Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 12, No. 3, Juni 2025, hlm. 687-694 e-ISSN: 2528-6579

ALGORITMA ENKRIPSI DAN *EMBEDDING* CITRA DIGITAL MENGGUNAKAN *LOGISTIC MAP*-3 DAN *LEAST SIGINIFICANT BIT*

Edi Sukirman[1], Suryadi MT[*2], Rindang R Pratiwi[3]

[1,3]Universitas Gunadarma, Depok, [2]Universitas Indonesia, Depok
Email: [1]ediskm@staff.gunadarma.ac.id, [2]yadi.mt@sci.ui.ac.id, [3]rindangrp@gmail.com
[*]Penulis Korespondensi

(Naskah masuk: 5 November 2024, diterima untuk diterbitkan: 20 Juni 2025)

Abstrak

Upaya pencegahan kebocoran atau pencurian data dan informasi digital dilakukan untuk menghindari penyalahgunaan oleh pihak ketiga yang menimbulkan berbagai kerugian. Pencegahan tersebut salah satunya dengan meningkatkan upaya keamanan data dan informasi melalui penerapan proses enkripsi dan dekripsi serta *embedding* dan ekstraksi (dalam dua tingkat pengamanan). Citra digital yang sudah dienkripsi (disandikan) sehingga menghasilkan citra yang tidak tampak (gambar yang blur atau berantakan). Selanjutnya agar tidak mencurigkan maka dilakukan tahapan pengamanan berikutnya yakni dengan disembunyikan (di embedding) pada citra lainnya yang bersifat umum. Teknik enkripsi yang digunakan dalam penelitian ini adalah fungsi *chaos Logistic map*-3 dan teknik penyisipan data *Least Significant Bit*-1 terhadap data berupa citra digital. Algoritma yang dirancang dalam paper ini adalah melakukan proses enkripsi dan embedding secara berurutan. Begitu pula untuk mendapatkan data dan informasi asli dilakukan dengan proses ekstraksi dan dekripsi secara berurutan. Hasil pengujian berdasarkan data pengujian yang digunakan pada paper ini menunjukkan bahwa data citra digital rahasia atau asli (*secret image*) telah berhasil dienkripsi dan disisipkan dengan baik, sehingga tidak dapat dikenali bahwa data gambar tersebut berisi data citra rahasia (*secret image*). Hal tersebut ditunjukkan dengan nilai PSNR nya tak hingga. Begitu pula dengan proses ekstraksi dan dekripsi yang berhasil dilakukan sehingga data citra rahasia (*secret image*) dapat diperoleh kembali dengan baik. Hal tersebut ditunjukkan dengan nilai PSNR nya tak hingga.

Kata kunci: *Algoritma Embedding-Extracting, Algoritma Encryption-Decryption, Citra Digital, Least Significant Bit*

DIGITAL IMAGE ENCRYPTION AND EMBEDDING ALGORITHM USING LOGISTIC MAP-3 AND LEAST SIGNIFICANT BIT

Efforts to prevent leakage of digital data and information are carried out to avoid misuse by third parties that cause various losses. One of these preventions is by increasing the security of data and information through the application of encryption and decryption processes as well as embedding and extracting (in two levels of security). Digital images that have been encrypted (coded) so that they produce invisible images (blurry or messy images). Furthermore, so as not to be suspicious, the next security stage is carried out, namely by hiding (embedding) in other general images. The encryption technique used in this research is the chaos function of Logistic map-3 and the Least Significant Bit-1 data insertion technique. The algorithm designed is to perform the encryption and embedding processes sequentially. Likewise, to get the original data and information, it is done by sequentially extracting and decrypting processes. The test results based on the test data used, show that the original digital image data (secret image) has been successfully encrypted and embedded properly, so it cannot be recognized that the image data contains plain image data (secret image). This is indicated by the infinite PSNR value. Likewise, the extraction and decryption processes were successfully carried out so that the plain image data (secret image) could be retrieved properly. This is indicated by the infinite PSNR value.

Keywords: *Digital Image, Embedding-Extracting Algorithm, Encryption-Decryption Algorithm, Least Significant bit*

1. PENDAHULUAN

Keamanan data dan informasi menjadi suatu tuntutan untuk menjaga kerahasiaan dalam pernyimpanan khususnya ialah data dan informasi digital. Sehingga diperlukan upaya yang sungguh-sungguh untuk melindungi data dan informasi digital tersebut agar tidak mudah disalahgunakan oleh orang yang tidak bertanggung jawab.

Usaha pengamanan data citra digital telah banyak dilakukan dengan teknik kriptografi (Menezes, et al., 1996; Schneier, 1996; Cetin, 2009), aspek aljabar pada kriptografi (Koblits, 1998), Teknik kriptografi dengan algoritma *Advanced Encryption Standard*-AES (Stallings, 2011), algoritma MD5 (Nguyen, et al., 2010) dan algoritma enkripsi Diffie-Hellman dan *Multi-key* (Chen, et al., 2012).

Usaha pengamanan dengan teknik steganografi juga demikian telah banyak dilakukan diantaranya dengan Teknik LSB dan DCT (Walia, et al., 2010), penyembunyian pesat ke dalam citra digital menggunakan teknik LSB (Chan, et al., 2004), teknik *Hash Based Least Significant Bit* untuk penyembunyian video digital (Dasgupta, et al., 2012), penyembunyian suara digital dengan Teknik LSB (Rakshit, et al., 2021), penyembunyian dengan teknik *Block*-DCT dan *Huffman Encoding* (Nag, et al., 2010), penyembunyian dengan teknik *Improved Image Quality* (Al-Satnawi, 2012) dan Teknik penyembunyian citra digital dengan *modulo operator* (Wang, 2005). Hal tersebut menginsipirasi untuk dilakukan teknik pengamanan data digital secara simultan, yang diawali dengan teknik kriptografi dan dilanjutkan dengan teknik steganografi.

Penerapan teknik kriptografi memiliki berbagai macam metode diantaranya yaitu dengan metode *chaos* yang memiliki karakteristik sensivitas terhadap nilai awal, yaitu diantaranya penggunaan fungsi *chaos Reverse 2-dimensional Chaotic Map* (Zhang, et al., 2013), *Logistic Map Based on Feedback Stream Cipher* (Hossam, et al., 2023), *new chaotic algorithm* (Gao, et al., 2006), *logistic map* (Pereek, et al., 2006; Eva, et al., 2013; Suryadi, et al., 2014), *chaotic standard* dan *logistic map*s (Patidar, et al., 2009), menggunakan Henon map (Vajargah, et al., 2015), teknik sistem *chaotic* 1D (Zhou, et al., 2014), Teknik *New Modified map* atau MS *map* (Suryadi, et al., 2017), menggunakan teknik *Chaotic Permutation Multiple Circular Shrinking and Expanding* (Suryanto, et al., 2016; Suryanto, et al., 2017), menggunakan teknik *zigzag map* dan *hash function* (Magfirawaty, et al., 2018), menggunakan teknik *MS Map* dan *the Dyadic Transformation Map* (Suryadi, et al., 2020), dan menggunakan teknik *Gauss Map* dan *Circle Map* (Suryadi, et al., 2020). Prinsip seperti ini sama halnya dengan prinsip difusi dalam merancang sebuah algoritma kriptografi (Schneier, 1996; Zhang, et al., 2013). Prinsip difusi ini melakukan perubahan suatu bit nilai awal *chaos* yang dapat menyebabkan *cipher image* sangat sulit untuk didekripsi (Schneier, 1996). Maka untuk itu digunakan algoritma berbasis fungsi *chaos Logistic Map* yang memiliki sensitifitas dalam perubahan nilai awal. Jika nilai awal sedikit berbeda maka hasil pemetaan atau pembangkitan dengan fungsi *chaos* tersebut akan sangat berbeda secara signifikan untuk sejumlah kali iterasi. Untuk itu, pada paper ini digunakan salah satu jenis fungsi *chaos* hasil pengembangan dari fungsi *chaos Logistic Map* yaitu *Logistic Map*-3. Hal tersebut dikarenakan fungsi *chaos Logistic Map*-3 memiliki rentang nilai *r* yang lebih luas dibanding dua *logistic map* yang lainnya (Hossam, et al., 2023).

Penelitian lainnya melakukan upaya pengamanan data teks digital yang mengkombinasikan teknik kriptografi dan steganografi, yaitu menggunakan enkripsi *hybrid* (teknik BlowFish dan AES) yang dianjutkan dengan proses *embedding* pada citra digital menggunakan teknik LSB (Alanzy, et al., 2023). Selain itu terdapat penelitian terkait pengamanan data citra digital dengan dienkripsi menggunakan permutasi Josephus dan Teknik steganografi menggunakan LSB 3-3-2 (Yanuar, et al., 2024). Dalam paper ini rancangan algoritma yang dikembangkan yakni algoritma untuk proses enkripsi, yang diikuti dengan proses e*mbedding* secara simultan. Adapun untuk proses enkripsinya menggunakan fungsi *chaos Logistic Map*-3 dan proses *embedding*-nya menggunakan metode *Least Significant Bit-1* (LSB-1). Hal tersebut karena fungsi Logistic Map-3 bentuknya relatif sederhana dan bersifat chaotic. Adapun pertimbangan penggunaan metode LSB-1 bit yakni upaya penyisipan yang sederhana yakni pada 1 bit terakhir yang relatif tidak melakukan perubahan yang signifikan pada cover image nya. Berdasarkan hasil rancangan algoritma enkripsi dan *embedding* serta kebalikannya (algoritma ekstraksi dan dekripsi), selanjutnya diimplementasikan terhadap data uji citra digital. Hasil uji cobanya dianalisis berdasarkan fungsional proses dan analisis kualitas (kesamaan) citra, baik kualitatif maupun kuantitatif.

2. METODE PENELITIAN

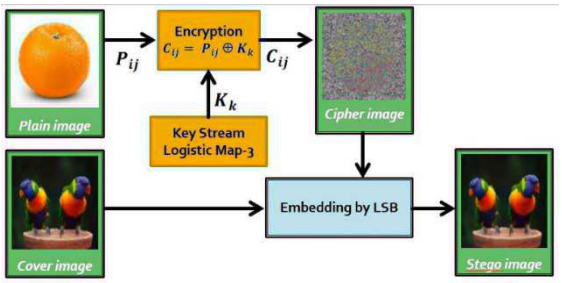
Pada paper ini dijelaskan terkait upaya pengamanan data dengan menggunakan metode kriptografi dan steganografi secara simultan. Tahap pertama dilakukan metode kriptografi dengan melakukan proses enkripsi terhadap data digital dan selanjutnya dilakukan tahap kedua dengan menerapkan metode stagnografi melalui proses *embedding*.

Proses enkripsi terhadap data citra digital yang diamankan (*plain image*) dengan memanfaatkan *keystream* yang dihasilkan (dibangkitkan) dari fungsi *chaos*. Adapun proses enkripsinya menggunakan operasi antar *bit* dengan operator XOR antara *bit* dari semua piksel citra asli (*plain image*) dengan *bit* dari *keystream*. Sehingga dihasilkan citra yang tersandikan (*cipher image*).

Fungsi *chaos* yang digunakan pada paper ini yaitu *fungsi Logistic Map*-3 untuk membangkitkan bilangan acak yang bersifat *chaos*, sesuai dengan nilai awal dan parameter yang diinginkan. Adapun bentuk persamaan fungsi *chaos Logistic Map*-3 tersebut (Zhang, et al., 2013) dalam bentuk rekursif tampak pada persamaan (1).

$$x_{n+1} = r \times (1 - x_n) \times (1 - 1.2 \times x_n)^2 \qquad (1)$$

dengan $x_0 \in (0,1)$, $x_n \in (0,1)$ untuk $n = 1, 2, 3, ...$ dan $r \in (0,9.5)$



Gambar 1. Proses Enkripsi dan *Embedding* Citra Digital

Berdasarkan nilai awal x_0 dan nilai parameter r, dibangkitkan bilangan acak yang bersifat *chaos* berdasarkan persamaan (1). Barisan bilangan acak yang dihasilkan tersebut bernilai real, sehingga harus dilakukan proses konversi menjadi bilangan bulat yang merupakan *keystream*. Aturan konversi yang digunakan tampak sebagaimana persamaan (2) sebagai berikut:

$$\begin{cases} E_n = \|x_n \times 10^4\| \\ F_n = \lfloor E_n \rfloor \\ K_n = F_n \bmod 256 \end{cases} \quad (2)$$

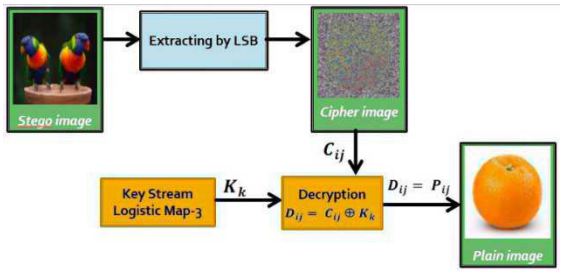
untuk $n = 1, 2, 3, \ldots$.

Selanjutnya secara simultan, *cipher-image* tersebut akan disembunyikan pada suatu *cover-image* dengan menggunakan metode *Least Significant Bit*-1 (LSB-1). Sehingga *cipher-image* nya tidak akan terlihat karena sudah disembunyikan dibalik *cover image*. Proses tersebut dinamakan dengan proses embedding. Sehingga diperoleh *file* data digital yang dinamakan *stego image*. Hal tersebut menunjukkan bahwa *plain image* sudah terlindung dalam dua tingkatan yakni dengan proses enkripsi (dalam hal ini perubahan nilai piksel) dan proses penyembunyian dibalik data citra digital lainnya (*cover image*). Secara ringkas dan sederhana proses tersebut dapat disajikan sebagaimana tampak pada Gambar 1.

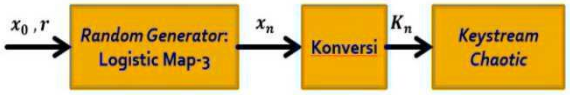
Berdasarkan Gambar 1, tampak bahwa hasil *cipher image* tersebut membuat orang (pihak ketiga) curiga bahwa gambar tersebut pasti ada yang dirahsiakan. Untuk itu dilakukan proses *embedding* (penyembunyian) pada citra lainnya sebagai *cover image* agar pihak ketiga tidak curiga (karena disembunyikan dibalik gambar pada umumnya).

Guna memperoleh kembali informasi dari *plain image*, dilakukan proses kebalikannya yakni proses *extracting* terlebih dahulu terhadap *stego image* dan dilanjutkan dengan proses dekripsi. Sehingga dapat diperoleh Kembali citra aslinya (*plain image*). Proses tersebut dapat disajikan secara sederhana dalam bentuk diagram sebagaimana tampak pada Gambar 2.

Keystream yang digunakan pada proses sebagaimana tampak pada Gambar 1 dan Gambar 2 diperoleh dari hasil pembangkit bilangan acak yang bersifat *chaos* (*chaotic*) Adapun prosesnya tampak sebagaimana pada Gambar 3.



Gambar 2. Proses *Extracting* dan Dekripsi Citra Digital



Gambar 3. Proses Pembentukan *Keystream Chaotic*

Hasil dari semua proses algoritma tersebut diukur kinerjanya berdasarkan perbandingan kualitas citra asli (*plain image*) dengan citra hasil *extracking* dan dekripsi. Hal lainnya juga dilihat hasil perbandingan antara *stego image* dengan *cover image*. Hal tersebut dilakukan dengan menghitung nilai *peak signal-to-noise ratio* (PSNR) nya.

3. HASIL DAN PEMBAHASAN

Berikut disajikan rancangan algoritma enkripsi dan embedding, berikut kebalikannya, juga hasil implementasi algoritma beserta analisis hasil uji cobanya berdasarkan data uji yang digunakan.

3.1. Algoritma Enkripsi dan *Embedding*

Rancangan algoritma enkripsi dan *embedding* diawali dengan proses enkripsi menggunakan *keystream* yang dihasilkan dari pembangkit bilangan acak (*random generator*) menggunakan fungsi *chaos Logistic Map*-3. Adapun persamaan fungsi tersebut sesuai dengan persamaan (1). Selanjutnya dilakukan proses embedding dari *cipher image* yang dihasilkan tersebut dengan teknik LSB-1. Rancangan algoritma enkripsi dan embedding tersebut secara lengkap dalam notasi *pseudocode* tampak pada Algoritma-1.

Algoritma 1. Enkripsi dan *Embedding* Citra Digital

Input: x_0, r, *plain image* (P_k) dan *cover image*
Output: *encrypted image* (C_k) dan *stego image* (S_k)

1. Baca x_0, r, $P_k(m \times n)$
2. $N = m \times n$; $k = 0$
3. While $k \leq (N-1)$ do
4. Hitung x_k: gunakan persamaan (1)
5. $K_k = floor(X_k * 10^4) \bmod 256$
6. $C_k = P_k \oplus K_k$
7. $k = k + 1$
8. Endwhile
9. Tampilkan C_k dalam *domain* citra
10. Embedding setiap 1 piksel C_k ke dalam 1 bit S_k
11. Tampilkan S_k dalam *domain* citra

Selanjutnya untuk memperoleh kembali data citra digital yang sudah dienkripsi dan disembunyikan (*embedding*), dilakukan proses *extracting* dan dilanjutkan dengan proses dekripsi. Adapaun rancangan algoritma yang dimaksud tersebut tampak sebagaimana Algoritma-2.

Algoritma 2. Ekstraksi dan Dekripsi Citra Digital

Input: x_0, r , *stego image* (S_k)
Output: *extracted image* (C_k) dan *decrypted image* (D_k)
1. Baca x_0, r dan stego image (S_k)
2. Ekstrak setiap 1 bit S_k dan simpan sebagai C_k
3. $N = m \times n;\ k = 0$
4. while $k \leq (N-1)$ do
5. Hitung x_k: gunakan persamaan (1)
6. $K_k = floor(X_k * 10^4)\ mod\ 256$
7. $D_k = C_k \oplus K_k$
8. $k = k + 1$
9. Endwhile
10. Tampilkan D_k dalam *domain* citra

3.2. Implementasi Algoritma

Berdasarakan rancangan algoritma sebagaimana tampak pada Algoritma-1 dan Algoritma-2, dilakukan implementasi program aplikasinya. Adapun tampilan menu proses enkripsi dan embedding serta kebalikannya yang dilakukan secara berurutan tampak pada Gambar 4.

3.3. Analisis Hasil Uji

Simulasi dari hasil implementasi algoritma dilakukan menggunakan data uji sebagaimana tampak pada Tabel 1, dengan menggunakan nilai awal dan parameter nya adalah $x_0 = 0.3$ dan $r = 8.4$.

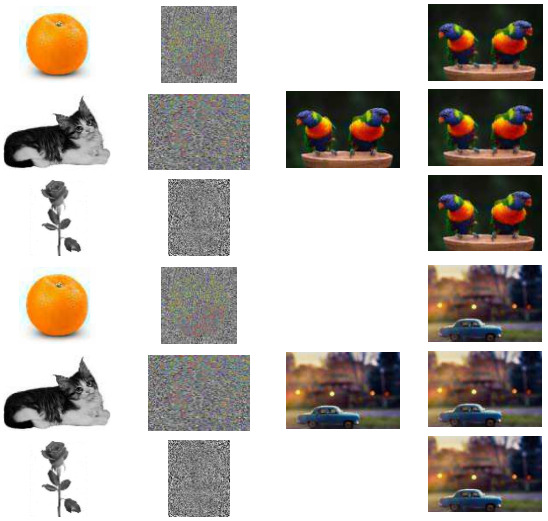
Pada Tabel 1 tampak data uji ke-1 sampai dengan data uji ke-3 ialah data uji yang digunakan sebagai citra asli (*plain image*) atau citra rahasia (*secret image*). Data citra tersebut yang diamankan dengan cara dienkripsi dan disembunyikan (*embedding*). Sedangkan data ke-4 dan data ke-5 adalah data yang digunakan sebagai *cover image*, yakni berfungsi sebagai tempat penyembunyian dari data ke-1 sampai data ke-3 secara masing-masing. Adapun hasil dari uji coba semua kemungkinan data uji yang digunakan tersebut tampak pada Tabel 2.

Tabel 2 memperlihatkan hasil proses enkripsi dan *embedding* dari data uji. Tampak bahwa secara kasat mata *stego image*-nya telihat sama (tidak ada perbedaan) dengan *cover image*. Hal tersebut berarti penyembunyian data citra asli kedalam *cover image* dapat dilakukan dengan baik. Sehingga pihak lain tidak curiga bahwa pada *stego image* sebenarnya ada data rahasia (data asli) yang telah disembunyikan. Dengan demikian algoritma yang diusulkan pada paper ini berfungsi dengan sangat baik.

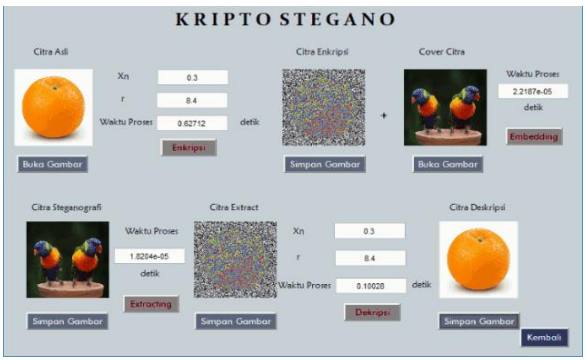
Tabel 1. Data Uji Citra Asli dan *Cover Image*

Test Data	Image Name	Image Display	File Size
1.	Orange.png (plain image)		301 kb
2.	Catgray.png (plain image)		378 kb
3.	Rose.bmp (plain image)		232 kb
4.	Bird.png (cover image)		22.8 mb
5.	Car.bmp (cover image)		871 kb

Tabel 2. Hasil Uji Proses Enkripsi dan *Embedding*

Plain Image	*Cipher Image*	*Cover Image*	*Stego Image*
			

Selanjutnya untuk memperoleh kembali data aslinya (*plain image*) atau data rahasia (*secret image*) dari data *stego image*, dilakukan dengan menjalankan proses ekstraksi dan dekripsi. Hasil uji terhadap data uji yang digunakan tampak pada Tabel 3.



Gambar 4. Tampilan Menu Proses Enkripsi dan *Embedding*

Tabel 3. Hasil Uji Proses Ekstraksi dan Dekripsi

Cipher image	*Cover image*	*Stego image*	*PSNR (dB)*
			Inf (∞)
			Inf (∞)
			Inf (∞)
			Inf (∞)
			Inf (∞)
			Inf (∞)

Tampak pada Tabel 3 bahwa hasil uji program aplikasinya yang merupakan implementasi dari algoritma ekstraksi dan dekripsi, berhasil mengembalikan data asli (*plain image*) atau data rahasia (*secrete image*) yang telah disembunyikan pada stego image berupa citra terdekripsi (*decrypted image*). Citra terdekripsi tersebut tampak secara kasat mata sama dengan data aslinya (*plain image*).

3.4. Analisis Kualitas Citra

Keberhasilan proses enkripsi dan *embedding* dianalisis berdasarkan kualitas citra secara kuantitatif dengan perhitungan nilai *peak signal-to-noise ratio* (PSNR). Untuk hal ini akan dihitung PSNR antara data *cover image* dengan *stego image*. Perhitungan nilai PSNR dalam satuan *decibel* (dB) diperoleh berdasarkan persamaan (3) dan persamaan (4).

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (3)$$

dengan:

$$MSE = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(S_{ij}-C_{ij}\right)^2 \quad (4)$$

S_{ij}: intensitas piksel dari *stego image*
C_{ij}: intensitas piksel dari *cover image*
$M \times N$: ukuran citra (*stego image* dan *cover image*)

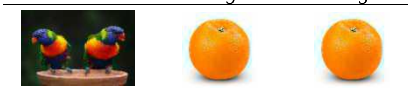
Adapun hasil perhitungan nilai PSNR berdasarkan persamaan (3) dan persamaan (4) untuk semua data uji tampak pada Tabel 4.

Tampak pada Tabel 4, nilai PSNR *cover image* terhadap *stego image* untuk semua data uji adalah *infinity* (takhingga). Hal tersebut menunjukkan bahwa nilai rata-rata dari selisih kuadrat antara semua nilai intensitas piksel *stego image* dengan *cover image* adalah nol. Dengan demikian dapat diartikan bahwa *stego image* dan *cover image* merupakan citra yang tepat sama. Sehingga *plain image* yang disembunyikan pada *cover image* sangat tidak tampak.

Tabel 4. Hasil Nilai PSNR *Cover Image* terhadap *Stego Image*

Stego Image	*Extract Image*	*Decrypted Image*
		
		
		
		
		
		

Tabel 5. Nilai PSNR *Decrypted Image* terhadap *Plain Image*

Stego Image	*Decrypted Image*	*Plain Image*	*PSNR (dB)*
			Inf (∞)
			Inf (∞)
			Inf (∞)
			Inf (∞)
			Inf (∞)
			Inf (∞)

Selanjutnya dengan cara yang sama dilakukan analisis kualitas citra atas keberhasilan proses ekstraksi dan dekripsi secara kuantitas yaitu dihitung nilai PSNR menggunakan persamaan (3) dan persamaan (4). Dalam hal ini perhitungan nilai PSNR terhadap citra terdekripsi (*decrypted image*) dengan citra asli (*plain image*). Adapun hasil uji coba terhadap data uji tampak pada Tabel 5.

Tabel 5 memperlihatkan bahwa nilai nilai PSNR untuk semua data uji adalah *infinity* (takhingga). Hal tersebut menunjukkan bahwa nilai rata-rata dari

selisih kuadrat antara semua nilai intensitas piksel *decrypted image* dengan *plain image* adalah nol.

Tabel 6 berikut menunjukkan perbandingan nilai PSNR dari tiga (3) penelitian walaupun data simulasi yang digunakan masing-masing berbeda.

Tabel 6. Hasil Perbandingan Nilai PSNR atas 3 Peneliti

Peneliti	Plain	Cover	Rata-rata nilai PSNR	
			Stego-Cover	Decrypt-Plain
Alanzy, et al. 2023	Citra	Citra	83,8657	NA
Yanuar, et al. 2024	Teks	Citra	42,9048	Inf (∞)
Diusulkan (Edi, et al. 2025)	Citra	Citra	Inf (∞)	Inf (∞)

Dengan demikian dapat diartikan bahwa *decrypted image* dan *plain image* merupakan citra yang tepat sama. Sehingga algoritma yang dikembangkan pada paper ini mampu mengembalikan *plain image* yang disembunyikan pada *cover image* tanpa ada informasi yang hilang.

Tampak dari Tabel 6, algoritma yang diusulkan dalam paper ini memperlihatkan rata-rata nilai PSNR adalah infinity (takhingga) baik antara *stego image* dengan *cover image*, maupun antara *decrypted image* dengan *plain image*. Hal tersebut menunjukkan tidak adanya perbedaan antara *stego image* dengan *cover image*, dan juga tidak adanya perbedaan antara *decrypted image* dengan *plain image*. Sehingga algoritma yang dikembangkan ini sebagai upaya penyembunyian hasil enkripsi pada cover image tidak menimbulkan kecurigaan pihak ketiga, serta algoritma ini juga mampu mengembalikan *plain image* yang disembunyikan pada *cover image* tanpa ada informasi yang hilang.

4. KESIMPULAN

Berdasarkan analisis dari hasil implementasi dan uji coba terhadap semua data uji citra digital yang digunakan, didapat kesimpulan sebagai berikut:

a. Hasil implementasi algoritma enkripsi dan *embedding* serta extracting dan dekripsinya terhadap data citra asli (*plain image*) dapat dapat berfungsi dengan baik dan dapat mengembalikan hasilnya seperti data aslinya dengan tepat sama.
b. *Stego image* yang dihasilkan pada proses *embedding*, secara kualitatif (kasat mata) tampak sama persis dengan *cover image*. Secara kuantitatif ditunjukkan dengan nilai PSNR nya adalah tak hingga. Hal tersebut berarti *stego image* dan *cover image* tepat sama. Sehingga tidak diketahui bahwa di dalam data *stego image* sebenarnya mengandung (berhasil disembunyikan) informasi berupa *plain image*.
c. *Decrypted image* yang dihasilkan dari proses *extracting* dan dekripsi juga tampak sama dengan data *plain image*. Secara kuantitatif ditunjukkan dengan nilai PSNR nya tak hingga. Sehingga algoritma tersebut mampu mendapatkan kembali data aslinya dari hasil enkripsi dan *embedding* dengan sempurna (tepat sama) atau tanpa ada informasi yang hilang

DAFTAR PUSTAKA

AL-SHATNAWI A.M., 2012. A New Method in Image Steganography with Improved Image Quality, *Applied Mathematical Sciences*, 6 (79), 3907–3915.

ALANZY, MAY., ALOMRANI, R., ALQORNI, B., and ALMUTAIRI, Saad, 2023. Image Steganography Using LSB and Hybrid Encryption Algorithms, *Applied Sciences*, 13, 11771, 1-20. https://doi.org/10.3390/app132111771

CETIN KAYA KOC, 2009. *Cryptographic Engineering*, Springer, New York.

CHAN, CHI-KWONG, and CHENG, 2024. L.M, Hiding data in images by simple LSB substitution, *Pattern Recognition*, 37, 469–474.

CHEN, LIQUN, and CHEN YU, 2012. The n-Diffie–Hellman problem and multiple-key encryption, *International Journal Information Security, Springer*, 11, 305–320.

DASGUPTA, K., MANDAL, J. K., and DUTTA, P., 2012. Hash Based Least Significant Bit Technique For Video Steganography (HLSB), *Proceedings of International Journal of Security, Privacy and Trust Management*, 1, 1–11.

DUE H NGUYEN, THUY T NGUYEN, TAN N DUONG, and PHOMH H PHAM, 2010. Cryptanalysis of MD5 on GPU Cluster, *Proceedings of International Conference on Information Security and Artificial Intelligence*, 2, 910–914.

EVA N and SURYADI MT., 2013. Chaos-Based Encryption Algorithm for Digital Image, *Proceedings IICMA*, 169–177.

GAO, H., ZHANG, Y., LIANG, S., and LI, D., 2006. A new chaotic algorithm for image encryption, *Journal of Chaos, Solutons and Fractals*, 29, 393–399.

HOSSAM ELDIN H AHMED, and AYMAN H, ABD EL-AZIEM., 2023. Image Encryption Using Development of Chaotic Logistic Map Based on Feedback Stream Cipher, *Recent Advances In Telecommunications, Informatics And Educational Technologies*, August, 274–283.

KOBLITZ, NEAL., 1998. *Algebraic Aspects of Cryptography*, Springer-Verlag Verlin Heidelberg, Germany.

MAGFIRAWATY, SURYADI MT, and RAMLI, K., 2010. Performance Analysis of zigzag map and hash function to generate random number, *IEEE Xplore*, DOI: 10.1109/ICELTICS.2017.8253286.

MENEZES, ALFRED J., VAN OORSCHOT, PAUL C., and VANSTONE, SCOTT A., 1996. *Handbook of Applied Cryptography*, CRC Press.

NAG, AMITAVA, BISWAS, S., SARKAR, D., SARKAR, P., 2010. A novel technique for image steganography based on Block-DCT and Huffman Encoding, *International Journal of Computer Science and Information Technology*, 2 (3), 1013-112.

PATIDAR, V., PAREEK, N.K., and SUD, K.K., 2009. A new subtitution-diffusion based image cipher using chaotic standard and logistic maps, *Journal of Communications in Nonlinear Science and Numerical Simulation*, 14, 3056–3075.

PAREEK, N. K., PATIDAR, V., and SUD, K. K., 2006. Image encryption using chaotic logistic map, *Journal of Image and Vision Computing*, 24, 926–934.

RAKSHIT, PRANATI., GANGULY, SREEPARNA., PAL, SOUVIK., and LE, DAC-NHUONG., 2021. Securing Technique Using Pattern-Based LSB Audio Steganography and Intensity-Based Visual Cryptography, *Computers Materials & Continua, 67, Issue* 1, 1207-1224.

SCHNEIER, BRUCE., 1996. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. John Wiley & Sons.

SHIUH-JENG WANG., 2005. Steganography of capacity required using modulo operator for embedding secret image, *Applied Mathematics and Computation*, 164, 1613–1626.

STALLINGS, WILLIAM., 2011. *Cryptography and Network Security: Principles and Practice*, 5th edition, Pearson Education, Inc., Publishing as Prentice Hall., New Jersey.

SURYADI MT, NURPETI, E., and Widya, D., 2014. Performance of Chaos-Based Encryption Algorithm for Digital Image, *TELKOMNIKA Telecommunication, computing, electronics, and control*, 12 (3), 675–682.

SURYADI MT, MARIA Y.T.I., and YUDI SATRIA., 2017. Encryption Algorithm using New Modified map for digital image, *Journal of Physisc: Conference series, 893, IOP Publishing*. doi: 10.1088/1742-6596/893/1/ 012050.

SURYADI MT, YUDI SATRIA, MELVINA, VENNY, PRAWADIKA, LUQMAN N and ITA M SHOLIHAT., 2020. A new chaotic map development through the composition of the MS Map and the Dyadic Transformation Map, *Journal of Physics: Conference Series ICoMPAC*, 1490, 01202.

SURYADI MT, YUDI SATRIA, and PRAWADIKA, LUQMAN N., 2020. An improvement on the chaotic behavior of the Gauss Map for cryptography purposes using the Circle Map combination, *Journal of Physics: Conference Series ICoMPAC*, 1490, 012045.

SURYANTO, Y., SURYADI MT, and RAMLI, K., 2016. A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding, *Journal of Information Hiding and Multimedia Signal Processing*, 7**,** 697–713.

SURYANTO, Y., SURYADI MT, and RAMLI, K., 2017. A New Image Encryption using color scrambling based on chaotic permutation multiple circuler shrinking and Expanding, *Multimedia Tools and Applications*, 76, 16831–16854.

VAJARGAH, B. F., and ASGHARI, R., A., 2015. Pseudo Random Number Generator Based on Chaotic Henon Map (CHCG), *International Journal of Mechatronics, Electrical, and Computer Technology (IJMEC)*, 5 (15), 2120–2129.

WALIA, E., JAIN, P., and NAVDEEP., 2010. An Analysis of LSB & DCT based Steganography, *Global Journal of Computer Science and Technology (GJCST Computing Classification)*, 10, Issue 1.

YANUAR, M.R., MT, SURYADI, APRIONO, C., and SYAWALUDIN, M.F., 2024. Image-to-Image Steganography with Josephus Permutation and Least Significant Bit (LSB) 3-3-2 Embedding, *Applied Sciences*, 14, 7119, 1-21.

https://doi.org/10.3390/app14167119

ZHANG, W., WONG, K., YU, H., and ZHU, Z., 2013. An Image Encryption Scheme Using Reverse 2-dimensional Chaotic Map and Dependent Diffusion, *Journal of Communications in Nonlinear Science and Numerical Simulation*, 18, 2066–2080.

ZHOU, Y., LOU, B., and CHEN, C.L.P., 2014. A New 1D Chaotic System for Image Encryption, *Signal Processing*, 97, 172–182.

Halaman ini sengaja dikosongkan