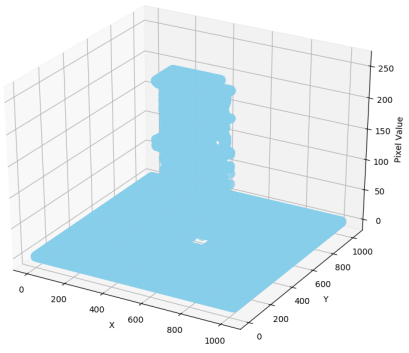
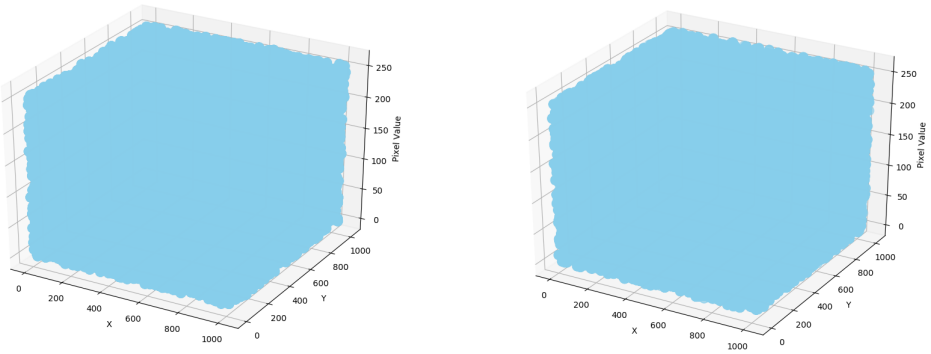


Gambar 5. Distribusi dari Nilai Piksel pada *Plain Image*

Jika terdapat dua piksel yang dienkripsi dengan kunci yang sama, penyerang masih dapat memulihkan selisih antara dua piksel tersebut. Dengan demikian, mereka dapat mengembalikan gambar dari informasi nilai selisih. Untuk mengamankan hal ini, algoritma permutasi dinamis diterapkan mengikuti Persamaan 2. Persamaan ini berfungsi untuk mengacak urutan dari sub-blok sehingga penyerang kesulitan untuk memperoleh pola jika ingin mengembalikan gambar seperti semula. Untuk mengembalikan seperti gambar asli, penyerang harus mengembalikan pengaturan asli (pola permutasi) dari sub-blok. Namun, untuk mendapatkan gambar yang dienkripsi menggunakan *stream encryption*, penyerang harus melakukan inversing dari permutasi. Untuk menebak permutasi tersebut, penyerang harus mencoba menebak paling banyak N! dimana *N* adalah jumlah sub-blok yang dibagi. Dengan demikian, itu akan meningkatkan keamanan dibandingkan dengan metode Huang, Shi.



((a)) SI ((b)) PSI

Gambar 6. Dsitribusi Nilai Pixel a) *Stream Image* b) *permuted Image*

Misalkan ”Gambar 1” digunakan sebagai gambar uji, maka distribusi nilai pixel dari gambar uji. Setelah proses enkripsi distribusi piksel dapat dilihat pada gambar 6(a), sementara setelah permutasi dinamis distribusi piksel dapat dilihat pada gambar 6(b). Sumbu X, sumbu Y dan sumbu Z pada gambar 6 adalah indeks baris, indeks kolom, dan nilai piksel dari gambar uji. Dalam proses *stream encryption*, kami melakukan *xor* pada setiap piksel dengan kunci yang dihasilkan, sehingga nilai piksel dari gambar yang terenkripsi terdistribusi secara merata dalam kisaran [0,255], yang serupa dengan hasil gambar 6(a) dan (b) . Itu berarti tanpa kunci permutasi, penyerang tidak dapat mengembalikan sub-blok permutasi sesuai dengan nilai piksel yang dienkripsi. Dengan kata lain, penyerang tidak dapat mengembalikan pengaturan sub-blok dari gambar yang dienkripsi.