

**TUGAS**  
**KRIPTOANALISIS**  
“Review Paper 2”



**Dosen Pengampu:**  
I Komang Ari Mogi, S.Kom., M.Kom.

**Disusun Oleh:**  
Kelompok 4  
Sang Putu Febri Wira Pratama      1808561012  
Muhammad Akbar Hamid      1808561064

**PROGRAM STUDI INFORMATIKA**  
**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM**  
**UNIVERSITAS UDAYANA**  
**2021**

#### A. Identitas artikel

1. Judul : A Secure Data Communication System  
Cryptography And Steganography
2. Tahun : 2013
3. Penulis : Saleh Saraireh
4. Jurnal/Prosiding : International Journal of Computer Networks &  
Communications (IJCNC)
5. Volume & Halaman : Vo. 5 No. 3 & Hal. 125 – 137
6. Reviewer : 1. Sang Putu Febri Wira Pratama (1808561012)  
2. Muhammad Akbar Hamid (1808561064)
7. Tanggal : Minggu, 06 Juni 2021

#### B. Hasil review

##### 1. Tujuan Penelitian

Tujuan utama yang dilakukan peneliti adalah untuk memperkenalkan sistem komunikasi aman yang menggunakan kriptografi dan steganografi untuk mengenkripsi dan menyematkan pesan rahasia yang akan dikirimkan melalui saluran yang tidak aman. Dalam sistemnya, proses enkripsi dilakukan dengan menggunakan *filter bank cipher*, yang menghadirkan kecepatan dan tingkat keamanan yang tinggi. Proses *embedding* akan dilakukan dengan menggunakan steganografi berbasis transformasi wavelet diskrit.

##### 2. Objek atau Data Penelitian

Penelitian yang dilakukan oleh penulis tersebut mengangkat masalah *security*, *integrity*, *originality*, dan *data confidentiality* pada citra berupa gambar berukuran yang didistribusikan dalam jaringan internet dengan menyisipkan sebuah pesan pada *cover image* dengan menggunakan konsep *Steganography* dan *Cryptography*. Ada lima citra gambar yang digunakan, yaitu *Cameraman*, *Lenna*, *Peppers*, *House*, dan *Baboon* yang masing-masing berukuran 256px x 256px

##### 3. Metode Penelitian

Metode utama sistem yang akan digunakan oleh peneliti terdiri dari empat tahapan, yaitu enkripsi, embedding, ekstraksi dan dekripsi. Algoritma kriptografi yang digunakan pada proses enkripsi dan dekripsi adalah filter bank cipher over sedangkan untuk proses steganografi yang digunakan pada proses penyematan dan ekstraksi adalah berbasis *discrete wavelet transform* (DWT) untuk menyembunyikan pesan menggunakan algoritma wavelet haar transformasi wavelet guna mengubah domain spasial menjadi domain frekuensi.

#### 4. Hasil Penelitian

Hasil dari penelitian ini dimana pesan yang telah diinputkan kemudian dienkripsi menggunakan skema *cryptography Filter Bank and Lifting*. Setelah itu, disisipkan ke *cover image* dengan metode *steganography Discrete Wavelet Transform* dan dikirimkan ke penerima. *Citra stego* yang dihasilkan diuji dengan analisis PSNR dan *histogram*. Hasil pengujian yang dilakukan dengan metode PSNR didapat nilai yang lebih besar dari 36 dB sehingga dapat dikatakan kombinasi dua metode tersebut sudah baik. Kemudian pengujian yang dilakukan dengan analisis *histogram* juga tidak mengalami perubahan signifikan antara *histogram cover image* dengan *citra stego*.

#### 5. Kesimpulan

Peneliti ingin mengkombine sistem kriptografi dan steganografi untuk mengenkripsi dan menyematkan pesan rahasia guna memperkenalkan sistem komunikasi yang aman. Proses enkripsi yang dilakukan menggunakan filter bank cipher sedangkan untuk proses embedding menggunakan steganografi berbasis DWT. Peneliti menggunakan objek citra berupa gambar yang terdapat pada jaringan internet dengan menyisipkan sebuah pesan pada *cover image*. Peneliti menggunakan empat tahapan utama yang akan dilakukan, yaitu enkripsi, embedding, ekstraksi dan dekripsi. Sistem yang diusulkan dengan hasil yang diberikan pada simulasi menunjukkan bahwa sistem memberikan tingkat keamanan yang tinggi dengan dasar pada evaluasi menggunakan PSNR dengan nilai yang lebih besar dari 36 db sehingga dapat dikatakan kombinasi dua metode yang dikombine sudah baik.

#### 6. Saran

*Reviewer* dapat mengajukan saran untuk mencoba melakukan *rotate*, *kompresi*, dan *crop* pada *citra stego* untuk memastikan *ciphertext* yang telah disisipkan yang ada pada citra tersebut tidak mengalami kerusakan. Metode lain yang dapat dikombinasikan, yaitu *Singular Value Decomposition*. *Singular Value Decomposition* biasa digunakan dalam *watermarking* karena nilai-nilai singular dari suatu citra memiliki stabilitas yang baik.