INTERNATIONAL CENTRE
OF EXCELLENCE FOR
EDUCATION IN
MATHEMATICS

Characterising random number generation from images
Nicholas Gladwin, Department of Mathematics, University of Queensland

I spent my AMSI scholarship studying a process of generating random numbers from images. The output of common random number generators (RNGs) are called pseudo-random numbers because they are based on an algorithm. They all require a seed (typically a number), which if recorded, can be used to recreate the same 'random' numbers repeatedly. This, while clearly a problem, is not really that serious for most applications of random numbers (ie. simulations, etc.) but with the case of security passwords and the like it does represent a risk.

Taking a different approach, Dr. Bulmer and Dr. Pimblet had developed a procedure whereby images could be used as a source for random numbers. Rather than creating another seed based algorithm it was aimed towards extracting what is presumed to be physical randomness in the form of camera noise. Initially these images were from radio telescopes thus the noise was cosmic radiation but due to the relatively small amount of information in a space photo compared to that of a regular photo, basing the generator on regular photos should be far more efficient.

Although it seemed any photo (digital) could be used, after the data was de-skewed some images resulted in only several thousand bits of acceptably random numbers. The purpose of my research project was to investigate how image conditions effected the efficiency of the process (which in terms of quantity is well behind pRNGs) to determine optimum conditions for both high final quantity and quality of bits. This involved coding several statistical tests of randomness to analyse how different images fared and automating the procedure. Similarities could then be recognised between 'successful' images to ultimately give a set of recommended properties for a candidate image.

My experience was very positive and I would definitely recommend the summer program to prospective students. It provided me with a chance to work on something which was not likely to turn up in regular coursework and also to get a taste of future study possibilities.

Nicholas received an ICE-EM Vacation Scholarship in January 2005.
See www.ice-em.org.au/students.html#scholarship.