OFFICIAL ABSTRACT and CERTIFICATION

Using RGB Pixel Data to Generate a Stream of True Random Numbers for Encryption

Ikey Croog
North Shore Hebrew Academy H.S., Great Neck, NY, USA

The encryption that protects important bank and security information currently relies on the generation of random numbers. The mainstream way of generating numbers used in encryption uses pseudo-random number generators (PRNG) and not real random processes of generating random numbers. PRNGs use a specific random number called a “seed” to start the process of generating seemingly random numbers which if it were to be known could allow for the encryption to be broken. True random number generators (TRNG) are an alternative generator that uses random processes such as the noise in audio files or visible light. The data from individual pixels RGB values in a random image can be averaged or multiplied together to give a random number. The algorithm can then move to a pixel mod X of the first pixel. This next pixel’s RGB values can also be averaged and then multiplied with the original pixels averaged number. This process can be repeated several times. Although picture TRNGs exist, this algorithm differs. Unlike other picture TRNGs, this algorithm can generate multiple numbers from one picture and not just one number per image. The algorithm is also a cross between a TRNG and a PRNG because the initial image acts as a seed but also is random in its own right. This algorithm is also safer because generating the same numbers would not only require the same image, but also the starting pixel and the mod X by which the algorithm moves by.

Category
Pick one only—
mark an “X” in box
at right

Animal Sciences	☐
Behavioral & Social Sciences	☐
Biochemistry	☐
Biomedical & Health Sciences	☐
Biomedical Engineering	☐
Cellular & Molecular Biology	☐
Chemistry	☐
Computational Biology & Bioinformatics	☐
Earth & Environmental Sciences	☐
Embedded Systems	☐
Energy: Chemical	☐
Energy: Physical	☐
Engineering Mechanics	☐
Environmental Engineering	☐
Materials Science	☐
Mathematics	☐
Microbiology	☐
Physics & Astronomy	☐
Plant Sciences	☐
Robotics & Intelligent Machines	☐
Systems Software	■
Translational Medical Sciences	☐

1. As a part of this research project, the student directly handled, manipulated, or interacted with (check ALL that apply):

   ☐ human participants ☐ potentially hazardous biological agents

   ☐ vertebrate animals ☐ microorganisms ☐ rDNA ☐ tissue

2. I/we worked or used equipment in a regulated research institution or industrial setting: ☐ Yes ■ No

3. This project is a continuation of previous research. ☐ Yes ■ No

4. My display board includes non-published photographs/visual depictions of humans (other than myself): ☐ Yes ■ No

5. This abstract describes only procedures performed by me/us, reflects my/our own independent research, and represents one year’s work only ■ Yes ☐ No

6. I/we hereby certify that the abstract and responses to the above statements are correct and properly reflect my/our own work. ■ Yes ☐ No

This stamp or embossed seal attests that this project is in compliance with all federal and state laws and regulations and that all appropriate reviews and approvals have been obtained including the final clearance by the Scientific Review Committee.