Jurnal Elektronik Ilmu Komputer Udayana
Volume 13, No 1. August 2024

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Penyisipan Digital Signature Ke Dalam Citra Digital Sebagai Keamanan Hak Cipta Dengan Metode DES dan BPCS

Michael Tanaya.[a1], I Gede Arta Wibawa.[a2], I Made Widiartha.[b3], Luh Gede Astuti.[b4]

[a]Informatika, Universitas Udayana
Kuta Selatan, Badung, Bali, Indonesia
[1]michaeltanaya94@gmail.com
[2]gede.arta@unud.ac.id (Corresponding author)

[b]Informatika, Universitas Udayana
Kuta Selatan, Badung, Bali, Indonesia
[3]madewidiartha@unud.ac.id
[4]lg.astuti@unud.ac.id

Abstrak

Dalam era digital saat ini, distribusi dan reproduksi konten digital menjadi sangat mudah, sehingga keamanan hak cipta citra menjadi isu yang semakin penting. Untuk melindungi integritas dan keaslian citra digital, penyisipan tanda digital telah menjadi pilihan yang efektif sebagai tanda integritas dan keaslian dari dokumen tersebut. Penelitian ini mengusulkan pendekatan inovatif yang menggabungkan metode Data Encryption Standard (DES) dan Bit-Plane Complexity Segmentation (BPCS) untuk menyisipkan tanda digital ke dalam citra digital guna meningkatkan keamanan hak cipta. Pada tahap pertama, tanda digital dienkripsi menggunakan algoritma DES untuk memastikan kerahasiaan data sebelum penyisipan. Tahap berikutnya melibatkan penerapan metode BPCS, di mana tanda digital yang telah dienkripsi disisipkan ke dalam bit-bit rendah signifikan citra digital. Keunggulan metode BPCS terletak pada kemampuannya menyisipkan data tanpa mengorbankan kualitas visual citra secara signifikan, menjaga estetika visual yang penting dalam konteks hak cipta. Dengan menggabungkan kedua metode ini, diharapkan citra digital dapat dilindungi secara lebih efektif dari ancaman pembajakan atau manipulasi yang mengancam hak cipta.

Keywords: *Penyisipan tanda digital, citra digital, keamanan hak cipta, Data Encryption Standard (DES), Bit-Plane Complexity Segmentation (BPCS).*

1. Pendahuluan

Pada Era Revolusi Industri 4.0, penggunaan teknologi digital semakin berkembang di berbagai sektor, mulai dari bisnis hingga pemerintahan. Maka dari itu, keamanan data digital menjadi isu yang semakin penting, karena data digital sangat mudah untuk disalin, dipalsukan dan dimodifikasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, banyak teknologi pengamanan telah dikembangkan, salah satunya adalah digital signature.

Digital signature adalah tanda digital yang berfungsi sebagai penanda kepemilikan sebuah dokumen digital. Digital Signature memungkinkan seseorang untuk memastikan keaslian dan integritas dokumen digital tersebut. Dalam sistem, digital signature hanya diketahui oleh pemilik dokumen, dikarenakan terdapat sebuah kunci rahasia yang digunakan untuk menghasilkan nilai hash atau tanda digital dari dokumen tersebut.[6] Nilai hash ini yang kemudian disisipkan ke dalam dokumen sebagai suatu tanda digital. Namun, dalam beberapa kasus, digital signature masih rentan terhadap serangan oleh pihak yang

tidak bertanggung jawab. Salah satu serangan yang mungkin terjadi adalah serangan man-in-the-middle (MITM), dimana pihak yang tidak bertanggung jawab akan memodifikasi tanda digital pada dokumen tersebut sehingga dokumen tersebut terlihat sah meskipun sebenarnya telah dimodifikasi. Untuk mengatasi masalah ini, teknologi bernama steganografi dapat digunakan untuk menyisipkan digital signature pada citra digital.[3]

Steganografi adalah suatu teknik yang digunakan untuk menyembunyikan suatu pesan atau informasi rahasia dalam sebuah media yang tampak normal. Citra digital adalah salah satu media yang sering digunakan untuk penyisipan pesan atau informasi rahasia.

Dalam proposal ini, akan membahas mengenai penyisipan digital signature ke dalam citra digital sebagai keamanan hak cipta menggunakan metode Bit-Plane Complexity Segmentation (BPCS). Metode BPCS adalah salah satu teknik steganografi yang menggunakan analisis kompleksitas bit-plane dalam citra digital untuk menyisipkan pesan rahasia.[2] Dalam kasus ini, digital signature akan disisipkan pada bit-plane yang memiliki kompleksitas tertentu se\hingga tidak merusak kualitas visual dari citra digital tersebut. [5]

Pada penelitian sebelumnya, metode BPCS ini digunakan untuk menyisipkan sebuah pesan rahasia pada pas foto digital. Dimana pesan yang digunakan pada penelitian sebelumnya itu adalah sebuah teks, sehingga pada penelitian ini akan digunakan digital signature berformat image untuk nantinya disisipkan pada sebuah citra digital.

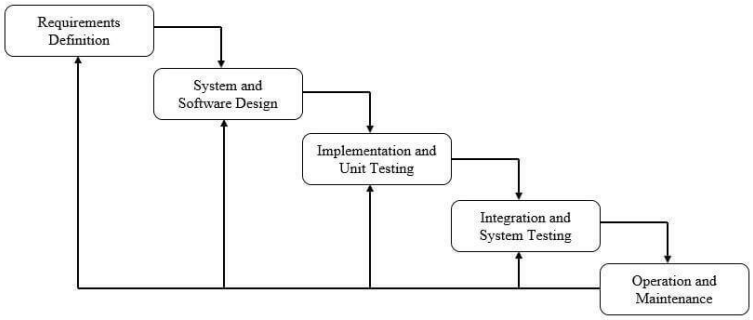
Penyisipan digital signature pada citra digital dengan menggunakan steganografi dapat meningkatkan keamanan dokumen digital dengan cara menyembunyikan informasi rahasia yang penting.[8] Oleh karena itu, proposal ini diharapkan dapat memberikan kontribusi dan manfaat dalam pengembangan teknologi keamanan informasi khususnya pada penggunaan digital signature. Selain itu, dengan adanya proposal ini, diharapkan dapat memicu minat untuk pengembangan teknologi steganografi pada digital signature di Indonesia.

.

2. Metodologi Penelitian

2.1 Metode Pengembangan Sistem

Aplikasi steganografi ini menggunakan metode pengembangan sistem Waterfall Mode. Alur pengembangan sistem dengan metode waterfall dapat dilihat pada gambar 1 :



Gambar 1. Waterfall Method

Berikut adalah penjelasan dari gambar 1 untuk setiap proses yang ada di dalam pengembangan sistem menggunakan metode Waterfall :

2.1.1 Requirement Definition

Pada tahapan ini melakukan persiapan dan analisa kebutuhan sistem yang ingin dikembangkan. Persiapan dan analisa sistem seperti, persiapan data,

p-ISSN: 2301-5373
e-ISSN: 2654-5101

manfaat dari sistem yang akan dibuat dan batasan-batasan dari sistem yang akan dibuat.

2.1.2 System and Software Design.
Pada tahapan ini melakukan proses perancangan desain sistem dengan menggunakan diagram UML seperti, use case diagram, flowchart dan activity diagram.

2.1.3 Implementation
Pada tahapan ini merupakan tahapan gambaran sistem ke dalam bentuk code. Jadi pada tahapan ini lebih berfokus pada hal teknis dari hasil desain yang telah dibuat pada tahap sebelumnya dan desain tersebut akan diterjemahkan ke dalam bahasa pemrograman.

2.1.4 System Testing
Pada tahapan ini sistem yang telah dibuat akan diuji dari berbagai sisi baik dari aspek desain dan fungsionalitas. Dengan tujuan untuk menentukan apakah terjadi kesalahan pada sistem yang telah dibuat , dimana jika ada kesalahan masih bisa dicegah dan diperbaiki kembali.

2.1.5 Operation and Maintenance
Pada tahapan ini merupakan tahapan pemeliharaan sistem yang mencakup perbaikan kesalahan seperti bug, error, dan penambahan fitur-fitur pada sistem yang telah dibuat.

2.2 Variabel Penelitian

Dalam penelitian ini terdapat dua variabel, yaitu variabel bebas dan variabel terikat. Variabel bebas pada penelitian ini adalah digital signature yang dienkripsi menjadi file txt dan file image dengan format **.jpg, *.png* dan **jpeg.* Sedangkan variabel terikat pada penelitian ini adalah file steganografi dengan format **png.*

2.3 Data Penelitian

Data penelitian yang digunakan berdasarkan cara memperolehnya yaitu data primer dan data sekunder. Data primer adalah data yang diperoleh peneliti secara langsung yaitu digital signature berbentuk image. Data sekunder adalah data yang diperoleh dari berbagai sumber yang telah ada, seperti sebuah foto hasil dari pengambilan gambar oleh seorang photographer.

2.4 Skenario Pengujian

Skenario pengujian pada penelitian ini bertujuan untuk mengukur kualitas dari citra yang telah dimodifikasi dengan citra asli. Citra yang dimodifikasi akan lebih baik jika citra yang telah dimodifikasi tersebut menyerupai aslinya, agar kualitas citra tetap terjaga. Perhitungan Mean Square Error (MSE) ini diperlukan untuk mengetahui besarnya error yang dihasilkan dari proses penyisipan. Perhitungan ini dilakukan untuk setiap piksel dalam citra. MSE yang dihitung adalah MSE dari hasil citra yang telah di steganografi dan citra asli memiliki hasil yang mendekati sama dengan citra asli.

Pada perhitungan Peak Signal Noise Ratio (PSNR) ini diperlukan untuk membandingkan citra hasil dengan citra asli. Dimana dengan semakin tinggi nilai PNSR maka citra yang dimodifikasi mirip dengan citra aslinya.

2.4.1 Mean Square Error (MSE)

Pengujian nilai error kuadrat rata-rata antara citra asli dengan citra hasil modifikasi

2.4.2 Peak Signal Noise Ratio (PSNR)

Metode pengujian untuk menghitung rasio antara nilai maksimum yang mungkin dari sebuah sinyal dan kekuatan gangguan distorsi yang mempengaruhi kualitas representasinya.

3. Hasil dan Pembahasan

3.1 Implementasi Tampilan

Pada tahap implementasi, website yang telah dibuat akan dijalankan pada server local. Dimana ketika website dibuka, maka akan memunculkan halaman tampilan awal yang berisi sebuah pesan welcome untuk user.

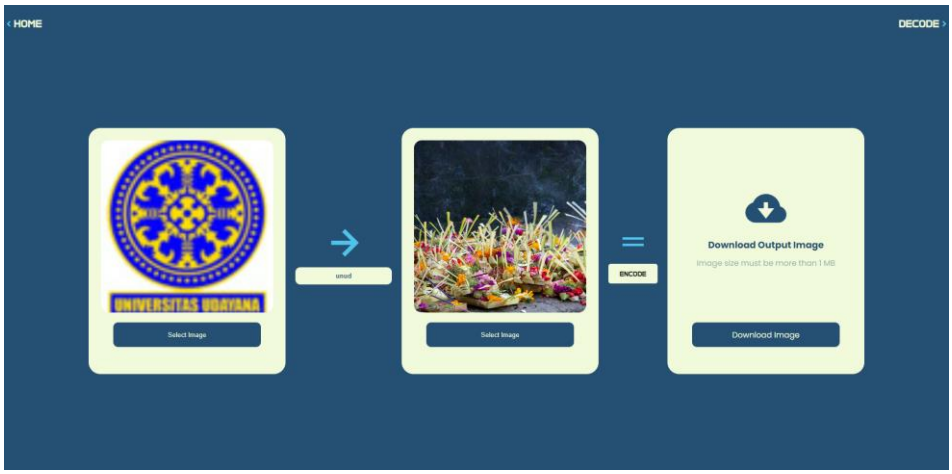
Gambar 2. Tampilan Halaman Home

Bisa dilihat pada gambar 2 diatas. Pada tampilan awal website user akan menemukan sebuah kalimat welcome dan tombol yang akan mengarahkan user ke halaman encode. Setelah user meng-klik tombol tersebut, maka user akan diarahkan ke halaman encode seperti gambar berikut :

Gambar 3. Tampilan Halaman Encode

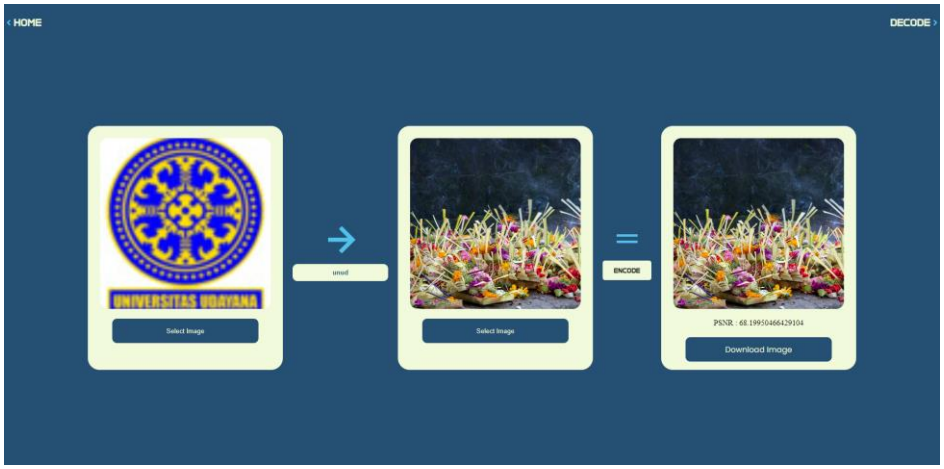
p-ISSN: 2301-5373
e-ISSN: 2654-5101

Bisa dilihat pada gambar 3 diatas. Ketika user sudah berada di halaman ini maka user sudah bisa melakukan penyisipan digital signature ke dalam citra digital.



Gambar 4. Tampilan Halamn Encode dengan Input Image

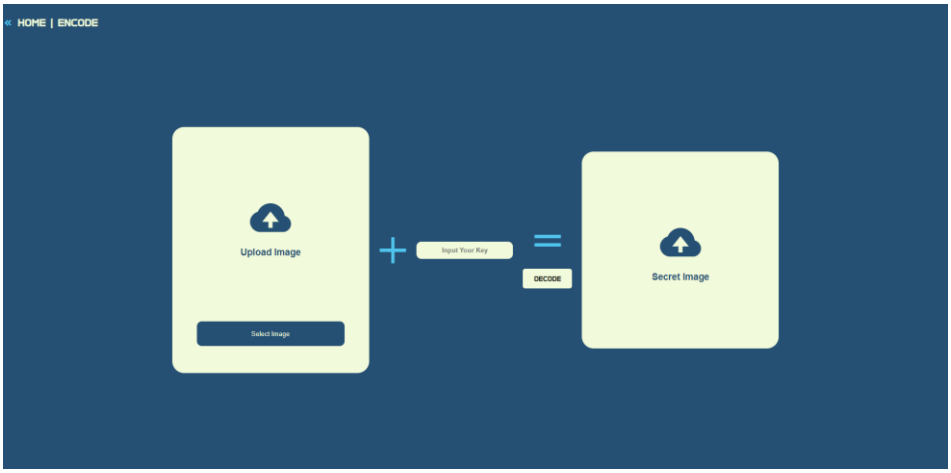
Bisa dilihat pada gambar 4 diatas. Untuk percobaan proses penyisipan digunakan file gambar sebuah desain yang dibuat oleh salah satu mahasiswa unud dan pesan yang disisipkan berupa logo unud sebagai digital signature dari desain mahasiswa tersebut.



Gambar 5. Tampilan Halaman Encode dengan Hasil Image Penyisipan

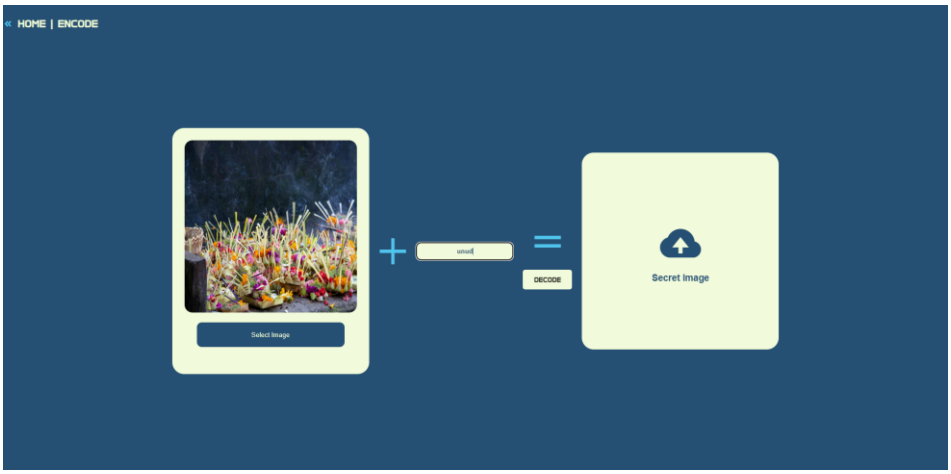
Bisa dilihat pada gambar 5 diatas. Jika proses enkripsi dan encode berjalan lancar maka akan tampil sebuah gambar. Dimana gambar tersebut adalah stego image yang dikeluarkan sebagai hasil oleh website tersebut, sehingga stego image tersebut dapat di download. Untuk pengujian digunakan pengujian Peak Signal to Noise Ratio (PSNR) yang membandingkan antara nilai sinyal yang diukur dengan besarnya error yang berpengaruh pada sinyal tersebut atau untuk mengetahui perbandingan kualitas citra asli dan citra stegano yang ada dalam satuan deciel (dB).[7] Sebelum menghitung PSNR, nilai error harus dicari telebih dahulu dengan perhitungan Mean Square Error (MSE). Untuk hasil uji dari citra desain tersebut dapat dilihat ketika proses enkripsi dan encode berhasil dilakukan. Untuk hasilnya dapat dilihat pada gambar diatas. Dari pengujian

diatas didapatkan nilai PSNR yaitu 68.19950466429104, dimana kualitas stegano image yang baik berada pada nilai diatas 40dB. Jadi dapat disimpulkan bahwa hasil penyisipan digital signature pada gambar desain tersebut berkualitas baik.



Gambar 6. Tampilan Halaman Decode

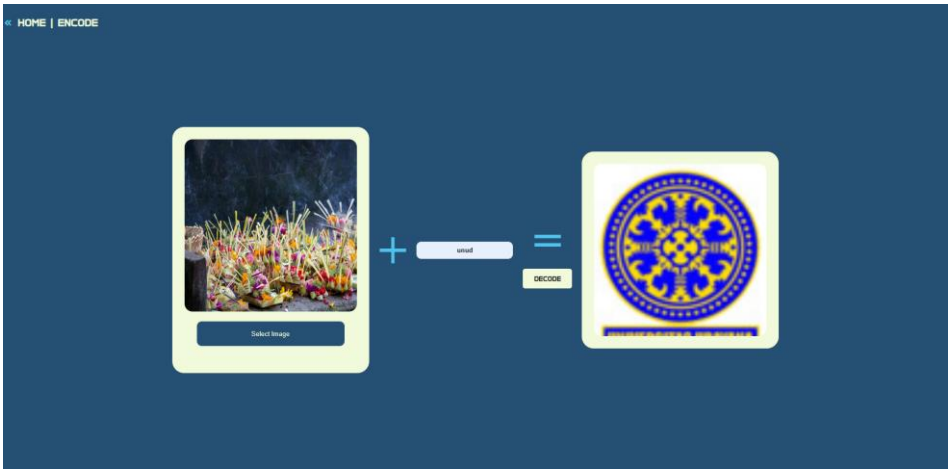
Bisa dilihat pada gambar 6 diatas. Untuk proses dekripsi dan decode file dapat dilakukan dengan klik menu decode terlebih dahulu dan website akan membawa user ke halaman decode.Dimana pada halaman ini user bisa menginputkan stego image dan decrypt key. Untuk tampilannya dapat dilihat pada gambar diatas.



Gambar 7. Tampilan Halaman Decode dengan Input Image

Bisa dilihat pada gambar 7 diatas. Untuk percobaan digunakan file stego image yang merupakan hasil penyisipan yang dilakukan pada proses sebelumnya dan dibutuhkan juga kata kunci yang sebelumnya digunakan.

p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 8. Tampilan Halaman Decode dengan Hasil Ekstraksi Image

Bisa dilihat pada gambar 8 diatas. Kemudian user dapat meng-klik tombol decode dan akan dilakukan proses decode dan dekripsi. Jika proses decode dan dekripsi berhasil dilakukan maka digital signature akan muncul.

3.2 Pengujian

Pengujian merupakan salah satu aspek penting dalam pengembangan perangkat lunak. Tujuan dari dilakukannya proses pengujian adalah untuk menjamin bahwa perangkat lunak yang dibangun memiliki kualitas yang handal, dimana dengan adanya pengujian dapat menjamin kualitas serta mengetahui kekurangan dari perangkat lunak yang dibangun.

Hasil gambar stegano yang diciptakan akan berformat *.png sehingga gambar yang dihasilkan tentu memiliki ukuran file yang lebih besar namun tidak mengubah ukuran pixel panjang dan lebar dari gambar asli.

Karena digunakan metode BPCS maka bagian pixel pada gambar yang berubah tentu akan akan lebih banyak dibandingkan tidak menggunakan metode BPCS, sehingga akan mempengaruhi kualitas dari gambar itu sendiri, maka dilakukan percobaan pada 10 gambar berbeda untuk pesan rahasia yang sama dan kata kunci yang sama, contoh pesan yang digunakan adalah logo unud dan kata kunci “unud”.

Untuk hasil uji kualitas atau PSNRnya dapat dilihat pada tabel 1 berikut :

Tabel 1. Hasil Pengujian PSNR

No	Citra Asli	Citra Stegano	PSNR (dB)
1			71.40

2			66.35
3			73.59
4			74.80
5			74.05
6			69.48

p-ISSN: 2301-5373
e-ISSN: 2654-5101

7			69.94
8			66.45
9			69.96
10			72.92

Rata-rata dari kesepuluh kali percobaan PSNR :

Rata-rata = (Total seluruh PSNR) / Jumlah percobaan PSNR

= (71.40 + 66.35 + 73.59 + 74.80 + 74.05 + 69.48 + 69.94 + 66.45 + 69.96 + 72.92)

= 708.96 / 10

= 70.89

Dari hasil 10 kali uji coba diatas didapatkan nilai rata-rata PSNR masih berada diatas 40dB [7] yang berarti hasil uji untuk pesan dan kata kunci tersebut dengan gambar-gambar diatas dapat dikatakan kualitas stegano image yang dihasilkan termasuk tinggi.

4. Kesimpulan

4.1 Kesimpulan

a. Metode steganografi BPCS (Bit-Plane Complexity Segmentation) yang dibangun pada aplikasi ini berhasil menyisipkan file gambar digital signature pada gambar cover image dengan format *.jpg dan dapat menyimpan stegoimage serta berhasil mengekstraksi stegoimage dan melihat file gambar digital signature terenkripsi yang tersimpan.
b. Dari 10 kali pengujian kemiripan gambar dengan metode PSNR didapatkan bahwa rata-rata PSNR yang dihasilkan adalah 70.89 dB. Penggunaan metode DES dan BPCS termasuk baik karena rata-rata nilai PSNR yang dihasilkan masih diatas standar kategori baik yaitu diatas 40dB.[1]

4.2 Saran

Saran yang dapat diberikan penulis untuk penelitian berikutnya adalah sistem ini dapat dikembangkan dengan menggunakan media penampung selain citra atau gambar seperti media suara atau video juga dapat digunakan dalam mengimplementasikan metode steganografi.

Daftar Pustaka

[1] Aprilia, I., Ariyanti, D. and Izzuddin, A. (2019) ‘Analisa Pengukuran Kualitas Citra Hasil Steganografi’, pp. 116–121.

[2] Fatma, Y., Mukhtar, H. and Taufik, M. (2018) ‘Implementasi Steganografi Pada Teks Terenkripsi Dengan Algoritma Rsa Menggunakan Metode Bpcs’, *Jurnal Fasilkom*, 7(2), pp. 260–265. Available at: https://doi.org/10.37859/jf.v7i2.783.

[3] Gonzalez, R.C. and Woods, R.E. (2018) *4TH EDITION Digital image processing*.

[4] Jurnal, J. *et al.* (2023) ‘Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB)’, 3(1), pp. 40–46.

[5] Raharja, B.D. and Harsadi, P. (2018) ‘Implementasi Kompresi Citra Digital Dengan Mengatur Kualitas Citra Digital’, *Jurnal Ilmiah SINUS*, 16(2), pp. 71–77. Available at: https://doi.org/10.30646/sinus.v16i2.363.

[6] Rizqa, I., Safitri, A.N. and Harkespan, I. (2022) ‘Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar’, *Jurnal Masyarakat Informatika*, 13(2), pp. 111–120. Available at: https://doi.org/10.14710/jmasif.13.2.44547.

[7] Sajati, H. (2018) ‘The Effect of Peak Signal to Noise Ratio (PSNR) Values on Object Detection Accuracy in Viola Jones Method’, *Conference SENATIK STT Adisutjipto Yogyakarta*, 4. Available at: https://doi.org/10.28989/senatik.v4i0.139.

[8] Z, H. (2018) ‘Implementasi Metode Bit Plane Complexity Segmentation pada Citra Digital dalam Penyembunyian Pesan Rahasia’, *MEANS (Media Informasi Analisa dan Sistem)*, 3(2), pp. 159–165. Available at: https://doi.org/10.54367/means.v3i2.286.