JIKTEKS : Jurnal Ilmu Komputer dan Teknologi Informasi
Vol. 03, No. 02, April 2025, hlm. 70 - 78
ISSN : 2986-5417
DOI : doi.org/10.70404/jikteks.v3i02.178
Laman Jurnal: jurnal.faatuatua.com/index.php/JIKTEKS

Modifikasi Metode Chinese Remainder Theorem Menggunakan Blum Micali Generator Untuk Penyisipan Pesan Pada Citra Digital

Patima Lingga
Teknik Informatika, Universitas Budi Darma, Indonesia
e-mail: fatimalingga29@gmail.com

Keywords:

Steganography,
Modification,
Chinese Remainder Method,
Theorem,
Blum Micali-Generator
Algorithm.

ABSTRACT

Data security today is very important because information technology is currently developing very quickly. With so much information accessed on the internet, it makes it easier to use, such as text files. Digital images are very easy and are often misused by irresponsible people, such as personal photos. One of the techniques used in securing information is using steganography. In computer science, steganography is the art of hiding secret messages in messages or files, so that the existence of the secret message cannot be known by anyone. There are many methods used to utilize steganography, one of which is the Chinese Remainder Theorem method. Chinese Remainder Theorem is a technique of inserting a message that can only be seen by the sender and recipient so that no one can know or realize that there is a secret message in it. By including a randomization algorithm, it is thought to eliminate the possibility of an attacker guessing the results by knowing the algorithm used. The randomization algorithm that the author uses is the Blum Micali-Generator algorithm. The Blum Micali-Generator algorithm is useful for generating safe pseudo-random numbers. The aim of using the Blum Micali Generator algorithm is the process of determining the location of data insertion using the Chinese Remainder Theorem method based on a sequence of random values that are generated to determine the position of pixel points inserted to form a watermaking image.

Kata Kunci:

Steganografi,
Modifikasi,
Metode Chinese Remainder,
Theorem,
Blum Micali Generator.

ABSTRAK

Keamanan data pada saat sekarang ini merupakan hal yang sangat penting karena teknologi informasi pada saat ini berkembang sangat cepat. Dengan banyaknya informasi yang di akses di internet agar dapat memudahkan untuk digunakan seperti file teks. Citra digital sangat mudah dan banyak disalah gunakan oleh orang yang tidak bertanggung jawab seperti pada foto pribadi. Salah satu teknik yang digunakan dalam pengamanan informasi yaitu menggunakan steganografi. Dalam ilmu komputer steganografi merupakan seni dalam menyembunyikan pesan rahasia didalam pesan atau file, sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui oleh siapapun. Banyak metode yang digunakan untuk memanfaatkan steganografi, salah satunya yaitu metode Chinese Remainder Theorem. Chinese Remainder Theorem merupakan teknik menyisipkan pesan yang hanya dapat dilihat oleh sipengirim dan sipenerima sehingga tidak ada seorangpun yang dapat mengetahui atau menyadari bahwa ada sebuah pesan rahasia didalamnya. Dengan cara memasukkan algoritma pengacakan, dianggap bisa menghilangkan kemungkinan penyerang menebak hasil dengan mengetahui algoritma yang digunakan. Adapun algoritma pengacakan yang penenulis gunakan yaitu algoritma Blum Micali-Generator. Algoritma Blum Micali-Generator berguna untuk menghasilkan bilangan acak semu yang aman. Tujuan dalam menggunakan algoritma Blum Micali Generator adalah proses untuk menentukan lokasi penyisipan data metode Chinese Remainder Theorem berdasarkan urutan nilai acak yang dibangkitkan dalam menentukan posisi titik pixel yang disisipkan untuk membentukk watermaking citra.

Korespondensi Penulis *):

Patima Lingga
Universitas Budi Darma
Jalan Sisingamangaraja No. 338 Kota Medan, Indonesia.

Diajukan: 03-04-2025 | Diterima: 18-04-2025 | Diterbitkan: 30-04-2025

1. PENDAHULUAN

Keamanan data pada saat sekarang ini merupakan hal yang sangat penting karena teknologi informasi pada saat ini berkembang sangat cepat. Berbagai jenis informasi seperti teks, gambar, dan video yang dikonversikan menjadi media digital yang kemungkinan untuk diperbanyak atau pun dikirimkan melalui berbagai media seperti internet.

Dengan banyaknya informasi yang di akses di internet agar dapat memudahkan untuk digunakan seperti file teks. Citra digital sangat mudah dan banyak disalah gunakan oleh orang yang tidak bertanggung jawab seperti pada foto pribadi. Salah satu teknik yang digunakan dalam pengamanan informasi yaitu menggunakan steganografi. Dalam ilmu komputer steganografi merupakan seni dalam menyembunyikan pesan rahasia didalam pesan atau file, sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui oleh siapapun. Banyak metode yang digunakan untuk memanfaatkan steganografi, salah satunya yaitu metode Chinese Remainder Theorem. Chinese Remainder Theorem merupakan teknik menyisipkan pesan yang hanya dapat dilihat oleh sipengirim dan sipenerima sehingga tidak ada seorangpun yang dapat mengetahui atau menyadari bahwa ada sebuah pesan rahasia didalamnya. Pesan rahasia yang disembunyikan akan disisipkan pada suatu media penampung seperti pada citra gambar.

Metode Chinese Remainder Theorem dapat melakukan proses deteksi perubahan citra dan dapat mengembalikan citra yang sudah diubah kembali seperti semula. Metode ini cukup populer digunakan sebagai proses embedding watermark sehingga hal tersebut mudah untuk di ekstraksi berdasarkan pola teks yang disisipkan pada metode yang sudah banyak digunakan oleh penggunaan steganografi.

Namun, pada metode Chinese Remainder Theorem juga diperlukan sebuah cara agar tidak mudah terpecahkan salah satunya dengan cara memberikan kerumitan pada titik data yang disisipkan didalam citra digital dengan memanfaatkan algoritma pengacakan. Dengan cara memasukkan algoritma pengacakan, dianggap bisa menghilangkan kemungkinan penyerang menebak hasil dengan mengetahui algoritma yang digunakan. Adapun algoritma pengacakan yang penenulis gunakan yaitu algoritma Blum Micali-Generator. Algoritma Blum Micali-Generator berguna untuk menghasilkan bilangan acak semu yang aman. Tujuan dalam menggunakan algoritma Blum Micali Generator adalah proses untuk menentukan lokasi penyisipan data metode Chinese Remainder Theorem berdasarkan urutan nilai acak yang dibangkitkan dalam menentukan posisi titik pixel yang disisipkan untuk membentukk watermaking citra.

Berdasarkan pada penelitian sebelumnya yang dilakukan oleh Nur Laila pada tahun 2022 yang berjudul "Kombinasi Metode Pixel Value Differencing dan Metode Chinese Remainder Theorem dalam penyembunyian pesan pada citra" yang menyatakan bahwa sistem kombinasi metode Pixel Value Differencing dan metode Chinese Remainder Theorem dalam penyembunyian pesan pada citra dapat diimplementasikan dapat menjaga kerahasiaan data, serta mengintegrasikan data sehingga orang-orang yang berwenang saja yang dapat mengakses data tersebut[1].

Penelitian selanjutnya yang dilakukan oleh Josferi Pardosi pada tahun 2021 yang berjudul "Penyembunyian Pesan Pada File Audio Menerapkan Metode Chinese Remainder Theorem" yang menyatakan penyembunyian pesan dapat dilakukan dengan metode Chinese Remainder Theorem, dengan cara mengkonversi bilangan yang besar dari pesan dengan panjang eksponensiasi modular berukuran besar menjadi pesan yang lebih pendek dengan eksponensiasi modular berukuran relatif kecil[2].

Penelitian selanjutnya yang dilakukan oleh Soeb Aripin Dan Muhammad Syahrizal pada tahun 2022 yang berjudul "Analisis Modifikasi Algoritma Kriptografi Klasik Menggunakn Algoritma Blum-Micali Generator" yang menyatakan algoritma Blum-Micali Generator dapat dilakukan karena plainteks yang di enkripsi dapat di deskripsikan kembali. Hasil dari pengujian nampak terlihat jelas memiliki tingkat perbedaan dari hasil enkripsi[3].

Penelitian selanjutnya yang dilakukan oleh Darma Eka Putra Manulang pada tahun 2022 yang berjudul "Implementasi Metode Chinese Reminder Theorem Untuk Menyisipkan Citra Digital Kedalam File Video" menyatakan metode Chinese Reminder Theorem untuk proses penyisipan citra digital ke dalam file video dimana teknik untuk menyisipkan pesan rahasia dan metode Chinese Reminder Theorem untuk proses penyisispan citra digital ke dalam wadah penampung yaitu file video[4].

Penelitian selanjutnya yang dilakukan oleh Chaiarun Nisa Lubis pada tahun 2022 yang berjudul "Analisis Modifikasi Pembangkitan Kunci Rivest Code 2 Dengan Metode Blum-Micali Generator Untuk Meningkatkan Nilai Confusion Terhadap Record Data Login Pada Database" menyatakan pembangkit kunci Blum Micali Generator mempunyai tahap pembangkitan kunci dan proses yang sangat cepat karena menggunakan perhitungan yang sederhana[5]..

2. METODE PENELITIAN

2.1 Kerangka Kerja Penelitian

Kerangka kerja merupakan langkah langkah yang akan diambil dalam menyelesaikan masalah yang akan dibahas. Adanya pun kerangka kerja yang digunakan dalam penelitian ini dapat dilihat pada gambar berikut.

Gambar 1. Kerangka Kerja Penelitian

2.2 Steganografi

Steganografi merupakan ilmu dan seni menyembunyikan pesan rahasia dan sulit untuk diketahui dan menjadikan pesan tersebut tidak dapat terbaca orang lain kecuali pengirim dan penerima pesan tersebut[6]. Kata steganografi (steganography) berasal dari steganos, yang artinya tersembunyi atau terselubung, dan graphia yang berarti menulis, steganografi juga digunakan untuk meyembunyikan data rahasia ketika enkripsi tidak dapat dilakukan atau secara bersamaan dengan enkripsi. Steganografi membutuhkan dua wadah penampung dan data rahasia yang akan disembunyikan, steganografi digital menggunakan media digital sebagai wadah misalnya, citra, audio, teks, dan video. Data rahasia tersembunyi juga dapat berupa citra, audio, teks, atau video[7].

2.3 Chinese Remainder Theorem

Chinese Remainder Theorem adalah konsep yang didasarkan pada hubungan kongruensi. Namun, tidak seperti kongruensi pada umumnya, konsep ini didasarkan pada hubungan kongruensi simultan. Kongruensi simultan adalah beberapa hubungan kongruensi yang memiliki hubungan satu sama lain, dan hubungan ini terkait dengan nilai variabel yang sama tetapi dengan modulo yang berbeda. Teori ini merupakan teori kuno yang sering digunakan dalam penerapan kriptografi *Chinese Remainder Theorem* dapat mengkonversi sejumlah besar kunci dengan eksponensiasi modular besar ke kunci yang lebih pendek dengan eksponensiasi modular yang relatif lebih kecil[8]. Didalam teori bilangan, dasar dari algoritma CRT adalah kemampuannya untuk merekonstruksi bilangan bulat dengan rentang nilai tertentu dari sisa hasil bilangan–bilangan koprima.

Proses penyisipan pesan:

1. Menentukan lokasi piksel X, ubah nilai piksel biner 8-bit [0 255]
2. Ambil 2-MSB X, lalu mengubahnya ke nilai desimal [0 64, 128, 192] sebagai nilai Y.
3. Ambil 6-LSB dari X, lalu mengubah kenilai deksimal [0 63] sebagai nilai Z.
4. Menentukan nilai bilangan koprima M_1 dan M_2 (nilai yang diusulkan oleh petra et al adalah 6 dan dan 11).
5. Hitung: R_1= Z mod 6 dan R_2=Z 11.
6. Memodifikasi nilai Z dengan cara berikut:
7. Piksel stego X' = Z' + Y
8. Ulang langkah 1 – 7 sehingga seluruh pesan disisipkan ke dalam citra.

Rumus dari *MetodeChinese Reminder Theorem* (CRT)

$X_1 = 2_j(mod\ gcd(M_i M_j)$ ..... (1)

2.4 Blum Micali Generator

Konsep Algoritma *Blum Micali Generator* adalah algoritma yang menghasilkan urutan angka yang independen secara statistik dan tidak dapat menebak dengan susah payah untuk menghitung logaritma diskrit, yang didasarkan pada keyakinan bahwa modular modulo eksponensiasi adalah fungsi prima dan satu arah tujuan dalam menggunakan algoritma *Blum Micali Generator* adalah proses enkripsi yang dilakukan pengacakan yang sehingga hasil enskripsi yang didapatkan lebih sulit ditebak sehingga menyulitkan. kriptoanalis untuk membaca pesan atau informasi. Dengan demikian ukuran tingkat keamanan menjadi lebih tinggi dari sandi monoalfabet karena tidak dapat dideteksi dengan analisis frekuensi terjadinya huruf, dan juga lebih aman daripada *vigenere cipher* karena ukuran kata kunci lebih sulit[3].

$X_{i+1} = aX_i\ mod\ m, i \geq 0$ ..... (2)

Output dari generator adalah 1 jike Xi < m/2, selain itu menghasilkan 0

2.5 Citra Digital

Citra digital adalah gambar dua dimensi yang dihasilkan dari analog dua dimensi kontinu menjadi gambar melalui proses pengambilan sampel. Gambar analog dibagi menjadi baris N dan kolom M sehingga menjadi gambar deskrit. Gambar digital merupakan gambar yang dapat diproses oleh komputer, semua yang disimpan oleh komputer adalah angka yang menujukkan besarnya intensitas pada piksel individual. Karena berbentuk data numerik[9]

2.6 Pesan Teks

Pesan teks adalah layanan yang memungkinkan pengguna ponsel untuk mengirim pesan pendek untuk ponsel lain dengan cepat dan dengan biaya kecil. Pesan singkat yang ini juga akan dikirim jauh lebih cepat daripada mengrim pesan suara karena pesan teks hanya terdiri dari karakter teks dan angka[10].

3. HASIL DAN ANALISIS

3.1 Anlisa Masalah

Proses analisa yang dilakukan berdasarkan pada metodelogi yang digunakan. Dalam penelitian ini, digunakan metode kualitatif dalam melakukan perancangan perangkat lunak. Berikut dirincikan tahapan-tahapan kerja yang digunakan.

Steganografi citra atau gambar merupakan suatu konsep untuk menyisipkan suatu pesan teks ke dalam citra sehingga informasi data tersebut tersembunyi dan hanya pihak yang berhak yang dapat mengekstraksi keluar informasi tersebut. Dalam proses kerja steganografi citra atau gambar, terdapat dua buah proses *encoding* dan prose *decoding*. Dalam penelitian ini, data yang di ambil berupa sampel data citra digital dengan menggunakan foto asli dan berupa pesan teks yang akan disembunyikan. Berikut ini gambar sampel data yang akan digunakan dalam penelitian ini. Pesan Teks berupa password: "**ling**"

Gambar 1. Sampel Data

3.2 Modifikasi Metode

Modisikasi metode *Chinese Remender Theorem* (CRT) dilakukan menggunakan algoritma Blum-Micali Generator yang berguna untuk menghasilkan bilangan acak semu yang aman dan dianggap dapat menghilangkan kemungkinan penyerangan menebak hasil dengan mengetahui algoritmanya. Proses yang dilakukan untuk memodifikasi algoritma *Chinese Remender Theorem* (CRT) adalah sebagai berikut:

1. Input pesan yang akan disisipkan.
   Adapun pesan yang digunakan sebagai sampel data penerapan metode CRT pada penelitian adalah "**ling"**
2. Inputkan citra yang akan disisipkan pesan.
   Adapun citra yang digunakan sebagai sampel data pada penelitian ini dengan format JPG yaitu:

Gambar 2. Grayscale

Adapun nilai piksel yang dijadikan sampel data yaitu resolusi 10x10 piksel berdasarkan gambar grayscale sampel data citra yaitu:

	1	2	3	4	5	6	7	8	9	10
1	232	233	234	234	233	232	230	229	231	231
2	231	231	232	233	233	232	231	230	231	232
3	229	230	231	232	233	233	232	232	232	232
4	229	230	231	232	232	232	232	232	233	233
5	231	231	231	232	232	232	231	231	233	233
6	233	233	232	232	232	232	231	231	233	233
7	233	233	233	233	232	232	232	233	232	233
8	233	233	233	233	233	233	233	234	232	232
9	231	231	231	231	231	232	233	234	233	232
10	232	232	231	231	232	233	233	234	233	232

Gambar 3. Nilai Pixel Citra Digital 10x10

3. Ubah pesan yang telah terenskripsi menjadi ASCII.

Tabel 1. Nilai ASCII Sampel Data

No	Pesan	Nilai HexDesimal	Nilai Biner
1	l	6C	0110 1100
2	i	69	0110 1001
3	n	6E	0110 1110
4	g	67	0110 0111
		Total	32

4. Pilih lokasi piksel dari citra dengan menggunakan *metode Blum-Micali Generator*.
Adapun penerapan dari algoritma *blum-micali generator* dalam menentukan lokasi piksel berdasarkan jumlah pesan sebanyak 32bit berdasakan 4 titik yang metode *Chinese Remainder Theorem* sebagai berikut

$X_1 = 3, \quad M = 100, \quad a = 1$

$X_1 = 1 * 3 \; mod \; 100$
$= 3$
$X_{2+1} = 3 * 3 \; mod \; 100$
$= 9 \; mod \; 100$
$= 9$
$X_{3+1} = 9 * 3 \; mod \; 100$
$= 27 \; mod \; 100$
$= 27$
$X_{4+1} = 27 \; mod \; 100$
$= 81 \; mod \; 100$
$= 81$

Maka didapatkan titik piksel dibagi menjadi 4 lokasi awal memasukkan pesan yaitu: 3, 9, 27,81

Tabel 2. Pembagian Pesan Berdasarkan Lokasi

No	Pesan	Nilai *HexDesimal*	Nilai Biner	Lokasi Star Piksil Awal
1	l	6C	0110 1100	3= 011011
2	i	69	0110 1001	9=00 01101001
3	n	6E	0110 1110	27=01101110
4	g	67	0110 0111	81=01100111

5. Lakukan Metode CRT dengan cara subtansikan nilai bit kode ASCII pesan sebagai nilai piksel diakhir citra.

Tabel 3. Nilai Piksel 10x10

X	1	2	3	4	5	6	7	8	9	10
1	232	233	234	234	233	232	230	229	231	231
2	231	231	232	233	233	232	231	230	231	232
3	229	230	231	233	233	233	232	232	232	232
4	229	230	231	232	232	232	232	232	233	233
5	231	231	231	232	232	232	231	231	233	233
6	233	233	232	232	232	232	231	231	233	233
7	233	233	233	233	232	232	232	233	232	233
8	233	233	233	233	233	233	233	234	232	2322
9	231	231	231	231	231	232	233	234	233	232
10	232	232	231	231	232	233	233	234	233	232

Proses selajutnya menerapkan metode *Chinese Remainder Theorem* sebagai berikut:
Keterangan pada titik star 3:

Iterasi 1 menyisipkan pesan biner ke '0'

1. Menentukan nilai lokasi piksel X)
   X = 234 = 11101010
2. Mencari nilai Y = 2-MSB dari X)
   Ambil 2 digit biner X dari sebelah kiri dan hitung nilai 2^n dari MSB
   Maka sisa bit lainnya menjadi 0

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	0	1	0	1	0
1	1	0	0	0	0	0	0
128	64	0	0	0	0	0	0

   Y = 11000000 = 192
   Y = 192
3. Mencari nilai Z = 6 CRT dari X)
   Ambil 6 digit biner X dari sebelah kanan dan hitung nilai 2^n dari CRT

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	0	1	0	1	0
		32	0	8	0	2	0

   Z = 101010 = 42
   Z = 42
4. Ambil bilangan komprima M_1= 6 dan M_2= 11
5. R_1 = Z mod 6 dan R_2 = Z mod 11
   R_1 = 42 mod 6 R_2 = 42 mod 11
   R_1 = 0 R_2 = 9
6. Memodifikasi nilai Z

J	Z'	R_1	R_2	R_1 > R_2
0	42	0	9	YA

7. X_1+Z'+Y+42+192 = 234

Iterasi 2 menyisipkan pesan biner ke '1'

1. Menentukan nilai lokasi piksel X)
   X = 234 = 11101010
2. Mencari nilai Y = 2-MSB dari X)
   Ambil 2digit biner X dari sebelah kiri dan hitung nilai 2^n dari MSB
   Maka sisa bit lainnya menjadi 0

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	0	1	0	1	0
1	1	0	0	0	0	0	0
128	64	0	0	0	0	0	0

   Y = 11000000 = 192
   Y = 192
3. Mencari nilai Z = 6 CRT dari X)
   Ambil 6digit biner X dari sebelah kanan dan hitung nilai 2^n dari CRT

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	1	1	0	1	0	1	0
		32	0	8	0	2	0

   Z = 101010 = 42
   Z = 42
4. Ambil bilangan komprima M_1= 6 dan M_2= 11
5. R_1 = Z mod 6 dan R_2 = Z mod 11
   R_1 = 42 mod 6 R_2 = 42 mod 11
   R_1 = 0 R_2 = 9
6. Memodifikasi nilai Z

J	Z'	R_1	R_2	R_1 > R_2
0	41	5	8	YA

7. X_1+Z'+Y+41+192 = 233

3.3 Proses Ekstraksi Pesan

Ektrasi pesan adalah proses pengambilan pesan yang telah di sispkan pada citra digital. Adapun proses yang diakukan pada ekstrasi pesan dalam modifikasi metode *Chinese Remender Theorem* menggunakan algoritma *Blum-Micali Generator* sebagai berikut:

1.$X_{1.3}$ = 234 = 11101010 maka ambil 1bit terakhir pada piksel =0
2.$X_{1.4}$ = 234 = 11101011 maka ambil 1bit terakhir pada piksel =1
3.$X_{1.5}$ = 233 = 11101001 maka ambil 1bit terakhir pada piksel =1
4.$X_{1.6}$ = 232 = 11101000 maka ambil 1bit terakhir pada piksel =0
5.$X_{1.7}$ = 230 = 11100111 maka ambil 1bit terakhir pada piksel =1
6.$X_{1.8}$ = 229 = 11101001 maka ambil 1bit terakhir pada piksel =1
7.$X_{1.9}$ = 231 = 11100110 maka ambil 1bit terakhir pada piksel =0
8.$X_{1.10}$ = 231 = 11100110 maka ambil 1bit terakhir pada piksel =0
9.$X_{2.1}$ = 231 = 11100110 maka ambil 1bit terakhir pada piksel =0
10.$X_{2.2}$ = 232 = 11100111 maka ambil 1bit terakhir pada piksel =1
11.$X_{2.3}$=232=11101001 maka ambil 1bit terakhir pada piksel =1
12.$X_{2.4}$=232=11101000maka ambil 1bit terakhir pada piksel =0
13.$X_{2.5}$=233=11101001 maka ambil 1bit terakhir pada piksel =1
14.$X_{2.6}$=232=11101000 maka ambil 1bit terakhir pada piksel =0
15.$X_{2.7}$=231=11100110 maka ambil 1bit terakhir pada piksel =0
16.$X_{2.8}$=230=11100101 maka ambil 1bit terakhir pada piksel =1
17.$X_{2.9}$=231=11100110 maka ambil 1bit terakhir pada piksel =0
18.$X_{2.10}$=232=11101001 maka ambil 1bit terakhir pada piksel =1
19.$X_{3.1}$=229=11100101 maka ambil 1bit terakhir pada piksel =1
20.$X_{3.2}$=230=11100110 maka ambil 1bit terakhir pada piksel =0
21.$X_{3.3}$=231=11100111 maka ambil 1bit terakhir pada piksel =1
22.$X_{3.4}$=233=11101001 maka ambil 1bit terakhir pada piksel =1
23.$X_{3.5}$=233=11101001 maka ambil 1bit terakhir pada piksel =1
24.$X_{3.6}$=233=11101000 maka ambil 1bit terakhir pada piksel =0
25.$X_{3.7}$=232=11101000 maka ambil 1bit terakhir pada piksel =0
26.$X_{3.8}$=232= 11101001 maka ambil 1bit terakhir pada piksel =1
27.$X_{3.9}$=232=11101001 maka ambil 1bit terakhir pada piksel =1
28.$X_{3.10}$=232=11101000 maka ambil 1bit terakhir pada piksel =0
29.$X_{4.1}$=184=11101000 maka ambil 1bit terakhir pada piksel =0
30.$X_{4.2}$=189=11100111 maka ambil 1bit terakhir pada piksel =1
31.$X_{4.3}$=169=11100111 maka ambil 1bit terakhir pada piksel =1
32.$X_{4.4}$=167=11101001 maka ambil 1bit terakhir pada piksel =1

Maka hasil bit sebanyak 8 bit dari nilai bit yang diambil 01101100 01101001 01101110 01100111

Tabel 4. Hasil Ekstraksi Pesan

No.	Nilai biner	Pesan
1	01101100	l
2	01101001	i
3	01101110	n
4	01100111	g

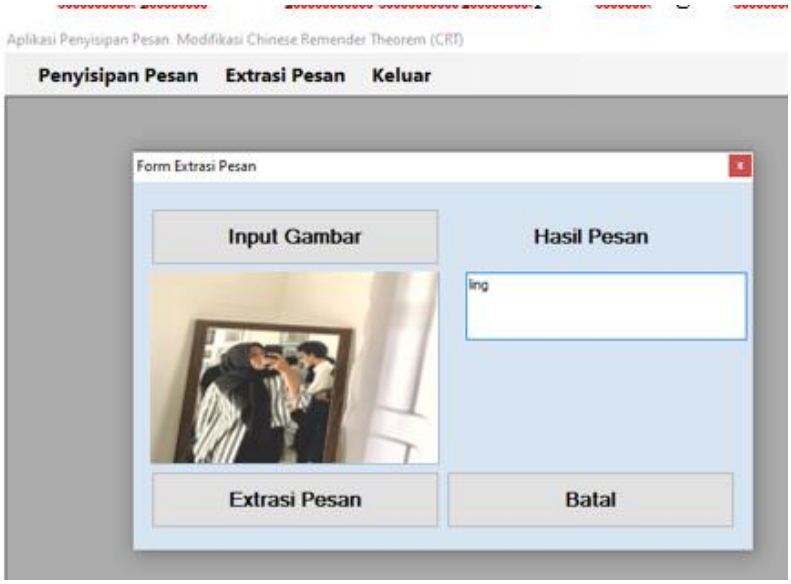
3.4 Implementasi

Aplikasi modifikasi metode Chinese Remender Theorem (CRT) menggunakan Blum micali Generator untuk penyisipan pesan pada citra digital yang telah dirancang merupakan aplikasi berbasis .netframework 3.5 yang dibuat menggunakan Visual Basic.Net 2008. Aplikasi modifikasi metode Chinese Remender Theorem (CRT) menggunakan Blum micali Generator untuk penyisipan pesan pada citra digital ini dapat dijalankan pada sistem operasi windows yang mendukung .netframework 3.5.

1) *Form* Penyisipan Pesan

Gambar 4. *Form* Penyisipan Pesan

2) Form Ekstraksi Pesan



Gambar 5. *Form Alternatif*

Dengan menggunakan aplikasi modifikasi metode Chinese Remender Theorem (CRT) menggunakan Blum Micali Generator untuk penyisipan pesan pada citra digital. Hasil dari pengujian aplikasi aplikasi modifikasi metode Least Significant Bit (CRT) menggunakan Blum Micali Generator untuk penyisipan pesan pada citra digital dilihat pada gambar 5. Diatas

4. KESIMPULAN

Dari hasil penulisan dan analisa bab-bab sebelumnya, maka dapat diambil kesimpulan, dimana kesimpulan-kesimpulan tersebut kiranya dapat berguna bagi para pembaca, sehingaa penulisan skripsi ini dapat lebih bermanfaat, Adapun kesimpulan-kesimpulan tersebut adalah sebagai berikut :

1. Prosedur yang dilakuakan pada modifikasi metode Least Significant Bit (CRT) menggunakan Blum micali Generator untuk penyisipan pesan pada citra digital dapat dilakukan dengan baik dimana algoritma Blum micali Generator digunakan untuk menentukan lokasi penyisipan data pada citra dengan metode CRT berdasarkan urutan nilai acak yang dibangkitkan dalam menentukan posisi titik pixel yang disisipkan untuk membentukk penyisipan pesan pada citra citra.
2. Blum micali Generator dapat digunakan pada metode CRT dimana pesan dapat disisipkan pada citra dan dapat pula informasi di dalam citra di extrasi untuk mendapatkan informasi pesan yang telah disisipkan dan pada citra hasil stegano-citra memiliki kulias yang hapir sama dengan citra asli secara kasat mata. Namu penerapan Blum micali Generator memiliki kelemahan dimana memiliki batas titik yang ditentukan dikarenakn algoritma Blum

micali Generator memiliki nilai yang sama pada hasil pengacakanyya

3. Aplikasi modifikasi metode Least Significant Bit (CRT) menggunakan Blum micali Generator untuk penyisipan pesan pada citra digital telah selesai dirancang dengan menggunakan Microsof Visual Studio 2008 dan dapat dijalankan pada sistem operasi windows yang mendukung

REFERENSI

[1] N. Laila, "Informasi dan Teknologi Ilmiah (INTI)," vol. 9, no. 2, pp. 41–44, 2022, [Online]. Available: http://stmik-budidarma.ac.id/ejurnal/index.php/inti/article/view/3824/2548

[2] I. M. Simbolon and M. Sianturi, "Penyembunyian Pesan Pada File Audio Menerapkan Metode Pixel Value Differencing," *Inf. dan …*, vol. 8, no. 2, pp. 57–59, 2021.

[3] S. Aripin and M. Syahrizal, "Analisis Modifikasi Algoritma Kriptografi Klasik Menggunakan Algoritma Blum-Micali Generator," *J. Sains Komput. Inform. (J-SAKTI*, vol. 6, no. 1, pp. 136–147, 2022.

[4] D. E. P. Manullang, "Penyisipan Pesan Ke Dalam File Video Menerapkan Metode Chinese Remainder Theorem," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 3, no. 1, pp. 108–117, 2019, doi: 10.30865/komik.v3i1.1576.

[5] C. N. Lubis, "Analisis Modifikasi Pembangkitan Kunci Rivest Code 2 Dengan Metode Belum-Micali Generator (BM-G) Untuk Meningkatkan Nilai Confusion Terhadap Record Data Login Pada Database," vol. 3, no. 2, pp. 73–82, 2022, doi: 10.47065/josyc.v3i2.953.

[6] R. Andri, R. K. Hondro, and K. Tampubolon, "Implementasi Metode Pixel Value Differencing Untuk Penyembunyian Pesan Pada Citra Digital," *KOMIK (Konferensi Nas. Teknol. Inf. dan Komputer)*, vol. 3, no. 1, pp. 355–361, 2019, doi: 10.30865/komik.v3i1.1613.

[7] D. Andika and D. Darwis, "Modifikasi Algoritma Gifshuffle Untuk Peningkatan Kualitas Citra Pada Steganografi," *J. Ilm. Infrastruktur Teknol. Inf.*, vol. 1, no. 2, pp. 19–23, 2021, doi: 10.33365/jiiti.v1i2.614.

[8] F. P. Johari, D. Murni, and H. Syarifuddin, "Modifikasi Algoritma Kriptografi RSA Multiprima Menggunakan Chinese Remainder Theorem dan Garner ' s Algorithm," *UNP J. Math.*, vol. 2, no. 2, pp. 36–41, 2019, [Online]. Available: http://ejournal.unp.ac.id/students/index.php/mat/article/view/6311

[9] N. Z. Munantri, H. Sofyan, and M. Y. Florestiyanto, "Aplikasi Pengolahan Citra Digital Untuk Identifikasi Umur Pohon," *Telematika*, vol. 16, no. 2, p. 97, 2020, doi: 10.31315/telematika.v16i2.3183.

[10] Y. Bin Pairin, "Kode Autentikasi Hash pada Pesan Teks Berbasis Android," *Eksplora Inform.*, vol. 8, no. 1, p. 6, 2018, doi: 10.30864/eksplora.v8i1.129.

[11] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, "Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang," *Appl. Inf. Syst. Manag.*, vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[12] C. O. Purba, "Implementasi Metode Chinese Remainder Theorem Untuk Menyisipkan Citra Digital Kedalam File Video," vol. 1, no. 3, pp. 67–72, 2022.

[13] C. Ulandari, "Penyisipan Pesan Pada File Dokumen Berekstensi Xls/Xlsx Menggunakan Metode Chinese Remainder," *KLIK Kaji. Ilm. Inform. dan Komput.*, vol. 2, no. 5, pp. 156–162, 2022, doi: 10.30865/klik.v2i5.365.

[14] D. Iqbal, A. R. Panggabean, I. W. Sinaga, and ..., "Implementasi Algoritma RC4+ Untuk Mengamankan Pesan Teks Pada Aplikasi Chatting," *... Teknol. Komput. …*, pp. 916–920, 2019, [Online]. Available: http://seminar-id.com/prosiding/index.php/sainteks/article/view/254

[15] A. Z. F. Rangkuti and H. Fahmi, "Implementasi Kriptografi Untuk Keamanan File Text Dengan Menggunakan Metode MD5," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 3, no. 2, pp. 170–175, 2020, doi: 10.32672/jnkti.v3i2.2384.