithms when we selected Brain dataset, and a possible reason is that brain images are more homogenius and have large black background, so the distribution of the message may damage the image by imbedding the secret bits in the background.







We see that all algorithms are not secure in term of RS analysis in Brain dataset



Conclusion:

* Decomposition of the message to n sub-messages gives better results in hetrogenious images, and the images that not contain a large background.
* A possibel solution for applying the decomposition algorithms in the images that have a large background is to avoid embidding the secret bits in the background that may be recognised by smoothness calculation.

Tracing Example:

In video folder