Terbit *online* pada laman: http://jurnal.utu.ac.id/JTI

Jurnal Teknologi Informasi

| ISSN (Online): 2829-8934 |

Pengembalian Penyembunyian Data Dari Gambar Enkripsi Menggunakan Penyediaan Ruang Kapasitas Tambahan Sebelum di Enkripsi

Ryan Setiawan[1], Juniana Husna[2]
[1,2] Sistem Informasi, Universitas Abulyatama
Email: [1]ryan.stwn93@gmail.com, [2]nia.milig@gmail.com

INFORMASI ARTIKEL

Riwayat Artikel*:*
Diterima: 20 Oktober 2022
Revisi:-
Diterbitkan: 30 Oktober 2022

Kata Kunci*:*
RDH
Interpolasi
Histogram
Penyembunyian Data
Cover Images

ABSTRAK

Pengembalian data yang disembunyikan pada enkripsi images telah banyak digunakan dan menjamin kerahasiaan untuk medical imagery, military imagery, dan law forensics. Dan banyak kemajuan penelitian mengenai hal ini. Namun penyembunyian data menggunakan image juga memiliki keterbatasan terhadap kualitas dan kapasitas, dimana kedua hal ini selalu berbanding terbalik. Beberapa penelitian sebelumnya hanya terfocus pada salah satu keterbatasan tersebut. Maka dari itu pada penelitian kali ini, kami menggunakan metode reserving room untuk menyembunyikan data sebelum cover image dienkripsi. Metode yang diajukan ialah dengan menambahkan kapasitas sehingga mampu memenuhi permintaan penyembunyian data atau message untuk ukuran yang lebih besar. Sedangkan metode LSB-plane untuk pemilihan blok yang menerima untuk penyembunyian message data dan menggunakan tradisional teknik RDH untuk mengenkripsi dan dekripsi images sehingga cover image maksimal. Hasil eksperiment menunjukkan bahwa metode yang diajukan memberikan kualitas yang unggul untuk menjaga nilai PSNR proses embedding diatas 0.5 bpp sehingga aplikasi ini mampu menyembunyikan data yang lebih besar.

1. Pendahuluan

Reversible Data Hiding in Encryption Image (RDH-EI) merupakan salah satu teknik dari Reversible Data Hiding yang memanfaatkan enkripsi pada images cover untuk meningkatkan tingkat kerahasiaan untuk images cover dengan mengubahnya ke dalam sesuatu yang acak dan tidak dapat dimengerti [1], dengan menjamin pula bahwa message dari embedding berhasil diekstrak tanpa adanya error dan images cover berhasil direcovery seutuhnya tanpa adanya distorsi. Teknik ini juga biasa digunakan untuk medical imagery, military imagery, dan law forensics, dimana teknik ini menyajikan keamanan pada images cover dan informasi yang dapat dikembalikan secara utuh. Dan telah banyak research yang tertarik dengan pengembangan teknik RDH-EI sampai saat ini.

Banyak yang telah mempublikasikan metodenya menggunakan teknik RDH-EI seperti Hwang et al [7], dengan management scheme embedding data ke images cover yang akan dienkripsi dan software watermaking dimana data enkripsi dan coloring images menawarkan kemungkinan untuk membawa content yang penting dari privasi owner's dan data intergrity. Sehingga di lain pihak content yang penting ini akan dianggap notasi dari images enkripsi dan akan didekripsi dengan menggunakan cryptographic key maka image bisa direcovery.

Dari aspek lainnya RDH teknik hanya sebatas *recovery images cover* dan *message* secara utuh, namun untuk cara embedding message terdapat banyak cara lainnya seperti J. Tian [5] yang menggunakan difference expansion (DE) dengan membedakan dari pixel grup yang diperbesar dengan mengalikan 2 nilai tersebut dan teknik least significant bits (LSBs) untuk mengubah semua

nilai zero sehingga bisa dilakukan embedding message. Ada juga penilitian yang menggunakan *histogram shifting* (HS) [5], yang mana space yang dibuat untuk data embedding dengan shifting the bins dari histogram nilai gray images yang diaplikasikan pada teknik RDH.

X. Zhang et al. [3] juga memiliki frameworks for RDH-EI yaitu dengan "vacating room after encryption (VRAE). Di framework ini cover images dienkripsi dan space untuk hiding additional data itu dibuat ketika image telah dienkripsi. Sama seperti Ma et al. [8] dengan frameworks yang telah dipublikasikannya pada tahun 2013, namun pada framework ini yaitu menyajikan "reversible data hiding before encryption (RRBE)", dimana space yang digunakan untuk hiding data itu dibuat sebelum images dienkripsi. Dan images dienkripsi menggunakan sebuah enkripsi key yang akan di data-hider juga pada images location yang disediakan untuk data hiding key. Sejak lokasi additional data ini dilakukan sebelum images dienkripsi, maka framework ini dianggap lebih baik dari segi PSNR embedding data dari pada metode sebelumnya [3] dan data hiding bisa ditanamkan lebih dari 10 kali sebesar payloads [8], namun pada tahun 2014 metode framework RRBE ini dimodifikasi dengan menambahkan *active block exchange* (ABE) pada saat setelah melakukan interpolasi pada images sehingga nilai PSNR lebih tinggi 2dB dari metode sebelumnya.

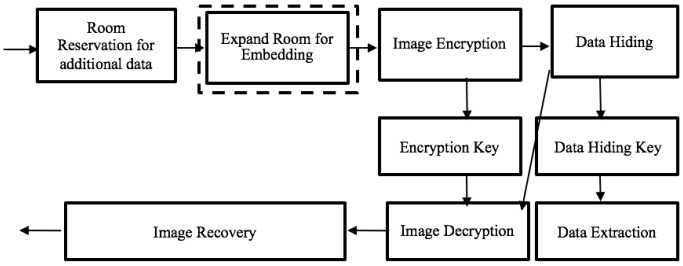
Namun seiring berjalannya waktu muncul permasalahan baru yaitu dalam hal data message semakin terus bertambah yang ingin disembunyikan ke dalam sebuah cover [6], maka dari itu pada paper ini proposed method, penulis mengacu pada RRBE framework [8] dengan meningkatkan kapasitas dari images pada saat dilakukannya interpolasi sebanyak 2 times dari metode sebelumnya, maka dari itu pada hasil yang diharapkan images mampu menampung message payload sebesar 15%.

Sebelumnya metode Reserving Room Before Encrypted diajukan oleh K. Ma dkk. [8] dengan melakukan interpolasi untuk menyediakan room pada image yang kemudian ditambahkan teknik histogram shifting untuk dapat melakukan embedding pada data hiding yang menerapkan RDH technique sehingga dapat dikatakan berhasil ketika images cover direcovery dan informasi data hasil extraksi dikembalikan. Metode RRBE ini juga dikerjakan pada proposed metode kali ini namun lebih berfocus pada peningkatan kapasitas embedding sehingga data yang akan dimasukkan ke dalam cover images jauh lebih besar dibandingkan sebelumnya karena image yang akan dilakukan embedding ialah images yang sudah dienkrip sehingga penulis tidak terlalu memikirkan kualitas dari image, walaupun pada akhirnya sebagai bentuk analisa akan dilakukan pengukuran nilai PSNR pada images cover dan images stegano.

Metode ABE yang diajukan oleh T. Mathew [9] hampir sama dengan metode sebelumnya [8] karena proposed [9] adalah teknik pengembangan dari RRBE dengan menambahkan Active Block Exchange (ABE) kedalam images cover yang diacukan sebagai kandidat dari data hiding, dengan menerapkan teknik LSB-planes dan image yang dihasilkan dienkrip menggunakan stream chipper, dan additional data disembunyikan ke dalam lokasi yang telah ditentukan menggukana data hiding key. Pada proposed method penulis menggunakan metodenya ketika melakukan interpolasi sehingga meningkatkan kapasitas beberapa blok pixel pada images cover namun tidak menambahkan teknik ABE sehingga teknik embedding lebih cepat dan tidak menambahkan kapasitas size Mb dari images cover dan hanya berfocus pada kapasitas embedding dimana dari hasil yang diharapkan nanti adalah size images cover tidak terlalu besar namun kapasitas data hiding dan nilai PSNR tetap terjaga.

2. Metodologi Penelitian

Karena permasalahan yang telah disebutkan sebelumnya, maka dari itu penulis ingin meningkatkan kapasitas dengan mengembangkan metode yang sudah ada sebelumnya RRBE [2]. Dari penambahan persamaan awal image partition dapat dilihat pada skema penjabaran Gambar 1. perkalian untuk menyediakan room sebelum dilakukan enkripsi pada images cover.



Gambar 1. Blok Diagram Metode yang Diajukan

Dengan menerapkan RDH teknik maka data ekstraksi dan image recovery berhasil kembali dengan sempurna seperti yang diterapkan metode sebelumnya pula, dengan menerapkan RDH algorima yang ideal maka tidak dipungkiri bahwa enkripsi key untuk dekrip image dan data hiding key untuk data ektraksi dapat mengembalikan data dengan sangat baik.

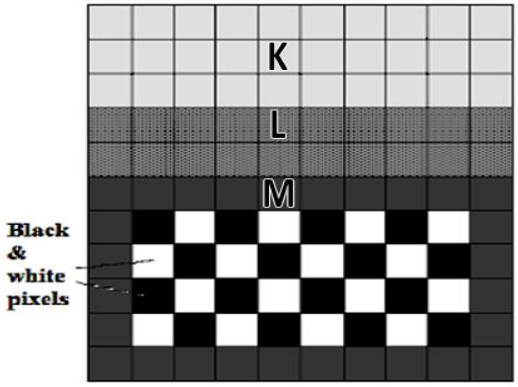
Untuk mengenerate *images* asli pertama kita bagi Image dengan menggunakan image partition menjadi 4 part A, B, C, D; dimana A adalah LSBs dari data boundary map untuk enkripsi key dan data hiding key, dan C adalah room dari metode sebelumnya [2] dan D adalah reserving room yang ditambahkan dari proposed method.

a. Partisi Image

Agar nilai pixel dari reserving room sebelum dienkipsi yang akan diberikan, maka nilai tersebut akan dikalkulasi dengan image pixel asli dari nilai B. untuk itu maka diberikan persamaan yang kita asumsikan C adalah original image 8 bits gray-scale dengan size M x N dari pixel $C_{i,j} \in [0, 255]$, $1 \leq i \leq M$, $1 \leq j \leq N$. dimana perhitungan akan mengambil bagian penting dari perhitungan blocks dari setiap rows.

$$f = \sum_{u=2}^{m} \sum_{v=2}^{N-1} \sum_{v=2}^{K-1} | \, C_{u,v} - \frac{C_{u-1,v} + C_{u+1,v} + C_{u,v-1} + C_{u,v+1}}{4} \tag{1}$$

Dan hasil perhitungan akan menambahkan untuk nilai pixel pada reserving room dari size A, N, K. dengan nilai B sebagai pembanding dari pixel asli sehingga nilai PSNR tidak jauh berbeda dan itu menjadi acuan khusus dari metode ini.



Gambar 2. Skema Image Partitioning dari metode yang diajukan

b. Penanaman Bolak-balik

Dari nilai pixel B yang tersisa ketika telah dilakukan reserving room ke nilai A, maka untuk embedding dibagi atas 2 pixel: white pixel dengan nilai *i* dan *j* yang dijelaskan ($i+j$) mod 2 = 0 dan black pixel ($i+j$) mod 2 = 1.

$$B'_{i,j} = \omega_1 B_{i-1,j} + \omega_2 B_{i+1,j} + \omega_3 B_{i,j-1} + \omega_4 B_{i,J+1} \tag{2}$$

Dengan menerapkan metode determined dari metode yang sama pada [4] maka digunakan the weight $\omega_i, 1 \leq i \leq 4$. Untuk mengestimasi nilai error yang dikalkulasi via $e_{i,j} = B_{i,j} - B'_{i,j}$ kemudian dilakukan embedding pada perhitungan estimasi tersebut dengan histogram shift yang akan dijelaskan nanti.

c. Enskripsi Image

Setelah ditentukan pixel yang ingin dilakukkan embedding pada image, sekarang kita tentukan konstruksi dari enkripsi image dengan mengubahnya menjadi stream cipher dari teknik RDH traditional, dimana range 0 to 255 dan dipresentasikan untuk 8 bits dengan mengikuti persamaan 3.

$$X_{i,j}(k) = \left[\frac{X_{i,j}}{2^k}\right] mod\ 2, \quad k = 0, 1, \ldots\ldots, 7. \tag{3}$$

$$E_{i,j}\ (k) = X_{i,j}\ (k)\ \oplus r_{i,j}\ (k) \tag{4}$$

d. Penyembunyian data di image enkripsi
Begitu data images cover sudah dienkripsi, maka selanjutnya dilakukan embedding payload ke dalam images dan proses embedding start dengan lokasi versi enkripsi dari A yang ditandai dengan A_E karena telah diatur ulang pada enkripsi E maka 10 bits informasi di LSB adalah 10 enkripsi pixel awal. Setelah diketahui berapa banyak bit-planes dan rows dari pixel maka data hider bisa dimodifikasi dengan menggunakan LSB replacement untuk mengganti bit-planes yang tersedia dengan additional data **m.** Untuk selanjutnya data hider sudah diset label dengan mengikuti nilai **m** sebagai process embedding, dimana data hiding key pada images juga dienkripsi dan dialokasikan sebagai **E`** jadi siapapun tidak dapat mendapatkan key untuk process hiding data sehingga tidak bisa mendapatkan extract additional data.

e. Data ekstraksi dan Pengembalian Image
Berdasarkan penjelasan dari RDH teknik, maka images cover dan data embedding harus kembali tanpa adanya error, maka pada process extraction terdapat 2 tahapan yaitu:
1) Ekstraksi Data: dengan process data hiding key $B'_{i,j}$ maka extract the additional data bisa diarahkan ke reserved location.
2) Dekripsi Image: dengan berdasarkan persamaan pada enkripsi maka bisa ditentukan cara mengembalikan nilai pixel images cover dengan dekrip nilai dari kebalikan enkripsi.

$$D_{i,j}\ (k) = X_{i,j}\ (k)\ \oplus r_{i,j}\ (k) \tag{5}$$

2. Hasil dan Pembahasan

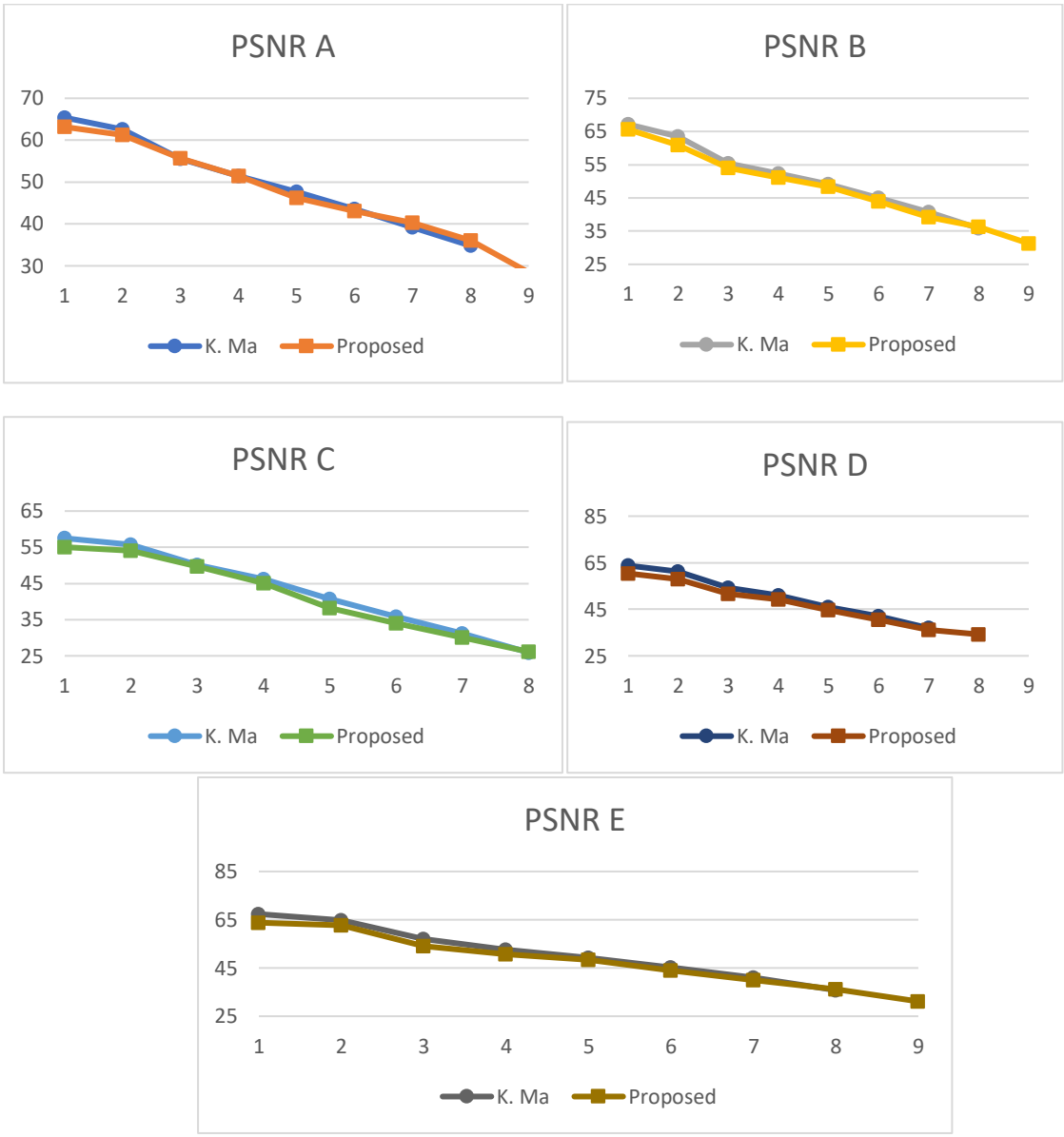
Model experiment dari metode yang diajukan ini diimplimentasikan pada matlab dengan menggunakan images cover barbara, lena, baboon, pappers, and football dengan size yang sama 512 x 512. Hasil penelitian adalah dengan membandingkan nilai PSNR metode dari [8] dengan menggunakan RRBE framework. Table 1 memperlihatkan perbandingan nilai tersebut dari hasil dekrip stego image yang bervariasi pada saat embedding yang diberikan dari bit-per-pixel (bpp). Hasil tersebut membandingkan satu LSB-plane dan double LSB-plane dari cara melakukkan proses embedding berdasarkan metode masing-masing. Dan dari nilai keseluruhan proses embedding dari PSNR, metode kami memiliki nilai yang rendah namun mampu menambah kapasitas dari proses embedding secara dua kali lipat dan menjaga nilai PSNR.

Dari LSB-Planes data yang disembunyikan dipilih berdasarkan angka yang sangat berpengaruh pada nilai PSNR untuk stego images proses, maka proses experiment kami dengan menggunakan beberapa images untuk databases, penambahan kapasitas dapat dilihat dari proses embedding bpp.

Tabel 1. Hasil Perbandingan SNR

Embedding rate		**0.05**	**0.01**	**0.05**	**0.1**	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**
barbara	**K. Ma**	65.39	62.56	55.56	51.46	47.68	43.56	39.24	34.8	
	Proposed	63.15	61.26	55.66	51.44	46.18	43.03	40.25	36.01	28.44
lena	**K. Ma**	67.16	63.44	55.46	52.33	49.07	45.01	40.65	35.84	
	proposed	65.61	60.94	53.99	51.09	48.32	43.87	39.22	36.24	31.28
baboon	**K. Ma**	57.49	55.71	50.19	46.17	40.68	35.87	31.16	25.92	
	Proposed	55.03	54.11	49.71	45.07	38.23	34.04	30.13	26.13	
peppers	**K. Ma**	63.77	61.3	54.17	51.02	46.01	42.08	36.91		

	Proposed	60.38	57.92	51.72	49.23	44.54	40.54	36.07	34.22
football	**K. Ma**	67.34	64.77	56.92	52.66	49.16	45.21	41.1	35.79
	Proposed	63.78	62.74	54.12	50.71	48.31	43.97	39.88	36.26	31.15



Gambar 4. hasil perbandingan dari nilai PSNR dari metode yang diajukan dan metode [8]. (a) Barbara, (b) Lena, (c) Baboon, (d) Peppers, (e) Football.

3. Kesimpulan

Dalam paper ini, penulis mengusulkan sebuah pendekatan baru untuk Reversible Data Hiding dalam gambar terenkripsi (RDH). yang bekerja dengan memesan blok yang paling sesuai dari berbagai bagian images cover untuk data hiding sebelum enskripsi. Metode yang diusulkan ini belum dapat menampakkan peningkatan kualitas dari metode sebelumnya [8]. Hal ini dapat dibuktikan dari hasil penelitian pada Tabel 1. Dimana cover images yang digunakan sama namun dengan metode enkripsi yang berbeda beda, sesuai dengan algoritma enkripsi yang dipelajari dari penelitian sebelumnya. Hasil baik dapat dilihat pada bagian *proposed method* bahwa kapasitas data yang mampu disisipkan kedalam images menggunakan algoritma yang telah dijelaskan pada algoritma persamaan 1 ~ 5 memiliki kapasitas yang lebih besar. Hal ini dikarenakan hanya berfokus pada peningkatan kapasitas dari sebuah data yang ingin disembunyikan dengan memanfaatkan kekuatan metode RDH tradisional untuk

menenkripsi image untuk dilakukan embedding dan menstabilkan PSNR pada kapasitas data yang besar. Dengan hasil ini, kami menekankan bahwa pendekatan menggunakan metode RDH tradisional di RDH-EI adalah arah yang kredibel.

Daftar Pustaka

[1] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 1996

[2] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Comput., vol. 14, no. 5, pp. 14–22, Sep./Oct. 2010.

[3] X. Zhang, "Separable reversible data hiding encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012

[4] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.

[5] Z. Ni, Y. Shi, N. Ansari, and S. Wei, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[6] S. Singh, A. K. Singh, S.P. Ghrera, "A recent survey on data hiding technique," IEEE conference on I-SMAC., pp. 882-892, 2017.

[7] L. Luo et al., "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187– 193, Mar. 2010.

[8] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.

[9] T. Mathew, M. Wilsey, "Reversible Data Hiding in Encrypted Images by Active Block Exchange and Room Reservation," IEEE Int. Conf. Contemporary Computing and Informatics (IC3I). 2014.

[10] L. Luoetal, "Reversible image watermarking using interpolation technique," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.