Simulation Steps and Matrix:

In my simulation to check Salsa20 and ChaCha20 performance, I have simulated the results using the below steps.

1. I have used 6 different types of data to check its performance.
   1. Int (ex: 12345)
   2. Float Int (ex: 123456578.999999\*\*\*\*\*\*\*\*\*)
   3. Small String Value (30 chars)
   4. Big String Value (1000 chars)
   5. Small File data (250 kb)
   6. Big File data (50 mb)
2. Apart from Salsa20, ChaCha20 I have worked on adding other ciphers to process this data. List of ciphers used for this experiment.
   1. Salsa20 – stream cipher
   2. ChaCha20 – stream cipher
   3. RC4 (ARC4)
   4. AES – block cipher
   5. (AES-CTR) – stream cipher implementation of AES.
3. I have gathered matrix of
   1. Memory consumption (after encryption) in kb
   2. Time takes between encryption and decryption in milli sec.
   3. Memory diff between original data and encrypted data in kb.
4. I have run each data type with each cipher nearly 50 times, for example I have sampled the recordings when the same small int with salsa20 for 50 times, I graphs will display the performance for the above-mentioned matrix.
5. All the code/sampled data results has been pushed into github
   1. <https://github.com/manogna1997/CS698>
6. The data that’s used to plot the graphs comes from the output of the cipher\_main.py file in the repository, I have also pushed the data used in charts to
   1. <https://github.com/manogna1997/CS698/tree/main/result>

Final Observation and Conclusion:

* The Memory consumption for ciphered data between all the 5 ciphered different extensively but when it comes to Salsa20 and ChaCha20 the margins are very small, where Salsa20 consumes about ~5% more then chacha20 but larger data gets the difference negligible if you check the charts for large file and Small file data.
* The time take between encryption and decryption for all the ciphers varied by data size like AES-CTR takes more time for larger data while AES cipher takes larger time for smaller data but is very competitive for larger data sets. When it comes to Salsa20 and Chacha20 both perform identical with different sets of data and generate constant results across various runs.
* Memory consumption difference between original data and ciphered data also varies by ciphers has AES has the lowest difference between original and ciphered data, while AES-CTR memory consumption increases with data size which you can see for big file data. While Salsa20 and ChaCha20 the difference between memories starts decreasing from smaller data set to larger data set for example, when you check small int charts the difference is notable about (25%) between Salsa20 and Chacha20 while big file data chart the difference is negligible.

Observation:

1. Small Int observation across 5 different ciphers.
   1. Memory size of a given data after encryption

Chart, bar chart, histogram

Description automatically generated

* 1. Time difference between encryption and decryption.

Chart, histogram

Description automatically generated

* 1. Memory difference between encryption and decryption data.

Chart, bar chart, histogram

Description automatically generated

1. Float Int observation.
   1. Memory size of a given data after encryption

Chart, bar chart, histogram

Description automatically generated

* 1. Time difference between encryption and decryption

Chart, histogram

Description automatically generated

* 1. Memory difference between encryption and decryption data.

Chart, bar chart, histogram

Description automatically generated

1. Small String observations across 5 different ciphers
   1. Memory size of a given data after encryption.

Chart, histogram

Description automatically generated

* 1. Time difference between encryption and decryption.

Chart, histogram

Description automatically generated

* 1. Memory difference between encryption and decryption data.

Chart, bar chart, histogram

Description automatically generated

1. Big String observations across 5 different ciphers.
   1. Memory size of a given data after encryption.

Chart, bar chart, histogram

Description automatically generated

* 1. Time difference between encryption and decryption.

Chart, bar chart

Description automatically generated

* 1. Memory difference between encryption and decryption data.

1. Small file observations across 5 different ciphers
   1. Memory size of a given data after encryption.

Chart, bar chart

Description automatically generated

* 1. Time difference between encryption and decryption.

Chart, histogram

Description automatically generated

* 1. Memory difference between encryption and decryption data

Chart, bar chart

Description automatically generated

1. Big file data observations across 5 different ciphers
   1. Memory size of a given data after encryption.

Chart, bar chart

Description automatically generated

* 1. Time difference between encryption and decryption
  2. Chart, histogram

     Description automatically generated
  3. Memory difference between encryption and decryption data

Chart, bar chart

Description automatically generated