

## ABSTRAK

Data gambar digital yang disimpan dan dipertukarkan dalam *cloud storage* dapat diamankan menggunakan teknik kriptografi dan steganografi. Informasi yang terdapat dalam suatu data diamankan agar terhindar dari pengambilan data atau informasi dari pihak yang tidak berkepentingan. Proses enkripsi dilakukan dengan mengubah data gambar asli dari yang dapat dimengerti menjadi tidak dapat dimengerti. Enkripsi menggunakan Algoritma *Arnold Transformation* yang mengacak piksel data gambar dengan menggunakan 4-bit Most Significant gambar hidden untuk kemudian disisipkan ke dalam 4-bit *Least Significant Cover* yang telah terenkripsi. *Peak Signal to Noise* (PSNR) digunakan untuk membandingkan kualitas gambar sebelum dan sesudah diekstrasi. Perbandingan ini berdasarkan hasil uji nilai kesalahan rata-rata atau *Mean Square Error* (MSE) dari data gambar asli dan data gambar penyisipan yang dihasilkan. PSNR yang dihasilkan pada penelitian ini diatas nilai standar minimal (40 dB) yaitu antara 45,60 dB – 46,10 dB, serta nilai distorsi yang dihasilkan sangat kecil ( $MSE > 2$ ). Dengan penggunaan penyisipan 4-bit terhadap data gambar yang ada, maka hasil ekstrasi gambar tidak jauh berbeda dengan dengan gambar hidden sebelum dilakukan penyisipan dan dapat diidentifikasi hasilnya. Sehingga penggunaan algoritma Arnold Transform dan *Position Power First Mapping* (PPFM) mengurangi distorsi dan perbedaan serta kemungkinan kebocoran data dari data gambar yang dihasilkan.

**Kata Kunci :** Algoritma *Arnold Transform*, *Position Power First Mapping*, Kriptografi, Steganografi