A new chaos-based fast image encryption algorithm

Link to the paper:
https://www.sciencedirect.com/science/article/abs/pii/S1568494609002658?casa_token=jPTeOsHmS9MAAAAA:ZbIqN1NZWjGpUCKl61ob_swc_WiaZkvHaB2ZB68hKyzqtbhiVyb0WQLmYhAYD0wEpfHi0gmXdV8

Goals:

- Implement and optimize the generation of the pseudorandom sequences generation presented in section 2.
- Implement and optimize the encryption algorithm presented in section 3.1.
- For testing (checking if decrypting an encrypted image yields the original image), the decryption process (3.2) should be implemented. It shares a large part of the encryption process. This doesn't have to be optimized.

Example implementation in python: https://github.com/Dspil/chaos-encryption

Notes:

- The paper has some typos:
  - The cycL function (described in Step 4 (ii) of the encryption process) is a y-bit left shift on the binary sequence x (so that it is the reverse of cycR)
  - At equations (14) and (17) the '×' in the beginning of the new line should be ignored
  - Wherever C is used, C_k is meant to be written instead with one exception: at step 4(ii) of the encryption process where it says "For the first block B0 , C(−1, j) = K_{j+8}…. There it should be C_0.
  - The numbering of the decryption process is a bit wrong (number 4 is used twice)
  - In step 6 (called step 5) of the decryption process it should write "in reverse order of Step 3 in encryption" (instead of Step 2)
- The chaotic map 'f' is defined in equation (2) (x_{i+1} is in reality $f(x_i)$)
- In the encryption process, steps 4(i)-(iv) are done for every block but 4(v) is done only after all blocks are processed (In the encryption diagram at Fig 5. this is more clear)
- The same holds for the decryption process although there it is more clear that the steps that are being repeated are the steps 4(ii) to 4(v).
- IMPORTANT: The way this algorithm is presented, the decryption doesn't work for R > 1. The only way to repeat the encryption process multiple times is to restart the NCML every time. This means that the implementation will either:

- Work for R = 1 and ignore step 5 of the encryption process and step 5 (written as the second step 4) in the decryption process
- Reset the NCML to the original value after each encryption/decryption round which is equivalent of calling encrypt/decrypt R times on the original image