Rastgele Sayı Üreteçleri İçin NIST İstatistiksel Test Paketi

Tunahan Gökçimen

185541005

- NIST TESTİ KAPSAMINDA 1’ er milyonluk veri setine uygulanacak 15 ayrı NIST testi:
- 1. Frekans (monobit) testi
- 2. Bir blok içinde frekans testi
- 3. Akış (Runs) testi
- 4. Bir blok içinde en-uzun-birlerin akış (longest-run-of-ones) testi
- 5. İkili matris rankı testi
- 6. Ayrık Fourier dönüşümü (spektral) testi
- 7. Örtüşmeyen şablon eşleştirme (Non-overlapping template matching) testi
- 8. Örtüşen şablon eşleştirme (Overlapping template matching) testi
- 9. Maurer’in “Evrensel İstatistik” testi
- 10. Doğrusal karmaşıklık (linear complexity) testi
- 11. Seri (serial) test
- 12. Yaklaşık entropi (approximate entropy) testi
- 13. Kümülatif toplamlar (cumulative sums – cusums) testi
- 14. Rasgele gezinimler (random excursions) testi
- 15. Rasgele gezinimler değişken (random excursions variant) testi

Örnek Test Sonuçları

	Veri
frekans testi	1
blokataki en uzun birler testi	1
örtüşmeyen şablon eşleştirme testi	1
doğrusal karmaşıklık testi	1
birikimli toplamlar testi	1
blok frekans testi	1
rank testi	1
örtüşen şablon eşleştirme testi	1
seri testi	1
rastgele gezinim testi	1
akış testi	1
ayrık fourier dönüşüm testi	1
maurer's evrensel testi	1
yaklaşık entropi testi	1
rastgele gezinim değişken testi	1
Toplam Başarı Sayısı	15

1’ er milyonluk veri setinin NIST test sonuçları yanda gösterilmektedir.

Testler	Veri
frekans testi	p_value = 0,5974
blokataki en uzun birler testi	p_value = 0,6119
örtüşmeyen şablon eşleştirme testi	p_value = 0,7792
doğrusal karmaşıklık testi	p_value = 0,1055
birikimli toplamlar testi	p_value = 0,3099
blok frekans testi	p_value = 0,1658
rank testi	p_value = 0,48013
örtüşen şablon eşleştirme testi	p_value1 = 0,6371
seri testi	p_value = 0,0236
rastgele gezinim testi	p_value = 0,5657
akış testi	p-value = 0,2284
ayrık fourier dönüşüm testi	p-value = 0,3239
maurer's evrensel testi	p-value = 0,2830
yaklaşık entropi testi	p-value = 0,2339
rastgele gezinim değişken testi	p-value = 0,4200

Elde edilen P değerleri önem değeri olan 0,01‘ den büyük olduğu için testleri başarıyla geçmiştir.

Tüm testleri başarılı olarak tamamlayan veri setlerinin rastgeleliği kanıtlanmış olup verilerin güvenliği için şifreleme algoritmalarında anahtar olarak kullanılabileceği sonucuna ulaşılmıştır.

Nist Testi Gerçekleştirme Adımları