Paper

Teknik Penyembunyian Pesan Pada Citra Digital Menggunakan Metode Kombinasi RC4 Dan Steganografi LSB Berbasis VB

Author: Sarmi Ningsih, Siti Sundari, Khairunnisa

ISNN: 2964-1950

Teknik Penyembunyian Pesan Pada Citra Digital Menggunakan Metode Kombinasi RC4 Dan Steganografi LSB Berbasis VB

Sarmi Ningsih[1], Siti Sundari [2], Khairunnisa [3]
[1,2,3]Universitas Harapan Medan, Medan, Indonesia
[1]sarmie596@email.com, [2]sundaristth@email.com, [3]khairunnisajv2@email.com

Abstrak

Pesatnya perkembangan teknologi, membuat kebanyakan masyarakat mengikuti perkembangan yang ada. Perkembangan teknologi, menjadikan masyarakat mudah dalam mengakses berbagai macam hal, diantaranya pesan. Ada beberapa resiko yang dapat menghambat dalam pengiriman pesan jarak jauh , diantaranya kita tidak dapat mengetahui apakah pesan yang dikirim sampai ke orang yang kita tuju. Ada kemungkinan pesan yang kita kirim telah dibaca oleh orang yang tidak berkepentingan. Maka dari itu dibutuhkan pengamanan untuk suatu sistem agar pesan yang dikirim tidak mudah dicuri orang lain. Salah satu cara pengamanan suatu sistem dibutuhkan metode kombinasi kriptografi yaitu RC4 (*Rivest Code 4*) dan steganografi yaitu LSB (*Least Significant Bit*). Sistem yang dirancang digunakan untuk mengamankan informasi dari suatu pesan dengan cara melakukan enkripsi menggunakan algoritma RC4 yang kemudian disisipkan pada file citra dengan metode LSB. Sistem yang dirancang memiliki dua fungsi utama, yaitu fungsi enkripsi untuk melakukan penyandian pada pesan dan steganografi pada citra. Fungsi kedua adalah fungsi dekripsi yang bertujuan untuk ekstraksi pada citra sehingga pesan yang tersembunyi dapat dimengerti.
.
Kata Kunci: *Kriptografi, Steganografi, RC4, LSB*

Abstract

The rapid development of technology, makes most people follow the existing developments. Technological developments have made it easy for people to access various things, including messages. There are several risks that can hinder the sending of long-distance messages, including we cannot know whether the message sent reaches the person we are going to. It is possible that the messages we send have been read by unauthorized persons. Therefore, security is needed for a system so that messages sent are not easily stolen by others. One way to secure a system requires a combination of cryptographic methods, namely RC4 (Rivest Code 4) and steganography, namely LSB (Least Significant Bit). The system designed is used to secure information from a message by encrypting it using the RC4 algorithm which is then inserted into the image file using the LSB method. The system designed has two main functions, namely the encryption function for encoding messages and steganography on the image. The second function is the decryption function which aims to extract the image so that the hidden message can be understood.

Keywords: *Cryptography, Steganography, RC4, LSB*

1. PENDAHULUAN

Pesatnya perkembangan teknologi, membuat kebanyakan masyarakat mengikuti perkembangan yang ada. Perkembangan teknologi, menjadikan masyarakat mudah dalam mengakses berbagai macam hal, diantaranya pesan. Pesan merupakan salah satu proses komunikasi yang melibatkan teknologi di dalamnya. Oleh sebab itu ada beberapa hal yang perlu di perhatikan dalam pengiriman pesan salah satunya adalah aspek keamanan dalam pengiriman pesan. terlebih jika pesan tersebut bersifat penting dan rahasia. Ada beberapa resiko yang dapat menghambat dalam pengiriman pesan jarak jauh , diantaranya kita tidak dapat mengetahui apakah pesan yang dikirim sampai ke orang yang kita tuju. Ada kemungkinan pesan yang kita kirim telah dibaca oleh orang yang tidak berkepentingan. Maka dari itu dibutuhkan pengamanan untuk suatu sistem agar pesan yang dikirim tidak mudah dicuri orang lain. Salah satu cara pengamanan suatu sistem dibutuhkan metode kombinasi kriptografi yaitu RC4 (*Rivest Code 4*) dan steganografi yaitu LSB (*Least Significant Bit*).

Kriptografi adalah seni dan ilmu untuk melindungi pesan atau data dengan mengubah pesan asli menjadi pesan rahasia yang tidak dapat di pahami[1]. Steganografi merupakan seni dan ilmu tersembunyi pesan rahasia pada suatu media sehingga tidak seorang pun kecuali pengirim dan penerima mengetahui atau menyadari bahwa pesan rahasia itu ada[2]. Steganografi yang dibahas dalam penelitian ini adalah penyembunyian data di dalam citra digital saja. dengan demikian, penyembunyian data dapat juga dilakukan pada tempat berupa suara digital, teks, ataupun video[3]. *Least Significant Bit* (LSB) merupakan salah satu metode untuk menyembunyikan pesan pada media digital dengan cara menyisipkan pesan tersebut pada satu bit paling kanan ke obyek file *pixel*[4]. Algoritma RC4

ISNN: 2964-1950

(*Riverst Code 4*) merupakan *stream cipher* yang dirancang di RSA (Rivest Shamir Adleman) *Security* oleh Ron Rivest tahun 1987. Sifat kunci pada algoritma RC4 merupakan simetris serta melakukan proses enkripsi per digit atau *byte* per *byte* dengan operasi biner (biasanya XOR) dengan sebuah angka semiacak[5]. Citra warna atau Model warna RGB yaitu model warna aditif di mana merah, hijau dan biru ditambahkan bersama dalam berbagai cara untuk membuat beragam warna[6]. JPG adalah jenis data yang dikembangkan oleh *Joint Photographic Experts Assemble* (JPEG) yang dijadikan standar untuk para fotografer profesional. Seperti metode yang digunakan oleh format ZIP yang digunakan untuk menemukan pengulangan (*redundancy*) dalam data untuk kemudian dikompresi, JPG mengompresi data gambar dengan cara mengurangi bagian-bagian dari gambar untuk memblok pixel dalam gambar tersebut[7]. Salah satu sistem yang digunakan untuk mewakili gambar yaitu sistem warna RGB (*Red, Green, Blue*). Sistem RGB adalah sistem yang menggabungkan warna primer gabungan (*additive primary colours*) untuk memperoleh gabungan-gabungan warna. Berikut ini adalah tabel warna yang merupakan gabungan warna primer [8].*Unified Modeling Language (UML)* suatu proses tetapi pemodelan bahasa secara grafis untuk menspesifikasikan, memvisualisasikan, membangun, dan mendokumentasikan seluruh artifak sistem perangkat lunak[9]. *Microsoft Visual Basic.NET* merupakan sebuah alat untuk mengembangkan dan membangun aplikasi yang bergerak di atas sistem *NET Framework* dengan menggunakan bahasa BASIC[10].

Bedasarkan permasalahan di atas, penulis bermaksud untuk membuat aplikasi sebagai pengujian pada suatu pesan dengan mengkombinasikan dua metode untuk penyembunyian pesan pada suatu citra dengan proses enkripsi dan deskripsi, sehingga dapat memberi keamanan yang maksimal pada pesan. Maka penulis bermaksud mengangkat judul " Teknik Penyembunyian Pesan Pada Cita Digital Dengan Menggunakan Metode Kombinasi RC4 Dan Steganografi LSB Berbasis VB.

2. METODE PENELITIAN

Pada penelitian ini penulis menggunakan kombinasi metode RC4 dan steganografi LSB, Adapun tahapan – tahapan pada metode penelitian dapat dilihat pada gambar 1.

Gambar 1. Metode Penelitian

Penjelasan tahapan – tahapan metode penelitian :

1. Identifikasi masalah
   Merupakan tahapan awal sebelum memulai penelitian, melakukan identifikasi masalah pada masalah yang ada.
2. Analisa masalah
   Setelah menemukan masalah yang akan di bahas maka selanjutnya menganalisa masalah tersebut.dimana masalah yang di dapat akan di analisa untuk mendapatkan solusi dari permasalahan tersebut.
3. Analisa sistem
   tahapan selanjutnya merancang suatu sistem untuk mengamankan informasi dari suatu pesan dengan cara melakukan enkripsi menggunakan metode RC4 yang kemudian di sisipkan pada file citra dengan metode LSB.
4. Perancangan aplikasi
   Aplikasi yang di rancang memiliki tiga form utama, yaitu form awal, form enkripsi dan steganografi, form dekripsi dan eksraksi
5. Implementasi sistem

Selanjutnya mengimplementasi sistem pada suatu perangkat laptop yang digunakan untuk melakukan proses enkripsi,steganografi, dekripsi dan ekstraksi pada pesan.

6. Pengujian sistem
   Selanjutnya melakukan pengujian sistem dilakukan untuk melihat apakah sistem yang dibangun dapat melakukan enkripsi pesan, menyisipkan pesan tersebut kedalam citra, menyimpan citra steganografi,melakukan ekstraksi dan deskripsi pada pesan yang tersembunyi,sehingga penerima pesan dapat mengerti informasi yang tersembunyi didalam citra tersebut.
7. Kesimpulan
   Kesimpulan merupakan hasil dari pengujian sistem pada penelitian yabng di buat.

3. HASIL DAN PEMBAHASAN

Untuk melihat halit dari penelitian ini memerlukan beberapa tahapan proses untuk mencapai hasil perancangan aplikasi yang baik dan sesuai. Ada beberapa proses yang akan di jelaskan sebagai berikut :

3.1 Analisa Dan Perancangan Sistem

Sistem yang dirancang digunakan untuk mengamankan informasi dari suatu pesan dengan cara melakukan enkripsi menggunakan algoritma RC4 yang kemudian disisipkan pada file citra dengan metode LSB. Sistem yang dirancang memiliki dua fungsi utama, yaitu fungsi enkripsi untuk melakukan penyandian pada pesan dan steganografi pada citra. Fungsi kedua adalah fungsi dekripsi yang bertujuan untuk ekstraksi pada citra sehingga pesan yang tersembunyi dapat dimengerti. Sistem yang dibangun harus dimiliki oleh pengirim dan penerima pesan agar kedua pihak dapat saling mengerti isi pesan yang dirahasiakan. Sistem ini dapat dijalankan pada perangkat komputer.

3.2 Algoritma RC4

Tahapan-tahapan yang harus dilakukan agar pesan dapat terenkripsi dengan algoritma RC4 sebagai berikut:

1. Inisialisasi Larik

Tahapan awal adalah melakukan inisialisasi larik, larik yang digunakan memiliki 256 elemen. Larik dimulai dari 0 hingga 255.

2. Penentuan Kunci

Kunci yang digunakan adalah “SARMI”, kunci tersebut harus terlebih dahulu diubah kedalam nilai desimal sesuai dengan kode ASCII. Kunci “SARMI” akan berubah menjadi nilai “83 65 82 77 73”. Kunci ini memiliki panjang 5 *byte*, karena panjang kunci < 256 *byte*, maka dilakukan *padding* dengan cara mengulangi kunci sampai panjang kunci mencapai 256 *byte*.

Tabel 1. Nilai Kunci 256 *Byte*

83	65	82	77	73	83	65	82	77	73	83	65	82	77	73	83
65	82	77	73	83	65	82	77	73	83	65	82	77	73	83	65
82	77	73	83	65	82	77	73	83	65	82	77	73	83	65	82
77	73	83	65	82	77	73	83	65	82	77	73	83	65	82	77
73	83	65	82	77	73	83	65	82	77	73	83	65	82	77	73
83	65	82	77	73	83	65	82	77	73	83	65	82	77	73	83
65	82	77	73	83	65	82	77	73	83	65	82	77	73	83	65
82	77	73	83	65	82	77	73	83	65	82	77	73	83	65	82
77	73	83	65	82	77	73	83	65	82	77	73	83	65	82	77
73	83	65	82	77	73	83	65	82	77	73	83	65	82	77	73
83	65	82	77	73	83	65	82	77	73	83	65	82	77	73	83
65	82	77	73	83	65	82	77	73	83	65	82	77	73	83	65
82	77	73	83	65	82	77	73	83	65	82	77	73	83	65	82
77	73	83	65	82	77	73	83	65	82	77	73	83	65	82	77
73	83	65	82	77	73	83	65	82	77	73	83	65	82	77	73
83	65	82	77	73	83	65	82	77	73	83	65	82	77	73	83

3. Key Schedulling Algorithm (KSA)

Pada tahap ini dilakukan permutasi nilai-nilai pada larik *S-box* dengan bantuan kunci yang telah ditentukan. Adapun rumus untuk permutasi ini sebagai berikut:

i = 0, j = 0

ISNN: 2964-1950

j = (j + S[i] + K[i]) mod 256
Tukar nilai S[i] dengan S[j] (1)
Nilai i dan j selalu dimulai dari angka 0, i memiliki nilai dari 0 hingga 255, maka iterasi untuk KSA dilakukan sebanyak 256 kali. S[i] merupakan nilai larik ke-i, sedangkan K[i] merupakan nilai kunci ke-i. Hitungan manual KSA dengan kunci "SARMI" sebagai berikut:

1) Iterasi-1
   i = 0, j = 0
   j = (j + S[0] + K[0]) mod 256
   j = (0 + 0 + 83) mod 256 = 83
   Tukar nilai S[0] dengan S[83], maka S[0] = 83 dan S[83] = 0
2) Iterasi-2
   i = 1, j = 83
   j = (j + S[1] + K[1]) mod 256
   j = (83 + 1 + 65) mod 256 = 149
   Tukar nilai S[1] dengan S[149], maka S[1] = 149 dan S[149] = 1

Iterasi dilanjutkan hingga perulangan ke 256. Hasil lengkap KSA

Tabel 2. Nilai Larik S Hasil KSA

83	149	233	45	134	222	68	70	13	6	130	34	44	4	221	183
240	212	82	174	35	238	173	54	141	102	188	81	247	154	53	40
76	59	182	12	119	160	123	11	74	178	217	168	21	93	61	132
101	117	250	112	128	26	150	32	162	249	27	75	176	25	23	94
163	72	186	79	42	51	126	29	151	17	140	133	159	1	167	230
137	99	127	204	105	166	43	203	169	152	210	10	36	226	122	145
197	155	207	8	198	251	232	205	2	108	19	139	62	180	165	113
110	201	170	244	206	161	164	38	216	158	171	135	235	187	46	156
220	254	213	248	194	80	89	95	224	228	24	66	71	202	5	107
229	131	3	67	7	104	190	181	49	115	195	9	191	84	223	196
39	41	252	97	138	56	243	86	73	227	175	116	52	121	114	241
98	48	109	236	211	219	30	63	144	172	253	125	91	208	153	50
231	47	146	22	199	87	118	14	18	239	55	245	58	111	60	31
100	215	143	88	85	15	28	148	255	77	237	200	78	65	92	69
37	157	16	246	64	209	147	120	57	103	192	242	234	96	106	129
184	90	218	20	0	225	124	142	185	214	177	136	193	179	189	33

4. *Pseudo-Random Generation Algorithm* (PRGA) dan Enkripsi

Tahap PRGA merupakan tahapan pembangkitan aliran kunci, dimana rumus yang digunakan sebagai berikut:

i = 0, j = 0
i = (i + 1) mod 256
j = (j + S[i]) mod 256
Tukar Nilai S[i] dengan S[j]
t = (S[i] + S[j]) mod 256
K = S[t]
c = P $\oplus$ K (2)

Adapun proses enkripsi pesan "HARAPAN" sebagai berikut:

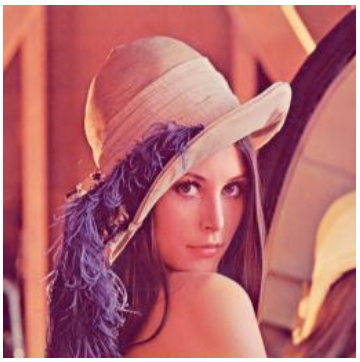
1) Enkripsi "H"
   i = 0, j = 0
   i = (0 + 1) mod 256 = 1
   j = (0 + S[1]) mod 256
   j = (0 + 149) mod 256 = 149
   Tukar nilai S[1] dengan S[149], maka S[1] = 104 dan S[149] = 149
   t = (S[1] + S[149]) mod 256
   t = (104 + 149) mod 256 = 253
   K = S[t] = S[253] = 179

ISNN: 2964-1950

Konversi nilai ASCII “H” = 72 dan nilai K = 179 ke bilangan biner, lalu lakukan enkripsi, c = P ⊕ K, maka hasilnya adalah 01001000 ⊕ 10110011 = 11111011 = 251. Pada ASCII, 251_{10} adalah karakter “û”. Proses enkripsi dilakukan hingga selesai.
Hasil akhir enkripsi dari pesan “HARAPAN” dengan kunci “SARMI” menggunakan algoritma rc4 adalah “ûw{ÉÅ±â”.

3.3 Proses Penyisipan Pesan Pada Citra

Pesan yang akan disembunyikan merupakan pesan yang telah dienkripsi menggunakan algoritma RC4. Pesan tersebut adalah “ûw{ÉÅ±â”. Pesan ini akan disisipkan ke dalam citra dengan metode LSB. Pada metode LSB setiap bit dari karakter pesan yang ada akan disisipkan kedalam citra dengan cara menggantikan nilai bit terakhir dari citra tersebut, baik pada kolom warna merah, hijau ataupun biru hingga setiap bit pada pesan tersebut dapat mengganti nilai bit terakhir pada citra sesuai dengan panjang pesan yang akan disisipkan.



Gambar 2. Citra Lena

Pesan yang akan disisipkan adalah “ûw{ÉÅ±â”, *byte* pertama adalah “û” dengan nilai desimal 251 atau dalam biner 11111011. Setiap bit pada karakter û akan disisipkan pada bit terakhir citra Lena, maka karakter û disisipkan hingga kanal warna *green* pada piksel (1, 3). Proses penyisipan karakter û atau bit 11111011 sebagai berikut.

1) Piksel (1, 1)
   R : 226 → 11100010, penyisipan → 11100011
   G : 138 → 10001010, penyisipan → 10001011
   B : 118 → 01110110, penyisipan → 01110111
2) Piksel (1, 2)
   R : 226 → 11100010, penyisipan → 11100011
   G : 138 → 10001010, penyisipan → 10001011
   B : 118 → 01110110, penyisipan → 01110110
3) Piksel (1, 3)
   R : 224 → 11100000, penyisipan → 11100011
   G : 136 → 10001010, penyisipan → 10001011

Setelah penyisipan karakter û, maka proses penyisipan karakter w atau bit 01110111 dimulai dengan cara penyisipan yang sama.

3.5 Implementasi Antarmuka

Aplikasi yang dibuat terdiri dari tiga *form*, yaitu *form* awal, *form* enkirpsi-steganografi dan *form* dekripsi-ekstraksi. *Form* awal berisi pilihan menu untuk menuju ke *form* enkirpsi-steganografi atau ke *form* dekripsi-ekstraksi.

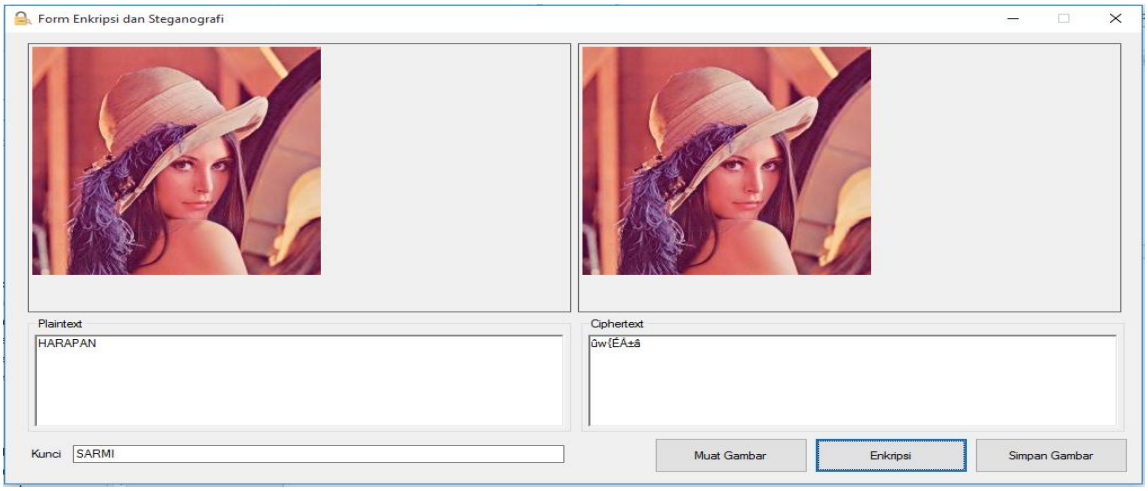
Gambar 3. Tampilan *Form* Awal

ISNN: 2964-1950

3.6 Pengujian Sistem

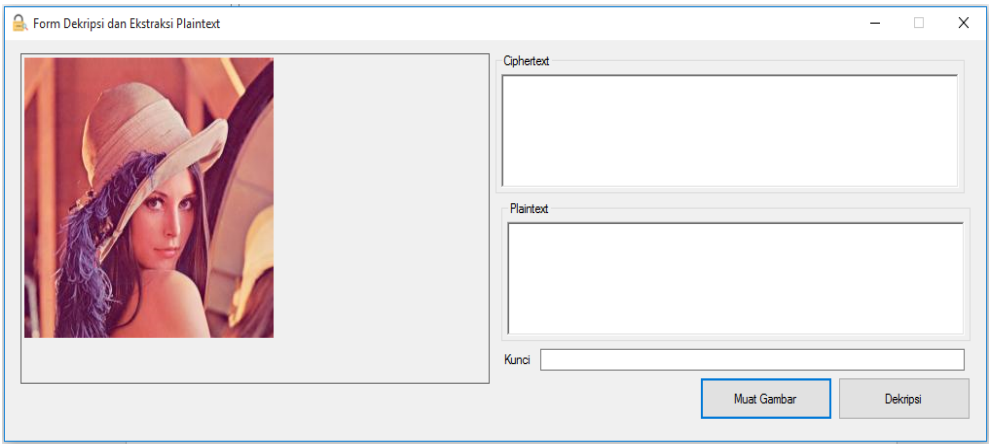
Pengujian sistem dilakukan untuk melihat apakah sistem yang dibangun dapat melakukan enkripsi pesan, menyisipkan pesan tersebut kedalam citra, menyimpan citra steganografi, melakukan ekstraksi dan dekripsi pada pesan yang tersembunyi, sehingga penerima pesan dapat mengerti informasi yang tersembunyi didalam citra tersebut.

Pesan yang akan dienkripsi dan disisipkan kedalam citra adalah "HARAPAN" dengan kunci "SARMI". Ketika tombol enkripsi ditekan, maka akan muncul pesan yang telah dienkripsi di kolom teks *ciphertext* dan citra steganografi pada sisi sebelah kanan atas dari aplikasi



Gambar 4. Tampilan Hasil Enkripsi dan Steganografi

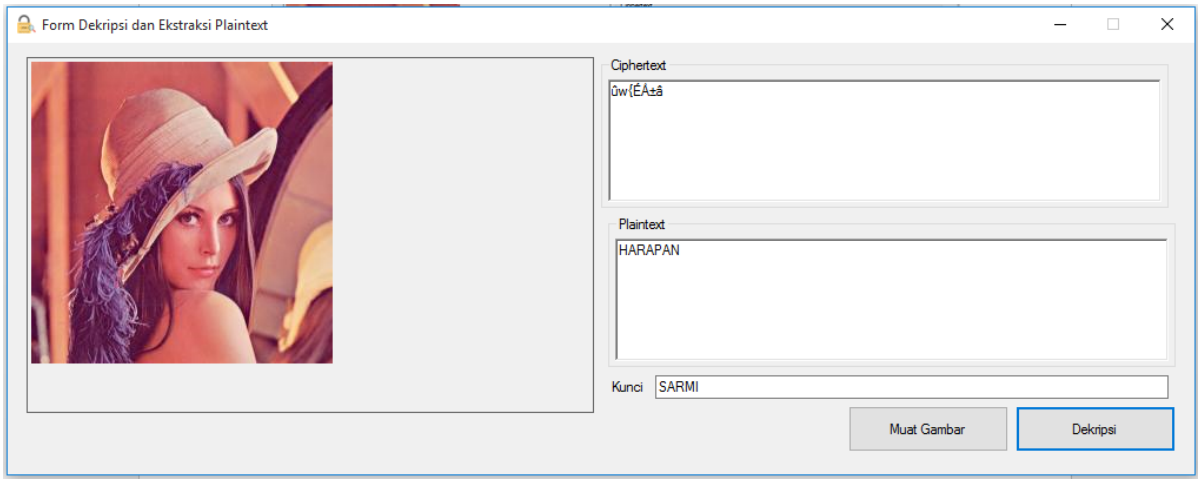
Pengujian selanjutnya adalah pengujian dekripsi dan ekstraksi pesan dari citra steganografi. Pengujian dilakukan dengan memilih menu dekripsi dan steganografi pada aplikasi. Citra yang dipilih bernama Lena Steganografi.jpg, citra ini akan dimuat pada kotak gambar *form* dekripsi dan ekstraksi yang terletak pada bagian kiri aplikasi. Ketika citra dimuat, maka tombol dekripsi menjadi berfungsi.



Gambar 5. Posisi Citra Pada *Form* Dekripsi dan Ekstraksi

Setelah melakukan pengisian kunci dekripsi yang benar dan menekan tombol dekripsi, maka proses ekstraksi dan dekripsi pesan yang terdapat didalam citra akan berlangsung. Hasil dari proses ini berupa *ciphertext* yang diekstraksi dari citra dan *plaintext* hasil dari dekripsi *ciphertext* tersebut.

ISNN: 2964-1950



Gambar 6. Tampilan Hasil Dekripsi dan Ekstraksi

Ciphertext yang berhasil diekstraksi dari citra yang dimuat adalah "ûw{ÉÅ±â", sesuai dengan hasil *ciphertext* yang didapatkan pada proses enkripsi.

3.7 Tabel Pengujian

Untuk melihat hasil pengujian citra dengan berbagai ukuran *file*, kunci, pesan, *Bit Depth* (BD), *Dots per* Inch (DPI) dan tipe warna seperti *Red, Green, Blue* (RGB) atau *Grayscale* (GS).

Tabel 3. Kondisi Awal Citra Sebelum Enkripsi dan Steganografi

Nama	Ukuran	Tipe	Piksel	BD/DPI	Plaintext	Kunci	Ciphertext
Lena	11,5 KB	RGB	256 x 256	24/96	HARAPAN	SARMI	ûw{ÉÅ±â
Nature	792 KB	RGB	1920 x 1080	32/72	Stegano	LSB	:ûÄCèòõ
Bird	1,62 MB	RGB	4498 x 2999	24/72	Stambuk	2018	Ec3š +Þ
Barbara	66,8 KB	GS	512 x 512	8/96	Image	rc4	+$»;<
Paprika	115 KB	GS	640 x 963	8/96	Unhar	Medan	ûUrºÃ

Tabel 4. Kondisi Citra Setelah Enkripsi dan Steganografi

Nama	Ukuran	Tipe	Piksel	BD/DPI	Plaintext	Kunci	Ciphertext
Lena	171 KB	RGB	256 x 256	32/96	HARAPAN	SARMI	ûw{ÉÅ±â
Nature	5,07 MB	RGB	1920 x 1080	32/96	stegano	LSB	:ûÄCèòõ
Bird	24,6 MB	RGB	4498 x 2999	32/96	Stambuk	2018	Ec3š +Þ
Barbara	334 KB	GS	512 x 512	32/96	Image	rc4	+$»;<
Paprika	774 KB	GS	640 x 963	32/96	Unhar	Medan	ûUrºÃ

4. KESIMPULAN

Setelah menyelesaikan perancangan aplikasi pengamanan data pada steganografi dengan menerapkan metode RC4 dan LSB, maka penelitian dapat menarik beberapa kesimpulan sebagai berikut:

1. Dengan dibuatnya aplikasi yang dapat mengkombinasikan metode RC4 dan LSB, sehingga dapat dilakukan pengiriman pesan dengan aman. Dimana pesan yang akan dikirim disembunyikan kedalam suatu citra.
2. Pesan yang akan di kirim di ubah kedalam bentuk pesan rahasia dengan menggunakan proses enkripsi dan deskripsi menggunakan metode RC4, dimana pesan yang yang dikirim di enkripsikan terlebih dahulu sehinggan menjadi pesan rahasia yang sulit dibaca, dan kemudian deskripsikan kembali untuk melihat pesan asli.
3. Algoritma *RC4* dan LSB dapat diterapkan kedalam penymbunyian pesan tanpa mengurangi kualitas gambar yang telah disisipkan pesan.

ISNN: 2964-1950

DAFTAR PUSTAKA

[1] Ayu, Devi Komala, and Jeffry H. Sinaulan. 2019. "**済無**No Title No Title No Title." 1:105–12.

[2] Azlansyah, Muhammad, and Budi Setiyono. 2019. "Penyisipan Pesan Pada Citra Digital Menggunakan Metode Least Significant Bit." *Jurnal Sains Dan Seni ITS* 8(1). doi: 10.12962/j23373520.v8i1.37658.

[3] Eko Setiawan, Agustinus, and Alfredo Pasaribu. 2020. "Penerapan Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit (LSB) Kombinasi RC4 Berbasis Mobile Android." *Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E)* 2(1):18–28. doi: 10.30604/jti.v2i1.27.

[4] Fadjeri, Akhmad, Arief Setyanto, and Mei P. Kurniawan. 2020. "Pengolahan Citra Digital Untuk Menghitung Ekstrasi Ciri Greenbean Kopi Robusta Dan Arabika (Studi Kasus: Kopi Temanggung)." *Jurnal Teknologi Informasi Dan Komunikasi (TIKomSiN)* 8(1):8–13. doi: 10.30646/tikomsin.v8i1.462.

[5] Fajar, Rizky, Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Petukangan Utara, and Kebayoran Lama. 2021. "APLIKASI KRIPTOGRAFI RC4 UNTUK PENGAMANAN EMAIL." 4(1):45–50.

[6] Ismail, Muh, Al Ghazali Syam, and Masnur Masnur. 2021. "APLIKASI QR CODE SEBAGAI SARANA PENYAMPAIAN INFORMASI POHON DIKEBUN RAYA JOMPIE Informasi Artikel." *Jurnal Sintaks Logika* 1(1):2775–412.

[7] Perbandingan, Analisis, Algoritma Rc, R. C. Ngg, D. A. N. Algoritma, and R. C. Gghn. 2018. *PENGAMANAN FILE CITRA TESIS*.

[8] Rachmawati, Yunianita, and Uce Indahyanti. 2020. *Buku Ajar Pemrograman Dasar Menggunakan Visual Basic Net 2013*.

[9] Sari, Jane Irma, Hengki Tamando Sihotang, and Teknik Informatika. 2017. "Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma Hill Cipher Dan Metode Least Significant Bit (LSB)." *Jurnal Mantik Penusa* 1(2):1–8.

[10] Siregar, Rananda Satia, Munjiat Setiani Asih, and Nur Wulan. 2019. "Penerapan Algoritma RC4 Dan Rail Fence Untuk Enkripsi Database Mahasiswa Pada Kampus POLTEKKES KEMENKES Medan." *Jitekh* 7(2):51–56.