Jurnal Elektronik Ilmu Komputer Udayana
Volume 10, No 4. May 2022

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

Penerapan Steganography Untuk Perlindungan Hak Cipta Menggunakan Metode Least Significant Bit (LSB)

I Gusti Ngurah Bagus Pramana Putra[a1], I Ketut Gede Suhartana[a2], I Komang Ari Mogi[a3], Cokorda Rai Adi Pramartha [a4], I Putu Gede Hendra Suputra[a5], I Gede Arta Wibawa[a6],

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Bali, Indonesia
[1]ngurahpramana170@gmail.com
[2]ikg.suhartana@unud.ac.id
[3]arimogi@unud.ac.id
[4]cokorda@unud.ac.id
[5]hendra.suputra@unud.ac.id
[6]gede.arta@unud.ac.id

Abstract

Lontar as one of the manuscripts (ancient manuscripts) which is the cultural heritage of the ancestors which is unique in recording and transferring traditional knowledge which is done through writing in the Lontar media. However, the slow pace of ejection made the manuscript very vulnerable for various reasons. The damage resulted in an increase in the information contained in Lontar, then the media was converted to digital. If these various types of letters are digitized, what will be the proof of authenticity that these lontar scripts are His? In addition, this digitization can also be used to develop access for triplets and the general public to their knowledge. From these problems, this research was conducted to build a desktop-based application that implements steganography by hiding secret messages into the PNG extension by utilizing the Least Significant Bit (LSB) method as a means of copyright protection in the Balinese Lontar Manuscript. This research succeeded in doing the insertion only with the last 3-2-3 bit formation in the RGB channel, so between the cover image and the stegoimage there will be no significant difference to the human sense of sight even though the inserted message is 100% of the maximum capacity of the image. The test results prove that there is an increase in security and the imperceptibility value is maintained. This is evidenced by the results of the average MSE value of 0.01856775 dB and PSNR 97.22405 dB. Then the user who first encrypts the file has definitive proof of copyright ownership and data security.

Keywords: *Steganography, Least Significant Bit (LSB), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)*

1. Pendahuluan

Lontar sebagai salah satu contoh manuskrip (naskah kuno) yang merupakan warisan kebudayaan dari leluhur yang memiliki Keunikan cara perekaman dan transfer pengetahuan tradisional dengan menulis di media daun lontar. Meski agak berbeda dengan perlakuan terhadap naskah-naskah Lontar kuno yang semakin ditinggalkan oleh peradaban modern di belahan dunia lain, naskah-naskah yang ditulis di atas daun lontar merupakan bagian aktif dari budaya literasi masyarakat Bali modern. Seiring dengan praktik budaya dan dukungan sumber daya alam, bagi orang Bali sendiri, Lontar adalah kitab suci yang dipelajari tidak hanya untuk disucikan, tetapi juga untuk digunakan sebagai pedoman dalam kehidupan sehari-hari (suluh nikang prabha). Namun lambat laun usia lontar tersebut membuat material naskah lontar sangat rentan terhadap kerusakan dari berbagai penyebab seperti jamur, kelembaban, invansi serangga, dan kontak tangan manusia sehingga lontar-lontar tua sangat rentan terhadap pelapukan. Adanya pelapukan tersebut berdampak pada hilangnya informasi yang terdapat pada lontar. Dengan adanya faktor tersebut, perlu dilakukan pelestarian seperti melakukan alih media ke digital. Selain itu, digitalisasi ini dapat digunakan untuk memberikan akses pengetahuan kepada pengunjung dan masyarakat umum.

Sementara itu, kebutuhan akan keamanan dan kerahasian data atau informasi semakin meningkat, terlebih lagi banyak jenis naskah lontar yang akan digitalisasi. Jika manuskrip lontar dari berbagai jenis didigitalkan, apa bukti definitif bahwa manuskrip lontar ini ada di tangan mereka? Oleh karena itu, media diperlukan untuk melindungi kepemilikan hak cipta atas manuskrip digital dengan cara menyisipkan identitas kepemilikan ke dalam manuskrip lontar bali yang telah di digitalisasi. Steganografi adalah seni dan ilmu menyembunyikan pesan dalam suatu media sehingga tidak ada orang lain selain pengirim dan penerima yang mengetahui atau mengetahui bahwa pesan rahasia itu benar-benar ada. Dalam steganografi, ia berkembang dengan menyembunyikan informasi pada file media digital, yang dapat berupa media gambar, audio, atau video, khususnya pada naskah lontar yang akan digunakan yaitu dengan format PDF[1]. Terdapat penelitian dengan mengimplementasikan metode Least Significant Bit (LSB). Seperti penelitian [2], pada penelitian ini mengimplementasikan metode (LSB) dan metode (EOF) untuk menyisipkan pesan teks kedalam file video. Penelitian proses *embedding* teks LSB memerlukan waktu lebih sedikit dibandingkan EOF dan sebaliknya proses ekstraksi EOF memerlukan waktu lebih sedikit dibandingkan LSB. Kemudian terdapat penelitian [3], pada penelitian ini menghasilkan kombinasi Teknik steganografi dan kriptografi dengan metode LSB-RSA. Dalam eksperimen membuktikan adanya peningkatan keamanan serta nilai imperceptibility yang tetap terjaga. Hal ini membuktikan dengan hasil PSNR 57.2258dB, MSE 0.1232dB, metode ini juga tahan terhadap serangan salt and papper.

Berdasarkan penjelasan tersebut, penulis ingin melakukan penelitian yang akan digunakan untuk membuat aplikasi desktop yang menerapkan metode least significant bit (LSB) untuk menyimpan pesan pada gambar. Least Significant Bit (LSB) menambahkan bit-bit data yang akan disembunyikan (message)[4], metode ini melakukan penyimpanan data dengan mengganti bit-bit yang tidak signifikan (paling sedikit piksel) pada file yang berisi (image) dengan bit file untuk penyimpanan. Untuk meningkatkan keamanan, digunakan kombinasi steganografi dan kriptografi, di mana pesan rahasia dienkripsi terlebih dahulu menggunakan algoritma Advanced Encryption Standard (AES) untuk memungkinkan penerapan yang efisien, lebih efektif dalam perangkat lunak dan dokumentasi.

2. Metode Penelitian

Pada penelitian yang dilakukan penulis terdiri dari beberapa tahapan, yaitu data yang digunakan berupa file dokumen dalam bentuk PDF yang telah dikumpulkan dimasukan ke dalam sistem, setelah itu akan dilakukannya enkripsi/penyisipan file PDF ke dalam *cover-image* RGB dalam bentuk .PNG, enkripsi file pdf ini menggunakan metode AES dan menyisipkan file PDF terenkripsi ke dalam gambar dengan metode LSB. Setelah itu untuk poses dekripsi/ekstraksi dimulai dengan mengambil gambar yang sudah terenkripsi sebelumnya dan melakukan ekstraksi stego-image dengan metode LSB yang dimana user akan mendapatkan file dokumen yang disisipkan dalam gambar. Pada penelitian ini, *cover-image* yang digunakan berupa gambar RPG (24 bit), berbeda dengan penelitian yang telah disebutkan sebelumnya [2][3] yang menggunakan *cover-image* gambar *grayscale* (8 bit) dan juga dalam bentuk video. Tahapan enkripsi yang dilakukan pada penelitian ini terdapat 3 pilihan yaitu untuk menyisipkan pesan dalam bentuk teks, dokumen, atau gambar sedangkan pada penelitian sebelumnya hanya menyisipkan pesan dalam bentuk teks. Pada sistem yang dibangun oleh penulis, terdapat juga penambahan fitur yang tersedia dalam 2 jenis untuk memilih jumlah piksel gambar, hal ini memungkinan pengguna untuk memilih antara kualitas gambar yang lebih baik atau kapasitas penyimpanan yang lebih baik.

2.1. Data

Jenis data yang digunakan pada penelitian ini yaitu data primer. Data primer yang berasal dari berbagai sumber yang dikumpulkan dengan menggunakan Teknik observasi. Berupa dokumentasi manuskrip lontar. Pengambilan data gambar perlu dilakukan alih media ke digital dengan cara scanner atau dokumentasi dan disimpan dalam format file .PNG. Data file PDF dikumpulkan sendiri dengan cara membuat beberapa file PDF yang bersumber dari https://archive.org/details/Bali. Data yang diambil sebanyak 50 data, permasing-masing file PDF memiliki halaman dan ukuran yang menyesesuaikan dengan banyaknya isi file PDF tersebut. Pesan teks dengan minimal 1 dan maksimal 16 karakter sebanyak 50 data. Seluruh data akan digunakan sebagai evaluasi (testing)[5].

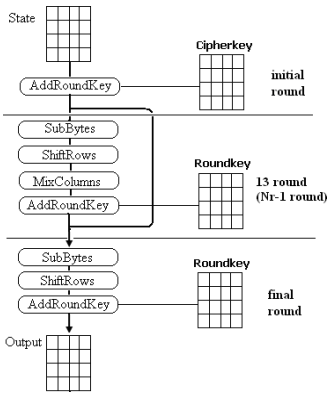
p-ISSN: 2301-5373
e-ISSN: 2654-5101

Tiap bagian lontar tersebut memiliki bahasan yang berbeda-beda seperti lontar usada yang membahas pengobatan tradisional bali contohnya seperti :

Gambar 1. Manuskrip Lontar Bali Usada.
(Sumber; https://archive.org/details/Bali)

2.2. Enkripsi AES

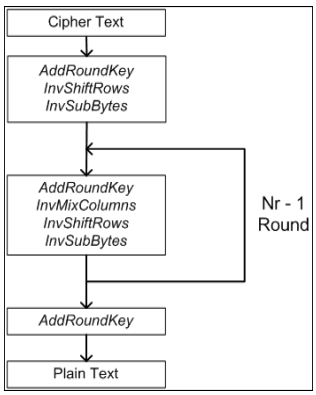
Sebelum melakukan proses penyisipan pesan kedalam gambar manuskrip lontar bali, data terlebih dahulu melalui tahapan enkripsi AES. Ketika enkripsi sangat penting dalam kriptografi, maka keamanan untuk menjaga kerahasiaan data yang dikirim[6]. Pesan aslinya adalah teks biasa yang diterjemahkan ke dalam kode yang tidak dapat dipahami. Enkripsi dapat diartikan sebagai enkripsi atau kode.



Gambar 2. Ilustrasi Proses Enkripsi

2.3. Dekripsi AES

Dekripsi adalah kebalikan dari enkripsi. Pesan terenkripsi dikembalikan ke bentuk aslinya (teks asli) yang disebut dekripsi pesan. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan algoritma yang digunakan untuk enkripsi[7].



Gambar 3. Ilustrasi Proses Dekripsi

Dengan membalikkan transformasi enkripsi dan mengimplementasikannya ke arah yang berlawanan, Anda dapat menghasilkan enkripsi balik yang mudah dipahami dari algoritme AES[8]. Konversi byte yang digunakan dalam enkripsi terbalik adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey. Gambar 4 menunjukkan proses umum dekripsi AES.

Gambar 4. Proses Enkripsi dan Dekripsi secara sederhana

Gambaran enkripsi dan dekripsi secara matematis dapat di notasikan sebagai berikut:

C = ciphertext
P = plaintext
Fungsi enkripsi E memetakan P ke C
E(P) = C
Fungsi dekripsi D memetakan C ke P
D (C) = P
D (E(P)) = P

Enkripsi bertujuan untuk memberikan layanan keamanan seperti :

1. Kerahasiaan. Tujuannya adalah untuk mencegah orang yang tidak berwenang membaca pesan tersebut.
2. Integritas data. Kami menjamin semua bagian pesan tidak akan berubah sejak pengirim membuat/mengirim data sampai penerima data membuka data.
3. Otentikasi. Berkaitan dengan identifikasi, ini mengidentifikasi kebenaran pihak yang berkomunikasi dan kebenaran pengirim pesan.
4. Non-penyangkalan. Ini memberikan cara untuk membuktikan bahwa dokumen tersebut berasal dari orang tertentu. Ini akan terbukti benar berdasarkan pengakuan orang tersebut jika seseorang mencoba mengakui kepemilikan dokumen tersebut.

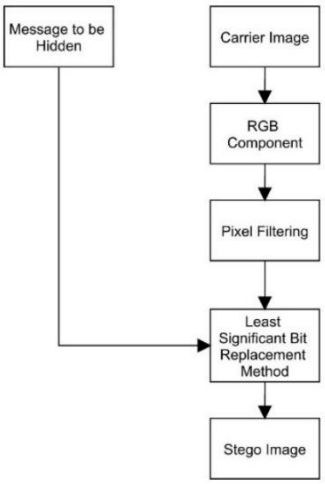
2.4. LSB

Metode ini paling sederhana, tetapi paling tidak tahan terhadap semua proses yang dapat mengubah nilai intensitas gambar. Citra adalah representasi (gambar) atau kemiripan dari suatu objek. Citra digital adalah citra yang dapat diproses oleh komputer[9]. Sebuah citra digital dapat merepresentasikan sebuah matriks yang terdiri dari M kolom dan N baris. Di sini, perpotongan kolom dan baris disebut piksel dan merupakan elemen terkecil dari gambar. Piksel memiliki dua parameter: koordinat dan intensitas atau warna.

Dalam prosedur ini, sistem mengubah nilai LSB (least significant bit) bit warna untuk menyembunyikan bit yang sesuai dengan bit label. Proses ini hanya mengubah nilai bit terakhir dari data, membuat gambar yang direkonstruksi terlihat sangat mirip dengan gambar aslinya.

Metode LSB menyembunyikan data rahasia dari piksel paling tidak signifikan di file sampul. Perubahan kecil pada nilai piksel selalu mempengaruhi file container, tetapi perubahan yang terjadi sangat kecil sehingga tidak terdeteksi oleh indera manusia[3]. Fakta ini pada akhirnya digunakan sebagai teknik untuk menyembunyikan data dan pesan.

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



Gambar 5. Alur Proses Algoritma LSB

Untuk mengilustrasikan bagaimana data disimpan menggunakan metode LSB, misalnya piksel kontainer berikut:

01001101	**00101110**	**10101110**	**10001010**	**10101111**	**10100010**	**00101011**	**10101010**

Digunakan untuk menyimpan huruf "H" (01001000), yang mengubah piksel wadah menjadi:

01001100	**0010111**1	**1010111**0	**1000101**0	**1010111**1	**1010001**0	**0010101**0	**1010101**0

2.5. MSE dan PSNR

Saat mengembangkan dan mengimplementasikan rekonstruksi citra, citra yang direkonstruksi harus dibandingkan dengan citra aslinya. Metrik umum yang digunakan untuk tujuan ini adalah rasio signal-to-noise (PSNR) puncak yang tinggi. Artinya, hasil rekonstruksi sangat mirip dengan gambar aslinya. PNSR didefinisikan sebagai:

$$PSNR = 10Log_{10}\left(\frac{C^2_{Max}}{MSE}\right) \quad (1)$$

Di sini, MSE dinyatakan sebagai kesalahan kuadrat rata-rata yang didefinisikan sebagai:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(S_{xy} - C_{xy}\right)^2 \quad (2)$$

Dimana x dan y adalah koordinat gambar, M dan N adalah dimensi gambar, Sxy adalah gambar Stego, dan Cxy adalah gambar sampul. C_Max^2 adalah nilai maksimum untuk gambar. PSNR sering dinyatakan dalam desibel (dB) pada skala logaritmik[10]. Nilai PSNR di bawah 30 dB menunjukkan kualitas yang relatif rendah dengan distorsi penyisipan yang jelas. Namun, kualitas gambar *high stay gold* adalah nilai 40 dB atau lebih.

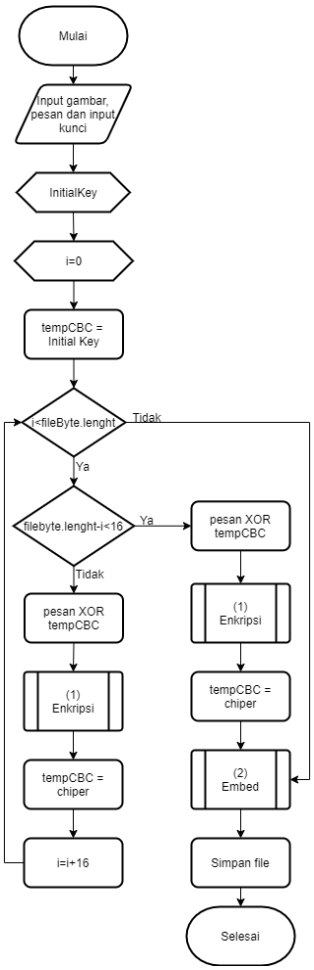
2.6. Analisis Kebutuhan

Tahap ini merupakan analisis kebutuhan sistem. Pengumpulan data pada tahap ini dilakukan untuk menemukan kondisi dan fitur yang dibutuhkan sistem untuk memenuhi kebutuhan dan keinginan penggunanya.

1. Aplikasi ini dapat dijalankan di komputer dengan sistem operasi windows.
2. Aplikasi ini dapat melakukan proses enkripsi file PDF.
3. Aplikasi ini dapat menyisipkan file PDF terenkripsi ke dalam gambar.
4. Aplikasi ini dapat mengekstrak gambar yang dimasukan ke dalam file PDF terenkripsi
5. Aplikasi ini dapat mendekripsi file PDF terenkripsi.

2.7. Desain Sistem

Perancangan aplikasi steganografi yang dibangun memiliki dua proses yaitu enkripsi embed dan dekripsi extraksi. Dalam proses enkripsi, pengguna memasukan kunci, pesan rahasia dalam bentuk dokumen, dan gambar dengan ekstensi *png. Setelah itu, hasil enkripsi akan dimasukkan menggunakan metode Least Significant Bit (LSB) ke dalam citra gambar yang sudah dimasukan oleh pengguna. Hasil penyisipan akan dikirim ke pengguna untuk di unduh.

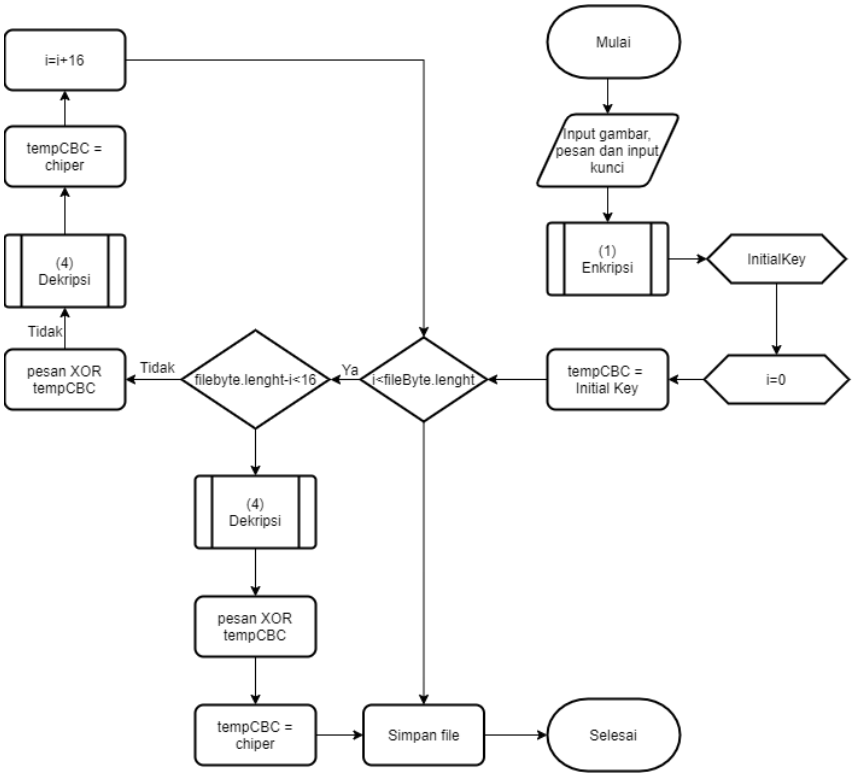


Gambar 6. Flowchart Enkripsi dan Embed

Flowchart pada Gambar 6 merupakan alur secara umum dari proses Enkripsi dan Embed, dimulai dengan menginputkan gambar, pesan dan kunci. Melakukan inisialisasi InitialKey dan i sama dengan 0 dan dilanjutkan melakukan proses mengambil nilai InitialKey dan menyimpan pada tempCBC.

Terdapat kondisi jika i lebih kecil dari fileByte.length maka masuk ke kondisi berikutnya yaitu jika fileByte.length dikurangi i lebih kecil dari 16 maka masuk pada proses XOR antara pesan dengan tempCBC kemudian masuk pada proses enkripsi dimana sebelumnya pesan dilakukan padding agar genap 16byte dan hasil chiper-nya akan menjadi tempCBC dan dilanjutkan melakukan proses Embed. Dan Jika fileByte.length dikurangi I tidak lebih kecil dari 16 sama akan masuk pada proses XOR antara pesan dengan tempCBC kemudian masuk pada proses enkripsi dan hasil chiper-nya akan menjadi tempCBC yang akan digunakan pada perulangan berikutnya[11]. Dan jika kondisi i tidak lebih kecil dari fileByte.length maka akan dilanjutkan dengan proses Embed, kemudian menyimpan file dan selesai.

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



Gambar 7. Flowchart Ekstraksi dan Dekripsi

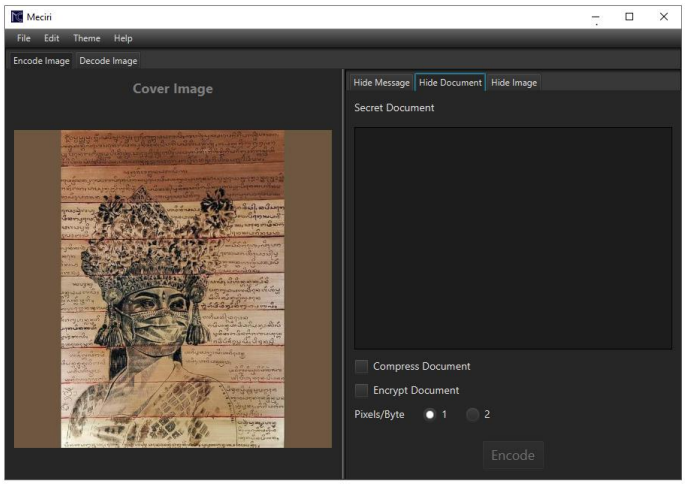
Flowchart secara umum dari proses Ekstraksi dan Dekripsi system ditunjukkan oleh Gambar 7 Proses dimulai dengan menginputkan gambar, pesan dan kunci. Setelah itu dilakukan proses Ekstraksi pesan pada gambar, dilanjutkan dengan melakukan inisialisasi initialkey dan i sama dengan 0 serta melakukan proses mengambil nilai initialkey dan menyimpan pada tempCBC.

Terdapat kondisi jika i lebih kecil dari fileByte.length maka masuk kekondisi berikutnya yaitu jika fileByte.length dikurangi i lebih kecil dari 16 maka masuk pada proses XOR antara pesan dengan tempCBC kemudian masuk pada proses enkripsi dimana sebelumnya pesan dilakukan padding agar genap 16 byte dan hasil chiper-nya akan menjadi tempCBC dan dilanjutkan menyimpan file. Dan jika fileByte.length dikurangi i tidak lebih kecil dari 16 maka sama akan masuk pada proses Dekripsi dan dilanjutkan dengan proses XOR antara pesan dengan tempCBC dan hasil dekripsinya akan menjadi tempCBC yang akan digunakan pada perulangan berikutnya. Dan jika i tidak lebih kecil dari fileByte.length maka akan dilanjutkan dengan menyimpan file dan selesai.

3. Hasil dan Pembahasan

3.1. Antarmuka Aplikasi

Antarmuka dari sistem yang dibuat untuk mengimplementasikan penelitian ini dibuat dengan bahasa pemorograman java. Pada antarmuka ini, terdapat 2 bagian yaitu bagian encode image, dan decode image.



Gambar 8. Tampilan sistem untuk Enkripsi dan penyisipan

Gambar 8. menunjukan implementasi tampilan aplikasi yang dibangun. Tampilan ini merupakan tampilan untuk melakukan enkripsi dan penyisipan (*embed*). Terdapat tiga pilihan tab atas yaitu untuk menyisipkan pesan dalam bentuk text, dokumen, dan gambar. Setelah gambar cover di-*input*-kan maka gambar *cover* akan ditampilkan pada aplikasi. Terdapat juga kotak centang di tab pesan dan dokumen untuk menyembunyikan atau mengenkripsi *file*. Kotak enkripsi akan membuka jendela yang memungkinkan *user* memvalidasi kata sandi tau memilih gambar sebagai kata sandi.

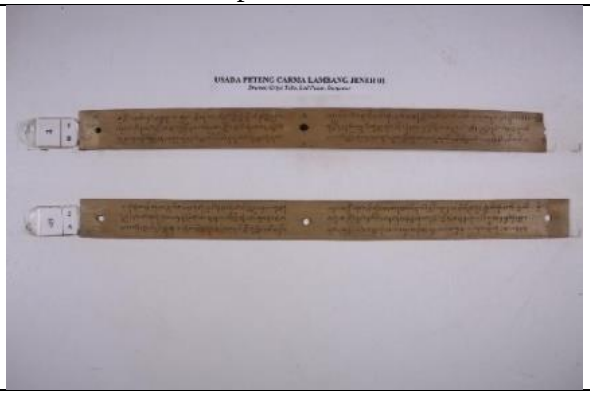
Tombol pilihan tersedia dalam 2 jenis untuk memilih jumlah piksel per byte (atau piksel per piksel). Dalam hal gambar, ini memungkinan user untuk memilih antara kualitas yang lebih baik atau kapasitas penyimanan yang lebih baik. Kemudian, tombol Encode memungkinkan user memilih tujuan gambar yang disandikan. Jika operasi berhasil, sebuah jendela akan memberi tahu user bahwa proses telah berhasil.

3.2. Aplikasi Pengujian

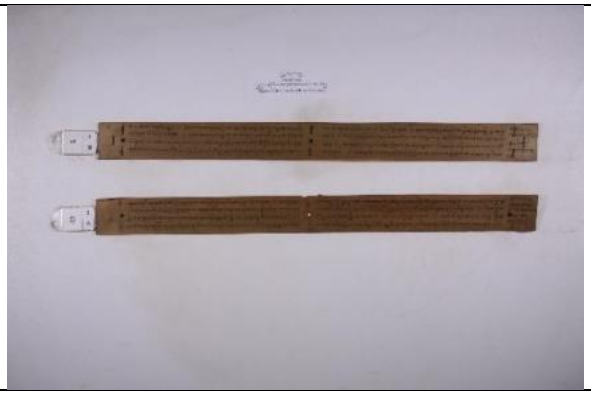
Pengujian dari sistem pengaman file pdf dengan menggunakan dua metode kemananan yaitu dengan algoritma AES-128 dan steganografi *Least Significant Bit* (LSB) pada citra digital ini bertujuan untuk memastikan apakah sistem yang dikembangkan sudah tepat sesuai dengan kebutuhan didapatkan.

a. MSE dan PSNR
   Pengujian ini dilakukan untuk mengetahui kemiripan *stegoimage* dengan *cover-image* menggunakan metode steganografi *Least Significant Bit* (LSB) dengan menghitung nilai PSNR. Pada pengujian ini dilakukan penyisipan file manuskrip lontar bali dengan format .pdf ke dalam *cover image* dengan format .png berukuran 1404x936 piksel. Dimana gambar tersebut memiliki perbedaan objek gambar dengan komposisi warna dalam piksel-pikselnya. Setiap gambar disisipkan sebanyak 1 kali dengan file pdf.

Tabel 1. *Cover-image* untuk pengujian

No	Tampilan Gambar	Nama Gambar
1		usada-peteng-carma-lambang-jener.png

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

2		usada-mata.png

Pada tabel 1 adalah contoh *cover-image* yang akan digunakan untuk wadah disisipkan pesan dokumen dalam bentuk .pdf

Tabel 2. Hasil pengujian nilai MSE

No	Gambar (.png)	File PDF	MSE(Red)	MSE(Green)	MSE(Blue)	MSE(Total)
1	usada-peteng-carma-lambang-jener.png	Data1	0.0221604	0.00571322	0.0235827	0.0171521
2	usada-mata.png	Data2	0.0257689	0.00572464	0.0284565	0.0199834

pada tabel 2 hasil pengujian *file* menggunakan MSE, didapatkan nilai MSE lebih kecil dari 0.15. sehingga dapat dikatakan akurasi dari pengujian citra digital dapat diterima dengan rata-rata 0.01856775 dB.

Tabel 3. Hasil pengujian nilai PSNR

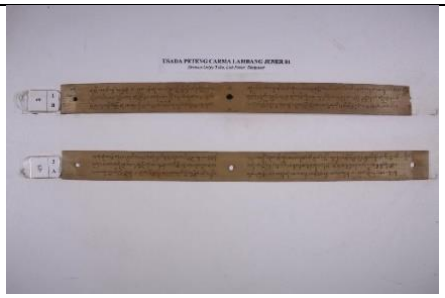
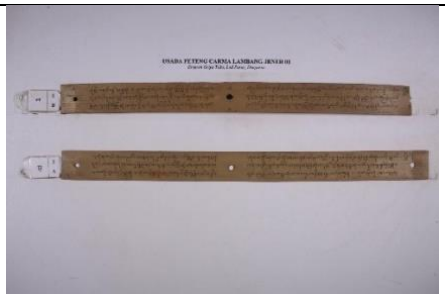
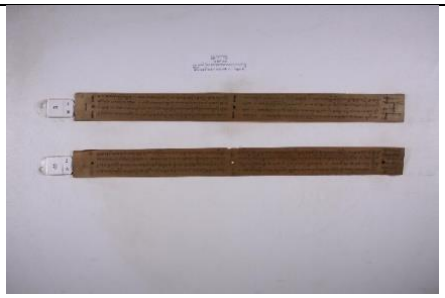
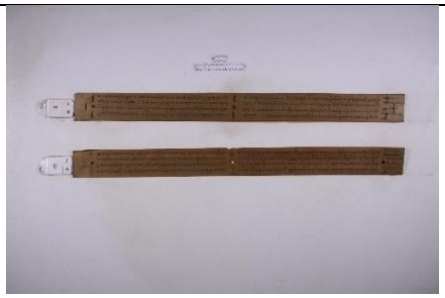
No	Gambar (.png)	File PDF	PSNR (Red)	PSNR (Green)	PSNR (Blue)	PSNR (Total)
1	usada-peteng-carma-lambang-jener.png	Data1	93.5071	106.984	92.8851	97.7919
2	usada-mata.png	Data2	91.9985	106.964	91.0064	96.6562

pada tabel 3 hasil pengujian *file* menggunakan PSNR dengan mengambil sempel *file* citra digital, didapatkan hasil yang sangat baik, yaitu lebih besar dari 37 desibel (dB), didapatkan bahwa nilai PSNR dari total *channel red* nilai rata-rata PSNR untuk penyisipkan pdf dari daya tamping maksimal gambar adalah 92.83349, nilai rata-rata PSNR dari total *channel green* untuk penyisipan pdf dari daya tampung maksimal adalah 106.7154, dan nilai rata-rata PSNR dari total *channel blue* untuk penyisipan pdf dari daya tamping maksimal gambar adalah 92.54417.dengan rata-rata 97.22405 dB.

b. Perbandingan tampilan *cover image* dengan *stegoimage*

Tabel 4. Contoh Perbandingan tampilan *cover-image* dengan Stegoimage

No	*Cover image*	*Stegoimage*

1		
2		

Pada tabel 4 adalah contoh perbandingan tampilan *cover-image* dengan *stegoimage* tidak akan terlihat perbedaan yang significant oleh indra pengelihatan manusia walaupun pesan yang disisipkan sebesar 100% dari daya tamping maksimal gambar.

c. Pengujian kesamaan file dengan *Hamming Distance*

Tabel 5. Hasil pengujian kesamaan file dengan *Hamming Distance*

No	File input		File Output		Hamming Distance	Persentase Kesamaan file pdf (%)
	Nama (pdf)	Ukuran (kb)	Nama (pdf)	Ukuran (kb)		
1	Data1	7.04	Dekrip1	7.04	0	100
2	Data2	6.99	Dekrip2	6.99	0	100

Pada tabel 5 didapatkan bahwa semua file yang diuji kesamaannya menunjukan *hamming* distance sebanyak 0, hal tersebut berarti antara bit-bit file pdf asli dengan bit bit file pdf setelah dienkripsi-dekripsi tidak ada yang terbalik (sama). Jadi, dari 10 kali pengujian, didapatkan bahwa file pdf asli dapat dikembalikan dengan presentase kesamaan 100%.

4. Kesimpulan

Penerapan steganografi menggunakan metode penyisipan least significant bit (LSB) yang dibangun pada aplikasi ini berhasil dalam menyisipkan chipper text terenkripsi pada gambar manuskrip lontar bali dengan format .png dan juga berhasil dalam mengekstraksi gambar dan mengembalikan berkas (file) pdf terenkripsi. Metode kriptografi AES (Advanced Encryption Standard) yang dibangun pada aplikasi ini juga berhasil melakukan enkripsi maupun dekripsi terhadap (file) pdf manuskrip lontar bali sehingga pesan dapat disandikan dan dikembalikan seperti semula dengan persentase keberhasilan 100%. Dilihat dari nilai MSE dan PSNR didapatkan bahwa besarnya pesan tidak berpengaruh pada tingkat akurasi karena pesan akan dimaksimalkan menjadi 16 karakter dan fungsi pad pada library AES 128 bit, sehingga penyisipan citra digital dikatakan sangat baik, karena tidak terdapat perbedaan yang significant melalui sinyal. Hasil pengujian membuktikan adanya peningkatan keamanan serta nilai imperceptibility yang tetap terjaga. Hal ini dibuktikan dengan hasil rata-rata nilai MSE 0.01856775 dB dan PSNR 97.22405 dB. Maka pengguna yang pertama kali mengenkripsi file memiliki bukti definitif atas kepemilikan hak cipta dan keamanan data.

.

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

Daftar Pustaka

[1] J. I. Logika, “Penelitian ini mengembangkan sebuah metoda pengamanan pesan yang dinamakan Steganografi dan dibangun pula sebuah Aplikasi Steganografi dengan algoritma Least Significant Bit . Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan,” vol. I, no. 2, pp. 35–38, 2019.

[2] U. A. Anti, A. H. Kridalaksana, and D. M. Khairina, “Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF),” *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 12, no. 2, p. 104, 2017, doi: 10.30872/jim.v12i2.658.

[3] J. I. Sari, H. T. Sihotang, and T. Informatika, “Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma Hill Cipher Dan Metode Least Significant Bit (LSB),” *J. Mantik Penusa*, vol. 1, no. 2, pp. 1–8, 2017, [Online]. Available: http://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/253.

[4] S. Nur’aini, “Steganografi Pada Digital Image Menggunakan Metode Least Significant Bit Insertion,” *Walisongo J. Inf. Technol.*, vol. 1, no. 1, p. 73, 2019, doi: 10.21580/wjit.2019.1.1.4025.

[5] Ketut Gura Arta Laras, “DIGITISASI LONTAR MUSEUM NASKAH LONTAR DESA ADAT DUKUH PENABAN, KECAMATAN KARANGASEM,KABUPATEN KARANGASEM, BALI,” vol. 26, no. 1, p. 6, 2021.

[6] A. Hafiz, “Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (Lsb),” *J. Cendikia*, vol. 17, no. 1, pp. 194–198, 2019.

[7] I. D. FADHILAH, “RANCANG BANGUN SISTEM KEAMANAN DATA DENGAN METODE STEGANOGRAFI LSB BERBASIS WEBSITE.” p. 85, 2019.

[8] D. Darwis, R. Prabowo, and N. Hotimah, “Kombinasi Gifshuffle, Enkripsi AES dan Kompresi Data Huffman untuk Meningkatkan Keamanan Data,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 5, no. 4, p. 389, 2018, doi: 10.25126/jtiik.201854727.

[9] N. Anwar, “Perancangan Steganografi Hidden Message Dengan Metode Least Significant Bit Insertion (Lsb) Berbasis Matlab,” *J. Algoritm. Log. dan Komputasi*, vol. 1, no. 1, pp. 25–30, 2018, doi: 10.30813/j-alu.v1i1.1107.

[10] U. Sara, M. Akter, and M. S. Uddin, “Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study,” *J. Comput. Commun.*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[11] G. Wibisono, T. Waluyo, and E. I. H. Ujianto, “Kajian Metode Metode Steganografi Pada Domain Spasial,” *JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer)*, vol. 5, no. 2, pp. 259–264, 2020, doi: 10.33480/jitk.v5i2.1212.

This page is intentionally left blank.