JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

IMPLEMENTASI ALGORITMA *PIXEL VALUE DIFFERENCING* (PVD) DALAM KEAMANAN DATA TEKS

Ratna Sabrina Nasution[1)], Muhammad Fakhriza[2)], Muhammad Dedi Irawan[3)].
[1,2,3]Sistem Informasi, Universitas Islam Negeri Sumatera Utara
nasutionratna11@gmail.com,

ABSTRAK

Steganografi telah menjadi solusi penting untuk mengamankan informasi sensitif dalam berkas yang tampak tidak mencurigakan seperti gambar atau dokumen. Makalah ini mengeksplorasi algoritma *Pixel Value Differencing* (PVD) untuk menyembunyikan data rahasia dalam teks PDF, memastikan kerahasiaan tanpa menimbulkan kecurigaan. Penelitian ini menganjurkan penggunaan langkah-langkah keamanan yang kuat untuk mencegah akses yang tidak sah, menyoroti tanggung jawab organisasi dalam melindungi informasi sensitif. Dengan memanfaatkan sistem berbasis web yang menggunakan *kriptografi Exclusive OR* (XOR) dan steganografi PVD, penelitian ini bertujuan untuk meningkatkan perlindungan data terhadap potensi pelanggaran dan kebocoran. Meskipun menghadapi tantangan seperti noise pada gambar stego akibat karakteristik PDF yang disisipkan (teks, tabel, gambar), pendekatan ini secara signifikan mengurangi risiko keamanan, sehingga memperkuat langkah-langkah kerahasiaan untuk data perusahaan.

Kata Kunci: Keamanan, *Kriptografi*, *Exclusive OR* (XOR), *Steganografi*, *Pixel Value Differencing* (PVD)

ABSTRACT

Steganography has emerged as a critical solution for securing sensitive information within seemingly innocuous files such as images or documents. This paper explores the Pixel Value Differencing (PVD) algorithm for concealing confidential data within PDF text, ensuring secrecy without raising suspicion. The study advocates for robust security measures to prevent unauthorized access, highlighting the responsibility of organizations in safeguarding sensitive information. Employing a web-based system utilizing Exclusive OR (XOR) cryptography and PVD steganography, the research aims to enhance data protection against potential breaches and leaks. Despite challenges like noise in stego images due to embedded PDF characteristics (text, tables, images), this approach significantly mitigates security risks, thereby bolstering confidentiality measures for corporate data.
Keywords: *Security, Cryptography, Exclusive OR (XOR), Steganography, Pixel Value Differencing (PVD)*

PENDAHULUAN

Keamanan dan kerahasiaan adalah aspek penting dari data, pesan, dan informasi. Pengiriman pesan, data, dan informasi yang sangat penting memerlukan tingkat keamanan yang tinggi [1]. Banyak orang menganggap informasi tertentu sangat berharga, sehingga mereka tidak ingin orang lain mengetahuinya. Namun, sering kali informasi tersebut disalahgunakan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan atau sekadar merusaknya [2].

Upaya dalam pengamanan data, informasi, dan pesan dalam sebuah perusahaan sangat penting, terutama bagi perusahaan yang memiliki *revenue* yang kuat dan merupakan bagian dari bisnis pemerintah [3].

Dalam konteks ini, *steganografi* dapat digunakan untuk mengamankan informasi rahasia dalam file yang tampaknya tidak mencurigakan, seperti gambar atau

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

dokumen lainnya [4]. Dengan menggunakan kunci atau metode ekstraksi yang tepat, hanya orang yang memiliki akses yang sah yang dapat mengakses informasi yang diamankan secara tersembunyi [5].

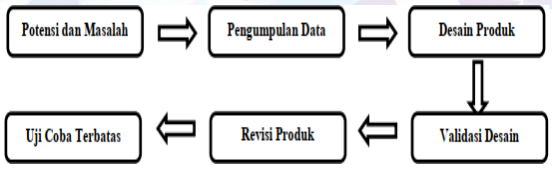
Dengan mengimplementasikan langkah-langkah keamanan yang tepat, seperti enkripsi data, pengendalian akses yang ketat, dan penggunaan teknik kriptografi dan steganografi dapat menjaga kerahasiaan data. Hal ini akan membantu menjaga integritas operasional secara keseluruhan dan meminimalisir kebocoran data. Salah satu cara mengamankan data teks rahasia dengan menggunakan metode *kriptografi Exclusive OR* (XOR) dan algoritma *Pixel Value Differencing* (PVD).

Berdasarkan penelitian yang dilakukan oleh Ricky Andri, dkk (2019). Dalam penelitan tersebut peneliti menggunakan metode PVD untuk mengasilkan sistem yang bisa menyembunyikan pesan ke dalam foto/gambar sehingga tidak mengundang kecurigaan dari pihak yang tidak bertanggung jawab.

Dari penelitian terdahulu tersebut, pada penelitian ini akan memfokuskan dalam pengamanan data teks dalam format pdf yang berisikan informasi rahasia dengan menggunakan metode *kriptografi Exclusive OR* (XOR) dan algoritma PVD untuk perlindungan keamanan tambahan dan menjaga stabilitas perusahaan.

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah *Research and Development* (R&D), yang bertujuan untuk menghasilkan produk. R&D merupakan suatu proses atau langkah-langkah yang dilakukan untuk mengembangkan produk baru atau memperbaiki produk yang sudah ada, dengan tetap mempertanggungjawabkan hasilnya [6].



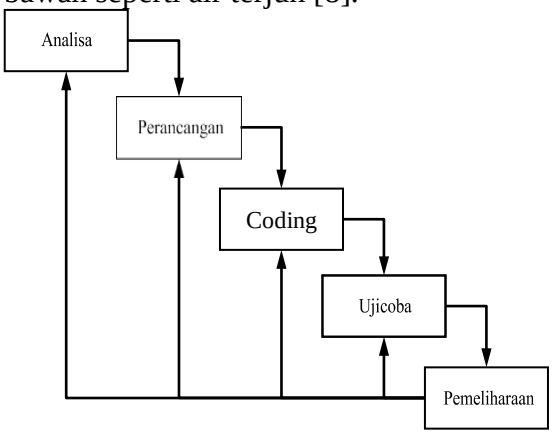
Gambar 1. Tahapan Metode R&D [7]

1. Potensi dan Masalah
   Tahap awal dari penelitian ini melibatkan analisis potensi dan masalah, yang terdiri dari dua bagian utama: analisis sistem yang sedang berjalan dan analisis sistem yang diusulkan.
2. Pengumpulan Data
   Pengumpulan data untuk perencanaan keamanan data diharapkan membantu dalam menjaga keamanan data perusahaan. Metode pengumpulan data yang dipilih adalah observasi, wawancara, dan studi pustaka, yang diharapkan dapat memberikan informasi dan data yang dibutuhkan dalam proses pembangunan aplikasi.
3. Desain Produk
   Pada penelitian ini desain produk yang akan dihasilkan dapat dimanfaatkan untuk kehidupan manusia adalah produk yang berkualitas dan menarik.
4. Validasi Sistem
   Validasi desain pada tahap ini adalah proses untuk mengevaluasi apakah rancangan produk baru lebih efektif dibandingkan dengan yang lama, penilaian berdasarkan pemikiran rasional.
5. Revisi Produk
   Melakukan revisi atau perbaikan produk setelah produk didesain untuk mengetahui kelemahannya dan memperbaiki desain.
6. Uji Coba Terbatas
   Selanjutnya produk yang telah jadi akan diuji coba terlebih dahulu untuk memastikan produk yang dibuat berfungsi dengan baik dan memenuhi kebutuhan yang ditetapkan.

Metode Pengembangan Sistem

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

Pada Penelitian ini metode *waterfall* digunakan sebagai metode pengembangan sistem, metode ini memiliki aliran sistem yang sederhana dan berurutan, mengalir ke bawah seperti air terjun [8].



Gambar 2. Tahapan Metode *Waterfall* [9]

1. Analisis
   Tahapan ini dilakukan untuk mengenal elemen-elemen situasi dalam permasalahan dan memahami komponen mana saja yang kritis agar dapat mengambil keputusan yang terbaik.
2. Perancangan
   a. Desain Proses
      Merancang berbagai proses yang terlibat dalam sistem informasi keamanan data teks dengan menggunakan UML, yang mencakup *use case*, *activity diagram*, *sequence diagram*, *dan class diagram*, serta merancang semua proses pembuatan sistem.
   b. Desain *Databse*
      Desain struktur *database* yang digunakan untuk menyimpan data-data yang dibutuhkan oleh sistem.
   c. Desain *Interface*
      Merancang antarmuka pengguna yang ramah pengguna agar memudahkan pemahaman fitur-fitur yang tersedia dalam sistem.
3. *Coding*
   Pada penulisan *Coding* yaitu menerjemahkan hasil dari proses perancangan yang sudah dilakukan sebelumnya ke dalam bentuk *coding*. Penelitian ini menggunakan bahasa pemrograman PHP dan *Visual Studio Code* sebagai teks editornya.
4. Pengujian
   Selanjutnya tahap pengujian yaitu melakukan pengujian terhadap modul yang sudah dibagun. Proses pengujian akan menggunakan *BlackBox testing* di dalam setiap pengujian dilakukan pada masing-masing menu, respon *interface* dan proses analisa yang berjalan pada sistem yang sudah dibangun.
5. Pemeliharaan
   Tahap ini sistem sudah dapat dipergunakan dengan baik dan akan dilakukan pemantauan untuk perawatan terhadap kemungkinan terjadinya kesalahan sistem pada saat pengoperasian.

HASIL DAN PEMBAHASAN

Penerapan Operasi *Exclusive OR* (XOR) dan Algoritma *Pixel Value Differencing* (PVD)

Proses penggunaan operasi *Exclusive OR* (XOR) dan *Pixel Value Differencing* (PVD) dalam melakukan proses pengamanan dan penyisipan data ke dalam citra dapat dilihat sebagai berikut:

1. Proses Enkripsi

Plaintext : MASTERDATA

Kunci : 2024

Proses pengamanan ini dilakukan dengan menghitung XOR antara plaintext dan kunci. Kunci akan diulang sesuai dengan panjang karakter plaintext, sehingga menghasilkan proses enkripsi sebagai berikut:

P1 = **M** = 0 1 0 0 1 1 0 1
K1 = **2** = 0 0 1 1 0 0 1 0 ⊕

C1 = 0 1 1 1 1 1 1 1

P2 = **A** = 0 1 0 0 0 0 0 1

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

K2 = **0** = 0 0 1 1 0 0 0 0 ⊕
C2 = 0 1 1 1 0 0 0 1

P3 = **S** = 0 1 0 1 0 0 1 1
K3 = **2** = 0 0 1 1 0 0 1 0 ⊕
C3 = 0 1 1 0 0 0 0 1

P4 = **T** = 0 1 0 1 0 1 0 0
K4 = **4** = 0 0 1 1 0 1 0 0 ⊕
C4 = 0 1 1 0 0 0 0 0

P5 = **E** = 0 1 0 0 0 1 0 1
K5 = **2** = 0 0 1 1 0 0 1 0 ⊕
C5 = 0 1 1 1 0 1 1 1

P6 = **R** = 0 1 0 1 0 0 1 0
K6 = **0** = 0 0 1 1 0 0 0 0 ⊕
C6 = 0 1 1 0 0 0 1 0

P7 = **D** = 0 1 0 0 0 1 0 0
K7 = **2** = 0 0 1 1 0 0 1 0 ⊕
C7 = 0 1 1 1 0 1 1 0

P8 = **A** = 0 1 0 0 0 0 0 1
K8 = **2** = 0 0 1 1 0 1 0 0 ⊕
C8 = 0 1 1 1 0 1 0 1

P9 = **T** = 0 1 0 1 0 1 0 0
K9 = **2** = 0 0 1 1 0 0 1 0 ⊕
C9 = 0 1 1 0 0 1 1 0

P10 = **A** = 0 1 0 0 0 0 0 1
K10 = **0** = 0 0 1 1 0 0 0 0 ⊕
C10 = 0 1 1 1 0 0 0 1

Hasil dari proses pengamanan data menggunakan operasi XOR adalah "**01111111 01110001 01100001 01100000 01110111 01100010 01110110 01110101 01100110 01110001**".

2. Proses penyisipan data yang telah diamankan menggunakan operasi XOR ke dalam citra menggunakan algoritma Pixel Value Differencing (PVD)
   a. Mengambil nilai pixel dari suatu citra sebagai berikut:

55 112 167
76 13 175
163 79 202

   b. Setelah memperoleh nilai piksel dari gambar, langkah selanjutnya adalah menyisipkan pesan. Berikut adalah langkah-langkahnya:
      1) Mengambil *pixel* yang berdekatan dari citra, yaitu pixel (0,0) dan pixel (0,1). Nilai pixel tersebut diambil untuk proses penyisipan, berikut adalah tabel nilai pixel yang berdekatan yaitu 55 dan 112.

55	112	167
76	113	175
163	179	202

      2) Menghitung nilai selisih *(differencing value)* dari kedua pixel tersebut. yaitu = |55 - 112|, sehingga didapat d = 57
      3) Mencari posisi rentang kontinu *(continues range)* dari nilai selisih *(difference value)* pada skema Wu dan Tsai.
         R= {[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]}.
         Letak rentang kontinu (continues range) yang didapat dari d = 57 yaitu [32, 63] dimana ik = 32, dan uk = 63.
      4) Menghitung jumlah bit dari pesan yang dapat dimasukkan ke dalam kedua piksel yang dibandingkan yaitu t =

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

LOG2(63 - 32) sehingga didapat = 5, maka ambil bit dari pesan sebanyak t yaitu **01111**.

5) Mengonversi nilai bit sebanyak t ke dalam bentuk desimal, misalnya 01111 yang jika dikonversi menjadi desimal adalah 15 (b = 15). Selanjutnya, menghitung nilai differencing value yang baru dengan rumus d' = 32 + 15, sehingga diperoleh nilai d' = 47..
6) Melakukan penyisipan dengan memodifikasi nilai dari piksel yang dibandingkan sesuai dengan aturan yang telah ditentukan. Aturan yang terpenuhi yaitu d' < d dan *P*'i < P'i + 1 maka Pi = 55 + |15/2| dan Pi+1= 112 - |15/2|.
7) Menyimpan nilai pixel yang baru, yaitu *P*i = 62,5 dan *P*i + 1 = 104,5 ke dalam citra. Proses ini dilanjutkan hingga seluruh pesan berhasil disisipkan, berikut adalah hasilnya:

62,5 104,5 167
76 13 175
163 79 202

3. Proses pengambilan/ekstraksi *watermark* dilakukan dengan menggunakan algoritma *Pixel Value Differencing* (PVD)
   a. Mengambil pixel yang berdekatan dari citra. Contoh pixel yang berdekatan adalah pixel (0,0) dan pixel (0,1) seperti yang terlihat pada gambar diatas. Nilai dari pixel yang bertetangga/berdekatan tersebut diambil untuk proses penyisipan. Jika Pi dan Pi +1 merupakan pixel yang bertetangga, maka Pi = 62,5 dan Pi+1 = 104,5.
   b. Menghitung nilai selisih (differencing value) dari kedua pixel tersebut menggunakan persamaan d = |62,5 – 104,5|, sehingga didapat d = 42.
   c. Mencari posisi rentang kontinus (continues range) dari nilai selisih (difference value) pada skema wu dan tsai.
      R= {[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]}.
      Letak continues range yang di dapat dari d = 41 yaitu [32,63] dimana lk = 32, dan uk = 63.
   d. Menghitung jumlah bit informasi yang disisipkan ke dalam kedua pixel. Jumlah bit ini dihitung dengan persamaan, yaitu t = $Log2$(63 - 32) sehingga didapat t = 5, atau terdapat 5 bit pesan yang disisipkan pada kedua pixel.
   e. Mengonversi nilai desimal pesan ke dalam bentuk bit sebanyak t, sehingga diperoleh bit pesan b = 011111. Proses ini dilanjutkan secara berulang hingga semua pixel teridentifikasi.

4. Proses Dekripsi

Ciphertext : 01111111 01110001 01100001 01100000 01110111 01100010 01110110 01110101 01100110 01110001

Kunci : 2024

Proses dekripsi ini dilakukan dengan menghitung XOR antara *ciphertext* dan kunci. Nilai kunci akan diulang sesuai dengan panjang karakter *ciphertext*, sehingga menghasilkan proses dekripsi sebagai berikut:

C1		= 0 1 1 1 1 1 1 1	
K1	= **2**	= 0 0 1 1 0 0 1 0	⊕
P1	=**M**	= 0 1 0 0 1 1 0 1	
C2		= 0 1 1 1 0 0 0 1	
K2	= **0**	= 0 0 1 1 0 0 0 0	⊕
P2	=**A**	= 0 1 0 0 0 0 0 1	

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

C3 = 0 1 1 0 0 0 0 1
K3 = **2** = 0 0 1 1 0 0 1 0 ⊕
P3 = **S** = 0 1 0 1 0 0 1 1

C4 = 0 1 1 0 0 0 0 0
K4 = **4** = 0 0 1 1 0 1 0 0 ⊕
P4 = **T** = 0 1 0 1 0 1 0 0

C5 = 0 1 1 1 0 1 1 1
K5 = **2** = 0 0 1 1 0 0 1 0 ⊕
P5 = **E** = 0 1 0 0 0 1 0 1

C6 = 0 1 1 0 0 0 1 0
K6 = **0** = 0 0 1 1 0 0 0 0 ⊕
P6 = **R** = 0 1 0 1 0 0 1 0

C7 = 0 1 1 1 0 1 1 0
K7 = **2** = 0 0 1 1 0 0 1 0 ⊕
P7 = **D** = 0 1 0 0 0 1 0 0

C8 = 0 1 1 1 0 1 0 1
K8 = **2** = 0 0 1 1 0 1 0 0 ⊕
P8 = **A** = 0 1 0 0 0 0 0 1

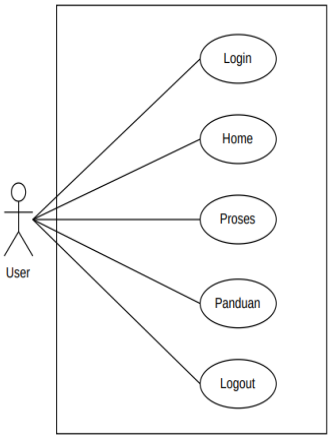
C9 = 0 1 1 0 0 1 1 0
K9 = **2** = 0 0 1 1 0 0 1 0 ⊕
P9 = **T** = 0 1 0 1 0 1 0 0

C10 = 0 1 1 1 0 0 0 1
K10 = **0** = 0 0 1 1 0 0 0 0 ⊕
P10 = **A** = 0 1 0 0 0 0 0 1

Desain Sistem

Use Case Diagram

Use case diagram adalah alat untuk menggambarkan interaksi antara aktor dan aktivitas dalam suatu sistem [10]. Diagram ini menjelaskan berbagai proses yang ada dalam sistem serta hubungan antara proses tersebut dan aktor yang terlibat.

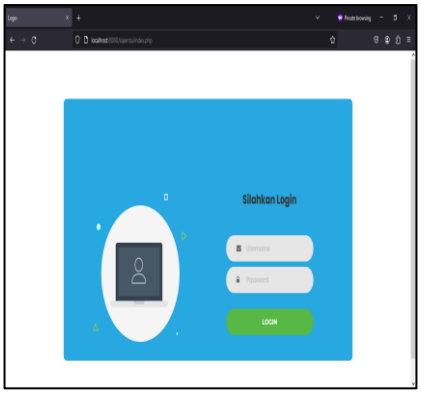


Gambar 3. *Use Case* Diagram

Implementasi

Tampilan Halaman *Login*

Halaman login yaitu halaman pertama ketika membuka website, pengguna harus terlebih dahulu login untuk masuk ke dalam website, akun untuk masuk harus didaftarkan.

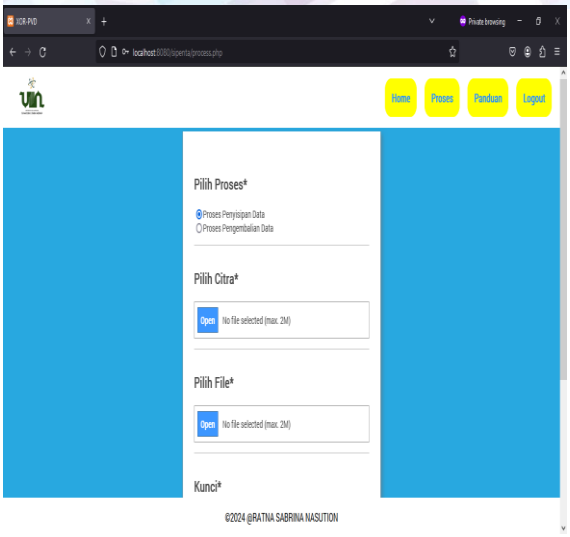


Gambar 4. Halaman *Login*

Halaman Proses Penyisipan Data

Halaman proses penyisipan data yaitu halaman yang akan digunakan untuk menyisipkan data rahasia di dalam citra foto sehingga data yang akan dikirimkan tidak diketahui oleh pihak yang tidak berwenang dan menjaga kemanan data perusahaan.

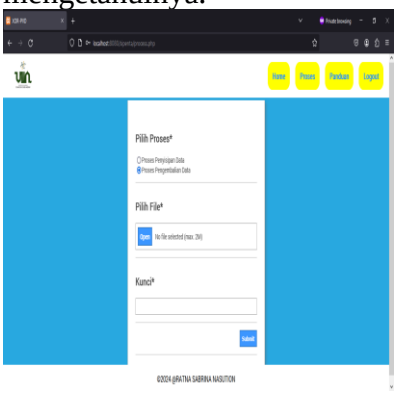
JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X



Gambar 5. Proses Penyisipan Data

Halaman Proses Pengembalian Data

Halaman proses pengembalian data yaitu halaman yang akan digunakan untuk mengembalikan data rahsia yang telah disisipi citra foto ke bentuk asli nya, dengan begitu hanya pihak tertentu yang mengetahuinya.



Gambar 6. Proses Pengembalian Data

Tampilan Halaman Panduan

Halaman panduan yaitu halaman yang berisi tata cara atau langkah-langkah dalam menggunakan website ini.

Gambar 7. Halaman Panduan

Pengujian *Black Box*

Pengujian *black box* dilakukan untuk memastikan bahwa semua menu dalam sistem berfungsi sesuai dengan desain yang telah ditetapkan [11]. Hasil pengujian *black box* dari Sistem Informasi Keamanan Data Teks Dengan Algoritma *Pixel Value Differencing* (PVD), dapat dilihat sebagai berikut:

No.	Komponen Yang Diuji	Skenario Pengujian	Hasil Yang Diharapkan	Validasi
1	*Login*	*Input username, password* dan klik login	Menampilkan halaman home setelah melakukan proses *login* menggunakan username dan *password* yang benar	√
2	Proses pengamanan dan penyisipan	Memilih file citra, file dan menginputkan kunci	Sistem dapat melakukan proses pengamanan data dan menyisipkan file yang dipilih ke dalam file citra yang telah dipilih	√
3	Proses pengembalian	Memilih file citra stego dan menginputkan kunci	Sistem dapat melakukan proses pengembalian data yang telah disisipkan ke dalam citra setelah pengguna memilih file citra stego dan	√

JURSIMA
Jurnal Sistem Informasi & Manajemen
ISSN : 2338-1523, E-ISSN: 2541- 576X

			menginputkan kunci yang sama dengan proses pengamanan dan penyisipan	
4	Halaman panduan	Memilih menu panduan	Sistem dapat menampilkan halaman panduan penggunaan aplikasi setelah pengguna memilih menu panduan	√
5	Proses *logout*	Memilih menu logout	Sistem dapat melakukan proses logout setelah pengguna memilih menu logout dan selanjutnya menampilkan halaman login dari sistem	√

Hasil Pengujian *Blackbox Testing*

Tipe *User*	*Test Case*	*Total Test Case*	Rumus Perhitungan	Hasil Perhitungan
Petugas	5	5x1	*Test Case Pass* $= \left(\frac{Test\ Case\ Pass}{Total\ Test\ Case}\right) \times 100\%$	*Test Case Pass* $= \left(\frac{5}{5}\right) \times 100\% = 100\%$

SIMPULAN

Berdasarkan pembahasan dan hasil yang telah dihasilkan sebuah sistem berbasis *website* yang memanfaatkan kriptografi *Exlusive OR* (XOR) dan steganografi *Pixel Value Differencing* (PVD) digunakan untuk mengamankan data teks berformat .pdf dengan menyandikan data tersebut dan menyisipkannya ke dalam citra berformat jpg sehingga data dapat lebih terjaga keamanannya dan mengurangi kemungkinan data tersebut dilihat/ bocor pada pihak yang tidak sah. Namun, akan terdapat noise pada citra stego yang dihasilkan karena data yang disisipkan adalah berkas pdf yang memiliki karakter, tabel ataupun gambar.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan Terima Kasih kepada pihak yang telah mendukung penelitian ini. Terimakasih kepada dosen pembimbing yang telah terlibat dalam penelitian ini dan memberikan bimbingan dalam penelitian ini sehingga penelitian dapat diselesaikan.

DAFTAR PUSTAKA

[1] B. Setiawan, B. Selviana, and A. S. Y. Irawan, "Mengoptimalkan Fungsi Payment Gateway Midtrans pada Website Coffee Shop Melalui Penggunaan Metode Prototype pada Proses Pengembangan," *JRST (Jurnal Ris. Sains dan Teknol.*, vol. 7, no. 2, p. 219, 2023, doi: 10.30595/jrst.v7i2.16964.

[2] R. A. Megantara and F. A. Rafrastara, "Super Enkripsi Teks Kriptografi Menggunakan Algoritma Hill Cipher Dan Transposisi Kolom," *Pros. SENDI_U*, pp. 85–92, 2019, [Online]. Available: https://www.unisbank.ac.id/ojs/index.php/sendi_u/article/view/7299

[3] H. Santoso and M. Fakhriza, "PERANCANGAN APLIKASI KEAMANAN FILE AUDIO FORMAT WAV (WAVEFORM) MENGGUNAKAN ALGORITMA

RSA," *Algoritm. J. Ilmu Komput. dan Inform.*, vol. 02, no. 01, pp. 47–54, 2018, doi: 10.0000/2422369ca3ff4b10a3a4b6dd84c6d819.

[4] S. Siaulhak and Safwan Kasma, "Sistem Pengiriman File Menggunakan Steganografi Pengolahan Citra Digital Berbasis Matriks Laboratory," *BANDWIDTH J. Informatics Comput. Eng.*, vol. 1, no. 2, pp. 75–81, 2023, doi: 10.53769/bandwidth.v1i2.522.

[5] M. Syahril and H. Jaya, "Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4," *Sensasi*, pp. 505–509, 2019, [Online]. Available: http://prosiding.seminar-id.com/index.php/sensasi/issue/archivePage%7C505

[6] B. Muqdamien, U. Umayah, J. Juhri, and D. P. Raraswaty, "Tahap Definisi Dalam Four-D Model Pada Penelitian Research & Development (R&D) Alat Peraga Edukasi Ular Tangga Untuk Meningkatkan Pengetahuan Sains Dan Matematika Anak Usia 5-6 Tahun," *Intersections*, vol. 6, no. 1, pp. 23–33, 2021, doi: 10.47200/intersections.v6i1.589.

[7] A. Fakhri, T. Hidayat, and Djamaludin, "Sistem Informasi Manajemen Pembudidayaan Ikan Lele Menggunakan Metode Research and Development," *JSiI (Jurnal Sist. Informasi)*, vol. 8, no. 1, pp. 53–58, 2021, doi: 10.30656/jsii.v8i1.3016.

[8] A. Abdul Wahid, "Analisis Metode Waterfall Untuk Pengembangan Sistem Informasi," *J. Ilmu-ilmu Inform. dan Manaj. STMIK*, no. November, pp. 1–5, 2020.

[9] S. M. Rambe and S. Suendri, "Geographic Information System Mapping Risk Factors Stunting Using Methods Geographically Weighted Regression," *J. Appl. Geospatial Inf.*, vol. 7, no. 2, pp. 1075–1079, 2023, doi: 10.30871/jagi.v7i2.6936.

[10] M. Alda, "Pemanfaatan Barcode Scanner Pada Aplikasi Manajemen Inventory Barang Berbasis Android," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 10, no. 3, pp. 368–375, 2021, doi: 10.32736/sisfokom.v10i3.1175.

[11] W. Yahya Dwi and A. Muna Wardah, "Pengujian Blackbox Sistem Informasi Penilaian Kinerja Karyawan Pt Inka (Persero) Berbasis Equivalence Partitions Blackbox Testing of Pt Inka (Persero) Employee Performance Assessment Information System Based on Equivalence Partitions," *J. Digit. Teknol. Inf.*, vol. 4, no. 1, pp. 22–26, 2021.