BIOSTech: Bulletin of Computer Science and Information Technology
Vol 1, No 2, Juni 2023
Hal: 72-86
Available Online at https://journal.grahamitra.id/index.php/biostech

Penyembunyian Data Teks Terenkripsi One Time Pad Pada Citra Digital Dengan Menggunakan Metode Redundant Pattern Encoding

Katini Gulo

Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: tinigulo12@gmail.com
Email Penulis Korespondensi: tinigulo12@gmail.com

Abstrak−Untuk dapat mengamankan data yang maksimal maka diperlukan suatu metode dalam teknik kriptografi dengan kombinasi teknik steganografi. Algoritma kriptografi yang dapat digunakan untuk mengamankan data adalah one time pad (OTP). Algoritma ini bekerja dengan mengkombinasikan setiap karakter plaintext dengan karakter key (dalam hal ini panjang key dan plaintext haruslah sama) sehingga menghasilkan bentuk yang tidak dimengerti (ciphertext). Salah satu metode steganografi yang dapat digunakan yaitu redundant pattern encoding (RPE). Metode ini bekerja dengan cara menyisipkan data yang akan disembunyikan kedalam citra, kemudian mengekstraknya untuk melihat kembali data tersebut. Hasil dari penelitian yang dilakukan penulis, dengan menerapkan teknik kriptografi dan mengkombinasikannya dengan teknik steganografi, didapatkan sebuah sistem kemananan data yang dapat mengamankan data secara maksimal.

Kata Kunci: Kriptografi; Steganografi; One Time Pad; Redundant Pattern Encoding

Abstract−To be able to secure maximum data, we need a method in cryptographic techniques with a combination of steganography techniques. The cryptographic algorithm that can be used to secure data is one time pad (OTP). This algorithm works by combining each plaintext character with a key character (in this case the length of the key and plaintext must be the same) so as to produce an incomprehensible form (ciphertext). One of the steganographic methods that can be used is redundant pattern encoding (RPE). This method works by inserting the data to be hidden into the image, then extracting it to view the data again. The results of the research conducted by the author, by applying cryptographic techniques and combining them with steganography techniques, obtained a data security system that can secure data optimally.

Keywords: Cryptography; Steganography; One Time Pad; Redundant Pattern Encoding

1. PENDAHULUAN

Seiring dengan kemajuan teknologi di era digital saat ini, banyak tersedia berbagai macam teknik untuk dapat mengamankan data teks yang bersifat penting dan dirahasiakan dari orang yang tidak berhak mengakses data tersebut. Data teks perlu diamankan untuk mencegah atau melindungi dari tindakan yang dapat merugikan, seperti pencurian maupun penyadapan. Salah satu data teks yang perlu diamankan dalam hal ini adalah kata sandi (password) akun email.

Teknik yang dapat digunakan untuk mengamankan data teks adalah dengan menerapkan teknik keamanan data kriptografi. Kriptografi dapat mengamankan data teks dengan cara mengubah data teks ke dalam bentuk yang sulit untuk dimengerti. Berdasarkan penelitian sebelumnya, mengatakan bahwa kriptografi dapat mengatasi masalah keamanan data dengan menggunakan kunci, dalam ini algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaanya [1].

Salah satu algoritma kriptografi yang dapat digunakan untuk mengamankan data teks adalah dengan menerapkan algoritma one time pad (OTP). Algoritma ini bekerja dengan mengkombinasikan masing-masing karakter pada plaintext dengan satu karakter pada kunci (key), oleh karena itu panjang kunci harus sama dengan panjang plaintext. Enkripsi dapat dinyatakan sebagai penjumlahan modulo 256 (menggunakan kode ASCII 8 bit) dari satu karakter plaintext dengan satu karakter kunci OTP. Berdasarkan penelitian sebelumnya, mengatakan bahwa kelebihan algoritma OTP ini adalah sangat sederhana, namun sangat aman karena kunci hanya digunakan satu kali [2].

Tidak semua algoritma kriptografi memiliki keamanan yang optimal dan masih banyaknya ditemukan data-data yang masih bisa dipecahkan oleh penyerang. Berdasarkan penelitian sebelumnya, bahwa algoritma kriptografi klasik masih bisa dipecahkan oleh penyerang, karena umumnya menggunakan karakter berupa huruf dengan berbagai pengkombinasian [3]. Beberapa algoritma kriptografi klasik yang dapat dipecahkan oleh penyerang, salah satunya adalah algoritma caesar chiper yang dapat dipecahkan dengan cara brute force attack dan menggunakan exhaustive key search.

Adapun teknik mengamankan data selain kriptografi yaitu dengan menggunakan teknik steganografi. Steganografi merupakan teknik menyembunyikan atau menyisipkan data ke dalam suatu media. Steganografi dapat mengamankan data dengan menyembunyikannya ke dalam media lain misalnya citra digital, video, audio tanpa mengubah bentuknya, sehingga orang lain tidak akan mengetahui keberadaan data rahasia tersebut. Berdasarkan penelitian sebelumnya, mengatakan bahwa salah satu keuntungan steganografi dibandingkan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian, sehingga media penampungnya tidak menimbulkan kecurigaan bagi pihak ketiga [4].

Salah satu metode steganografi yang dapat digunakan yaitu redundant pattern encoding (RPE). Metode ini bekerja dengan cara menyisipkan data yang akan disembunyikan kedalam citra, kemudian mengekstraknya untuk melihat kembali data tersebut. Berdasarkan penelitian sebelumnya, mengatakan bahwa kelebihan metode redundant pattern encoding ini adalah mampu bertahan dari cropping dan kompresi pada saat diproses.

Berdasarkan uraian permasalahan di atas, maka pada penelitian ini dilakukan pengkombinasian antara teknik kriptografi dengan teknik steganografi agar keamanan data rahasia lebih optimal. Algoritma OTP digunakan sebagai algoritma untuk melakukan enkripsi dan dekripsi data teks, sedangkan metode redundant pattern encoding digunakan

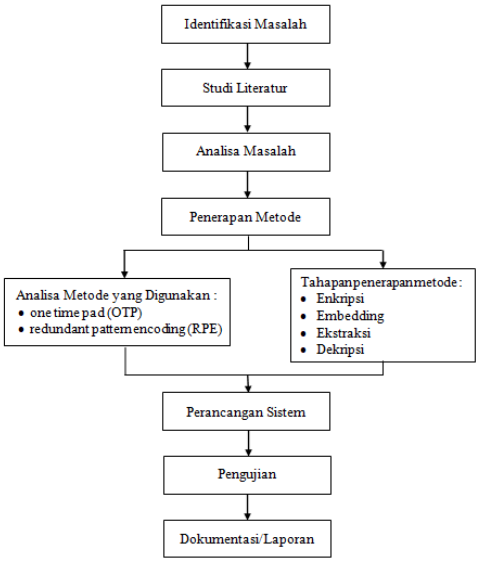
BIOSTech: Bulletin of Computer Science and Information Technology
Vol 1, No 2, Juni 2023
Hal: 72-86
Available Online at https://journal.grahamitra.id/index.php/biostech

sebagai metode dalam menyembunyikan data teks yang telah terenkripsi. Media yang digunakan sebagai penyembunyi dalam hal ini adalah citra digital.

2. METODOLOGI PENELITIAN

2.1 Kerangka Kerja Penelitian

Untuk membantu penyusunan dalam penelitian ini, maka diperlukan adanya susunan kerangka kerja (framework) yang jelas tahapan-tahapannya. Kerangka kerja ini merupakan langkah-langkah yang akan dilakukan dalam penyelesaian masalah yang akan dibahas. Adapun kerangka kerja penelitian yang digunakan seperti terlihat pada gambar



Gambar 1. Kerangka Kerja Penelitian

2.2 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan sebuah pesan dengan cara menyandikannya ke dalam bentuk yang tidak bisa dimengerti lagi maknanya. Teknik pengamanan data dengan kriptografi memiliki dua proses, yaitu dengan melakukan enkripsi dan dekripsi. Proses enkripsi dan dekripsi ini, dikenal istilah plaintext (data yang akan disandikan) dan ciphertext (teks sandi). Enkripsi adalah proses penyandian data, sedangkan dekripsi adalah kebalikannya, yaitu proses membaca data yang sudah dienkripsi.

2.3 Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan dengan suatu cara sehingga selain sender dan receiver, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia [4]. Salah satu kegunaan steganografi yaitu, untuk menyamarkan posisi keberadaan data-data rahasia sehingga menyulitkan untuk dideteksi. Berbeda dengan data yang diamankan dengan teknik kriptografi yang masih bisa tersedia meskipun sudah diamanakan, data-data pada steganografi bisa disembunyikan tanpa diketahui oleh pihak ketiga. Data yang disembunyikan pada teknik steganografi, dapat diekstraksi kembali sama seperti aslinya. Kelebihan dari steganografi dibandingkan dengan kriptografi adalah bahwa pesan yang dikirim tidak menarik perhatian, sehingga media penampung yang membawa pesan tidak menimbulkan kecurigaan pihak ketiga.

2.4 One Time Pad (OTP)

Metode ini merupakan metode yang relatif mudah untuk dipelajari dan dinyatakan sebagai “perfect encryption algorithm” oleh para ahli kriptografi. Sistem cipher pada metode ini tidak bisa dipecahkan karena barisan kunci acak yang ditambahkan ke pesan plaintext yang tidak acak menghasilkan ciphertext yang seluruhnya acak. Prinsip enkripsi pada algoritma ini adalah dengan mengkombinasikan masing-masing karakter pada plaintext dengan satu karakter pada kunci. Panjang kunci harus sama dengan panjang plaintext, sehingga tidak memungkinkan pengulangan penggunaan kunci selama proses enkripsi.

Proses enkripsi pada OTP membutuhkan barisan bilangan acak sebagai kunci. Enkripsi pada OTP merupakan proses mengubah plaintext menjadi chipertext. Sedangkan dekripsi merupakan kebalikan dari enkripsi yaitu proses mengubah chipertext menjadi plaintext. Adapun langkah-langkah dalam proses enkripsi dan dekripsi OTP adalah sebagai berikut

1. Menyiapkan plaintext dan key untuk dienkripsi (panjang plaintext dan key harus sama, begitupun sebaliknya).
2. Mengubah plaintext menjadi angka sesuai kode ASCII.

3. Mengubah key menjadi angka sesuai kode ASCII.
4. Melakukan enkripsi dengan ketentuan rumus enkripsi OTP yaitu :

$$Ci = (Pi + Ki) \bmod 26 \quad (1)$$

Keterangan rumus :
a. Ci = Ciphertext
b. Pi = Plaintext
c. Ki = Key (kunci)

5. Setelah proses enkripsi berhasil maka akan didapatkan kode dari ciphertext.
6. Proses enkripsi selesai.

Langkah-langkah proses dekripsi :
1. Menyiapkan ciphertext dan key yang didapat dari proses enkripsi.
2. Mengubah ciphertext menjadi angka sesuai kode ASCII.
3. Mengubah key menjadi angka sesuai kode ASCII.
4. Melakukan enkripsi dengan ketentuan rumus enkripsi OTP yaitu :

$$Pi = (Ci - Ki) \bmod 26 \quad (2)$$

Keterangan rumus :
a. Ci = Ciphertext
b. Pi = Plaintext
c. Ki = Key (kunci)

5. Setelah proses dekripsi berhasil maka akan didapatkan kode dari plaintext.
6. Proses dekripsi selesai.

2.5 Metode Redundant Pattern Encoding (RPE)

Metode ini merupakan salah satu metode penyisipan pesan pada teknik steganografi. RPE biasanya menggunakan media gambar sebagai cover dari pesan yang akan disembunyikan. Kelebihan metode ini, yaitu tahan terhadap cropping dan kompresi pada saat pemrosesan file gambar. Sementara kekurangan dari metode ini, yaitu ukuran file yang disisipkan terbatas [9]. Metode redundant pattern encoding ini hanya dilakukan pada tempat terbatas, maka kapasitas pesan yang disisipkan menjadi terbatas. Adapun cara untuk mengatasi keterbatasan tersebut yaitu dengan cara :
1. Menggunakan banyak file yang memiliki hubungan tertentu, seperti album foto.
2. Menggunakan file yang memiliki banyak noise, sehingga meningkatkan kapasitas pesan.
3. Mengkombinasikan dua cara yang sudah disebutkan sebelumnya, yaitu menggunakan banyak file dan menggunakan file yang memiliki banyak noise.

Adapun langkah-langkah penyisipan pada metode redundant pattern encoding adalah dengan menggambarkan pesan kecil pada kebanyakan gambar. Algoritma dari redundant pattern encoding yaitu memasukkan redundansi (penggandaan) ke dalam pesan yang akan disembunyikan dan kemudian menyebarkan pesan itu pada keseluruhan gambar. Sebuah generator yang bekerja secara pseudorandom (suatu algoritma untuk menghasilkan urutan angka yang mendekati sifat nomor acak) digunakan untuk menyeleksi dua area dari gambar patch A dan patch B (patch adalah metoda yang menandai area gambar). Intensitas pada pixel di suatu patch dinaikkan dengan nilai yang konstan, sementara patch lainnya diturunkan dengan nilai konstan yang sama. Perubahan pada bagian patch akan mengenkripsi tiap satu bit dan perubahan biasanya sangat kecil dan halus [10].

Sementara untuk langkah-langkah ektraksi berdasarkan metode redundant pattern encoding yaitu dengan mengekstrak bit-bit tersebut dan menggabungkan bit-bit tersebut menjadi sebuah pesan aktual [10].

3. HASIL DAN PEMBAHASAN

3.1 Analisa Penerapan Metode

Analisa merupakan proses memilah-milah suatu permasalahan menjadi elemen-elemen yang lebih kecil untuk dipelajari guna mempermudah menyelesaikan permasalahan yang ada. Pada tahap analisa diperlukan suatu pendekatan analisa guna menghindari kesalahan-kesalahan yang mungkin muncul pada tahap berikutnya, yaitu perancangan sistem. Tahap ini merupakan tahapan yang sangat penting, pendekatan yang dilakukan adalah mendefinisikan masalah pada sistem yang sedang berjalan dan sekaligus melakukan evaluasi setiap cara kerja sistem yang sedang berjalan berdasarkan prosedur-prosedur yang ada.

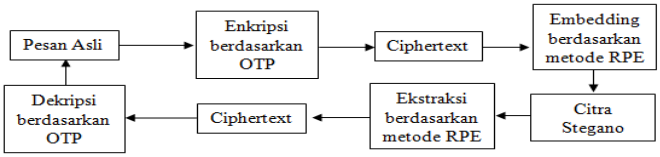
Permasalahan keamanan data teks yang sering bermunculan seperti pencurian data, penyadapan data, dan pengubahan data oleh pihak yang tidak bertanggungjawab. Sehingga setiap orang memerlukan sebuah sistem yang dapat mengamankan pesan rahasia dan penting agar data tersebut hanya bisa diakses oleh orang tertentu saja. Berdasarkan hasil analisa yang dilakukan oleh peneliti, maka solusi yang diperlukan adalah teknik kriptografi menggunakan algoritma one time pad, kemudian mengkombinasikannya dengan teknik steganografi menggunakan metode redundant pattern encoding, agar memberikan keamanan yang maksimal.

BIOSTech: Bulletin of Computer Science and Information Technology
Vol 1, No 2, Juni 2023
Hal: 72-86
Available Online at https://journal.grahamitra.id/index.php/biostech

3.1.1 Penerapan Metode

Data teks yang digunakan sebagai objek yang akan diamankan dalam penelitian ini adalah password sebuah akun email penulis. Pengamanan data teks tersebut dengan menerapkan teknik kriptografi menggunakan algoritma one time pad. Cara kerja dari algoritma one time pad itu sendiri adalah dengan mengenkripsi pesan ke dalam bentuk yang tidak dimengerti dan mendekripsikannya untuk mengembalikan pesan ke dalam bentuk aslinya. Penelitian ini menerapkan algoritma one time pad untuk mengenkripsi pesan rahasia dengan menyiapkan pesan yang akan diamankan (plaintext) dan kunci (key), dalam hal ini panjang dari plaintext dan key haruslah sama, kemudian mengubah keduanya menjadi angka sesuai kode ASCII. Hasil dari proses enkripsi maka akan mengubah pesan rahasia menjadi bentuk yang tidak dimengerti (ciphertext).

Untuk memberikan keamanan yang maksimal, maka ciphertext yang didapatkan dari hasil enkrispi menggunakan algoritma one time pad, membutuhkan pengkombinasian dengan teknik steganografi menggunakan metode redundant pattern encoding. Cara kerja dari metode redundant pattern encoding itu sendiri adalah dengan menyembunyikan pesan ke dalam citra digital dan mengekstraksinya untuk melihat kembali pesan aslinya. Penelitian ini menerapkan metode redundant pattern encoding untuk menyembunyikan pesan rahasia yang telah terenkripsi OTP, dengan memasukkan redundansi (penggandaan) ke dalam pesan kemudian menyebarkannya pada seluruh gambar. Berikut ini adalah skema penerapan kedua metode dalam mengamankan data penting.



Gambar 2. Skema proses kombinasi OTP dengan RPE

Proses pengkombinasian dimulai dari pesan asli dalam hal ini bersifat rahasia yang akan diamankan dengan algoritma OTP. Algoritma OTP melakukan pengamanan dengan mengenkripsi pesan asli, sehingga berubah bentuk menjadi ciphertext. Ciphertext yang didapatkan dari hasil enkripsi, disembunyikan (embedding) berdasarkan metode RPE, sehingga menghasilkan citrastegano. Proses selanjutnya yaitu ekstraksi berdasarkan metode RPE untuk mengambil kembali ciphertext. Terakhir yaitu proses dekripsi berdasarkan algoritma OTP untuk mengubah ciphertext kembali menjadi pesan aslinya.

Penyelesaian yang akan dilakukan dengan mengenkripsi pesan yang sehingga didapatkan ciphertext, kemudian menyembunyikannya ke dalam citra digital, lalu mengekstraksinya untuk mengembalikan ciphertetxt yang telah tersembunyi di dalam citra digital, dan terakhir mendekripsikannya untuk mengembalikan ciphertext yang di dapat dari dalam citra menjadi teks/pesan asli. Adapun langkah-langkah penyelesaiannya adalah sebagai berikut :

1. Proses Enkripsi
   Misalnya akan dilakukan enkripsi pesan yang dalam hal ini password akun email penulis yaitu “senang123!” dengan menerapkan algoritma one time pad. Adapun langkah-langkah penyelesaiannya adalah sebagai berikut :
   a. Menyiapkan karakter plaintext dalam hal ini password akun email penulis yaitu “senang123!” dan menyiapkan karakter kunci (key) yaitu “gmbtxrwado” (panjang karakter plaintext dan key haruslah sama, begitupun sebaliknya).

Tabel 1. Plaintext dan key

Plaintext	Key
s	g
e	m
n	b
a	t
n	x
g	r
1	w
2	a
3	d
!	o

   b. Mengubah karakter plaintext dan key menjadi bentuk angka sesuai nilai dari kode ASCII.
   c. Sesuai dengan tabel kode ASCII di atas, maka karakter plaintext dan key berubah menjadi :

Tabel 2. Nilai ASCII dari plaintext dan key

Plaintext	Nilai	Key	Nilai
s	115	g	103
e	101	m	109

BIOSTech: Bulletin of Computer Science and Information Technology
Vol 1, No 2, Juni 2023
Hal: 72-86
Available Online at https://journal.grahamitra.id/index.php/biostech

Plaintext	Nilai	Key	Nilai
n	110	b	98
a	97	t	116
n	110	x	120
g	103	r	114
1	49	w	119
2	50	a	97
3	51	d	100
!	33	o	111

d. Setelah didapatkan nilai kode ASCII dari plaintext dan key, langkah berikutnya adalah melakukan enkripsi dengan rumus algoritma OTP yaitu :

$$Ci = (Pi + Ki) \bmod 256 \quad (1)$$

Keterangan rumus :
Ci = Ciphertext
Pi = Plaintext
Ki = Key (kunci)

e. Sesuai dengan rumus enkripsi maka didapatkan ciphertext dengan proses enkripsi sebagai berikut :
C (1) = (115 + 103) mod 256 = 218 (Ú)
C (2) = (101 + 109) mod 256 = 210 (Ò)
C (3) = (110 + 98) mod 256 = 208 (Đ)
C (4) = (97 + 116) mod 256 = 213 (Õ)
C (5) = (110 + 120) mod 256 = 230 (æ)
C (6) = (103 + 114) mod 256 = 217 (Ù)
C (7) = (49 + 119) mod 256 = 168 (¨)
C (8) = (50 + 97) mod 256 = 147 (“)
C (9) = (51 + 100) mod 256 = 151 (—)
C (10) = (33 + 111) mod 256 = 144 (□)

f. Setelah proses enkripsi berhasil maka akan didapatkan ciphertext, seperti pada tabel di bawah ini :

Tabel 3. Hasil enkripsi algoritma OTP

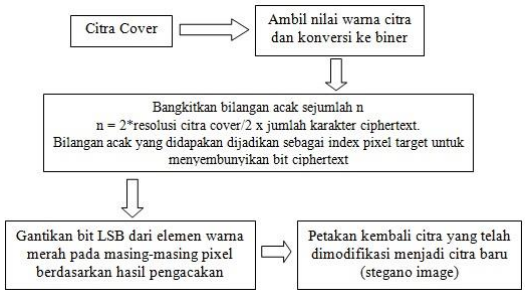
Plaintext	Key	Ciphertext
s	g	Ú
e	m	Ò
n	b	Đ
a	t	Õ
n	x	æ
g	r	Ù
1	w	¨
2	a	“
3	d	—
!	o	□

2. Proses Embedding

Gambar 3. Citra penyembunyi (cover image) resolusi 50x75 pixel (3750 pixel)

Data teks yang telah terenkripsi algoritma OTP (ciphertext) disembunyikan ke dalam citra digital dengan menggunakan metode redundant pattern encoding. Proses embedding berdasarkan metode redudanat pattern encoding, diawali dengan membangkitkan sejumlah bilangan acak (sesuai dengan jumlah bit ciphertext yang akan disembunyikan) untuk mendapatkan posisi pixel yang digunakan untuk menyembunyikan bit dari ciphertext. Proses penyembunyian bit dilakukan dengan mengganti setiap nilai bit Least Significant Bit (LSB) elemen warna merah dari setiap pixel citra cover dengan bit ciphertext. Proses ini dilakukan terus menerus hingga seluruh bit ciphertext disembunyikan ke dalam citra cover.

BIOSTech: Bulletin of Computer Science and Information Technology
Vol 1, No 2, Juni 2023
Hal: 72-86
Available Online at https://journal.grahamitra.id/index.php/biostech



Gambar 4. Alur proses embedding

a. Mengambil nilai warna dari citra cover yang dilakukan dengan menggunakan aplikasi matlab dan mengkonversinya ke dalam biner, sehingga dapat diuraikan nilai-nilai diskrit dari elemen warna merah (red), hijau (green) dan warna biru (blue), seperti pada tabel di bawah ini.

Tabel 4. Nilai diskrit warna citra cover

Pixel	Warna	Dec	Biner	Pixel	Warna	Dec	Biner
	Red	150	10010110		Red	30	00011110
0	Green	20	00010100	8	Green	60	00111100
	Blue	200	11001000		Blue	110	01101110
	Red	5	00000101		Red	150	10010110
1	Green	143	10001111	9	Green	24	00011000
	Blue	200	11001000		Blue	200	11001000
	Red	24	00011000		Red	35	00100011
2	Green	50	00110010	10	Green	20	00010100
	Blue	100	01100100		Blue	101	01100101
	Red	35	00100011		Red	155	10011011
3	Green	22	00010110	11	Green	143	10001111
	Blue	101	01100101		Blue	190	10111110
	Red	105	01101001		Red	10	00001010
4	Green	100	01100100	12	Green	50	00110010
	Blue	75	01001011		Blue	100	01100100
	Red	155	10011011				
5	Green	25	00011001		Sampai nilai pixel ke-3750		
	Blue	195	11000011				
	Red	10	00001010		Red	105	01101001
6	Green	145	10010001	3750	Green	145	10010001
	Blue	190	10111110		Blue	190	10111110

b. Berdasarkan resolusi citra cover di atas, akan dikalkulasikan banyaknya bilangan acak yang dibangkitkan untuk menentukan posisi pixel yang dijadikan sebagai penyembunyi masing-masing bit ciphertext.
Jumlah karakter ciphertext adalah 10 karakter (10 x 8 bit = 80 bit)
Resolusi citra cover adalah 50 x 75 pixel = 3750 pixel
Sehingga :
$n = \frac{3750}{2 \times 10}$ = 187.5 dibulatkan menjadi 188
Artinya bahwa akan dilakukan pembangkitan nilai acak sebanyak 188 nilai acak untuk mendapatkan posisi pixel citra cover yang akan dirubah dengan bit ciphertext.

c. Pembangkitan bilangan acak dilakukan dengan menggunakan metode linear congruent method (LCM). Formulasi untuk mencari nilai acak berdasarkan metode LCM adalah :

$$Z_{i+1} = (a \times z_{i-1} + c) \bmod m \quad (5)$$

Dimana :
Z_i = bilangan acak ke-i dari deretnya
a = faktor penggali
z_{i-1} = bilangan acak sebelumnya
c = angka konstan yang bersyarat (increment)
m = modulus

d. Proses pembangkitan bilangan acak pada contoh kasus ini dilakukan dengan menetapkan ketentuan nilai a = 17, c = 23, z_0 = 123 dan m = 256. Sesuai dengan formulasi LCM dan ketentuan nilai, maka didapatkan alamat pixel untuk menyembunyikan bit ciphertext, sebagai berikut :

BIOSTech: Bulletin of Computer Science and Information Technology
Vol 1, No 2, Juni 2023
Hal: 72-86
Available Online at https://journal.grahamitra.id/index.php/biostech

Z1 = (17 x 123 + 23) mod 256
Z1 = 66 artinya bahwa pixel ke-66 dari citra cover menjadi pixel target yang akan menyembunyikan bit ke-1 dari ciphertext.
Z1 = (17 x 66 + 23) mod 256
Z1 = 121 artinya bahwa pixel ke-121 dari citra cover menjadi pixel target yang akan menyembunyikan bit ke-2 dari ciphertext.
Proses untuk menentukan posisi pixel citra cover yang digunakan untuk menyembunyikan bit ciphertext yang lainnya dilakukan dengan cara yang sama seperti di atas, sehingga didapatkan 80 nilai acak sebagai berikut :

Tabel 5. Pengamatan penyisipan bit ciphertext

Bit ke-i	Pixel Target	Bit ke-i	Pixel Target	Bit ke-i	Pixel Target	Bit ke-i	Pixel Target
1	66	21	174	41	26	61	134
2	121	22	165	42	209	62	253
3	32	23	12	43	248	63	228
4	55	24	227	44	143	64	59
5	190	25	42	45	150	65	2
6	181	26	225	46	13	66	57
7	28	27	8	47	244	67	224
8	243	28	159	48	75	68	247
9	58	29	166	49	18	69	126
10	241	30	29	50	73	70	117
11	24	31	4	51	240	71	220
12	175	32	91	52	7	72	179
13	182	33	34	53	142	73	250
14	45	34	89	54	133	74	177
15	20	35	0	55	236	75	216
16	107	36	23	56	195	76	111
17	50	37	158	57	10	77	118
18	105	38	149	58	193	78	237
19	16	39	252	59	232	79	212
20	39	40	211	60	127	80	43

e. Proses penyembunyian bit ciphertext ke pixel target dilakukan dengan mengganti setiap bit akhir (LSB) elemen warna red pada pixel target.

Tabel 6. Konversi ciphertext ke biner

Ciphertext : Ú Ò Đ Õ æ Ù ¨ “ — □		
Char	**Decimal**	**Biner**
Ú	218	11011010
Ò	210	11010010
Đ	208	11010000
Õ	213	11010101
æ	230	11100110
Ù	217	11011001
¨	168	10101000
“	147	10010011
—	151	10010111
□	144	10010000

f. Bit terakhir (LSB) dari elemen warna merah (Red) dari citra cover diganti dengan bit ciphertext, seperti terlihat pada tabel di bawah ini.

Tabel 7. Proses embedding bit ciphertext

Citra Cover				Bit cipher	Stegano Image			
Pixel target	**Warna**	**Dec**	**Biner**		**Pixel target**	**Warna**	**Dec**	**Biner**
	Red	203	11001011	1		Red	203	11001011
66	Green	102	01100110		66	Green	102	01100110
	Blue	100	01100100			Blue	100	01100100
	Red	211	11010011	1		Red	211	11010011
121	Green	105	01101001		121	Green	105	01101001
	Blue	101	01100101			Blue	101	01100101
32	Red	222	11011110	0	32	Red	222	11011110

	Green	100	01100100			Green	100	01100100
	Blue	111	01101111			Blue	111	01101111
	Red	199	11000111	1		Red	199	11000111
55	Green	180	10110100		55	Green	180	10110100
	Blue	188	10111100			Blue	188	10111100
	Red	185	10111001	1		Red	185	10111001
190	Green	150	10010110		190	Green	150	10010110
	Blue	190	10111110			Blue	190	10111110
	Red	202	11001010	0		Red	202	11001010
181	Green	199	11000111		181	Green	199	11000111
	Blue	205	11001101			Blue	205	11001101
	Red	188	10111100	1		Red	189	10111101
28	Green	125	01111101		28	Green	125	01111101
	Blue	150	10010110			Blue	150	10010110
	Red	222	11011110	0		Red	222	11011110
243	Green	200	11001000		243	Green	200	11001000
	Blue	205	11001101			Blue	205	11001101
	Red	150	10010110	1		Red	151	10010111
58	Green	105	01101001		58	Green	105	01101001
	Blue	111	01101111			Blue	111	01101111
	Red	145	01101111	1		Red	145	01101111
241	Green	130	10000010		241	Green	130	10000010
	Blue	155	10011011			Blue	155	10011011

Dilakukan hingga 80 bit ciphertext digantikan pada bit LSB warna merah masing-masing pixel target

	Red	151	10010111	0		Red	150	10010110
43	Green	120	01111000		43	Green	120	01111000
	Blue	111	01101111			Blue	111	01101111

Berdasarkan proses embedding yang dilakukan, maka terlihat pada tabel 4.7 di atas bahwa perubahan nilai pixel hanya terjadi pada elemen warna merah saja sebanyak 1 bit dan menyebabkan nilai elemen warna merah (red) naik atau turun satu bit akibat penggantian nilai bit LSB-nya. Setelah proses penyisipan seluruh bit dari ciphertext, maka nilai-nilai pixel yang telah diubah dan nilai pixel keseluruhan dari citra cover akan dipetakan kembali menjadi citra yang baru (stegano image).

Gambar 5. Citra Stegano

Berdasarkan citra stegano yang dihasilkan, maka terlihat bahwa perubahan citra asli setelah dilakukan proses penyembunyian ciphertext ke dalamnya tidak terlihat signifikan, sehingga citra stegano yang dihasilkan masih terlihat sama dengan citra cover. Perbedaan tersebut dapat diketahui dengan menghitung nilai Mean Square Error (MSE) dan nilai Peak Signal to Noise Ratio (PSNR) antara kedua citra tersebut.

Melalui nilai MSE didapatkan tingkat perbedaan yang terjadi pada nilai citra asli sedangkan nilai PSNR menunjukkan tingkat kualitas citra stegano yang dihasilkan dengan syarat nilai PSNR di atas 40db memiliki distorsi yang rendah sehingga berkualitas baik.

Nilai MSE didapatkan dengan mencari nilai selisih antara nilai-nilai pixel citra asli pada elemen warna merah (red) dengan nilai pixel citra stegano pada elemen merah (red) dipangkatkan dengan dua dan dibagi dengan resolusi citra.ini. Mengingat resolusi citra sampel yang digunakan sangat besar, maka proses perhitungan nilai MSE dan PSNR hanya dilakukan untuk sejumlah pixel yang digunakan untuk menyembunyikan 80 bit ciphertext yaitu 80 pixel. Agar proses perhitungan lebih mudah, maka dimuat dalam bentuk tabel berikut ini :

Tabel 8. Perhitungan MSE

CITRA COVER			**CITRA STEGANO**		**MSE**
Pixel Target	**Warna**	**Decimal**	**Warna**	**Desimal**	**$(Red_{Cover} - Red_{Stegano})^2$**
66	R	203	R	203	0

CITRA COVER			CITRA STEGANO		MSE
Pixel Target	**Warna**	**Decimal**	**Warna**	**Desimal**	**$(Red_{Cover} - Red_{Stegano})^2$**
	G	102	G		
	B	100	B		
	R	211	R	211	0
121	G	105	G		
	B	101	B		
	R	222	R	222	0
32	G	100	G		
	B	111	B		
	R	199	R	199	0
55	G	180	G		
	B	188	B		
	R	185	R	185	0
190	G	150	G		
	B	190	B		
	R	202	R	202	0
181	G	199	G		
	B	205	B		
	R	188	R	189	1
28	G	125	G		
	B	150	B		
	R	222	R	222	0
243	G	200	G		
	B	205	B		
	R	150	R	151	1
58	G	105	G		
	B	111	B		
	R	145	R	145	0
241	G	130	G		
	B	155	B		
	R	199	R	198	1
24	G	180	G		
	B	188	B		
	R	185	R	185	0
175	G	150	G		
	B	190	B		
	R	202	R	202	0
182	G	199	G		
	B	205	B		
	R	188	R	188	0
45	G	125	G		
	B	150	B		
	R	222	R	223	1
20	G	200	G		
	B	205	B		
	R	155	R	154	1
107	G	199	G		
	B	180	B		
	R	188	R	189	1
50	G	185	G		
	B	150	B		
	R	190	R	191	1
105	G	202	G		
	B	199	B		
	R	205	R	204	1
16	G	188	G		
	B	125	B		
	R	199	R	199	0
39	G	180	G		
	B	188	B		

CITRA COVER			CITRA STEGANO		MSE
Pixel Target	**Warna**	**Decimal**	**Warna**	**Desimal**	**$(Red_{Cover} - Red_{Stegano})^2$**
	R	185	R	184	1
174	G	150	G		
	B	190	B		
	R	60	R	60	0
165	G	100	G		
	B	25	B		
	R	199	R	198	1
12	G	180	G		
	B	188	B		
	R	185	R	184	1
227	G	150	G		
	B	190	B		
	R	202	R	203	1
42	G	199	G		
	B	205	B		
	R	188	R	189	1
225	G	125	G		
	B	150	B		
	R	222	R	222	0
8	G	200	G		
	B	205	B		
	R	150	R	151	1
159	G	199	G		
	B	180	B		
	R	188	R	188	0
166	G	185	G		
	B	150	B		
	R	190	R	191	1
29	G	202	G		
	B	199	B		
	R	205	R	204	1
4	G	189	G		
	B	125	B		
	R	150	R	151	1
91	G	190	G		
	B	202	B		
	R	199	R	199	0
34	G	205	G		
	B	188	B		
	R	125	R	125	0
89	G	150	G		
	B	222	B		
	R	200	R	201	1
0	G	205	G		
	B	155	B		
	R	199	R	198	1
23	G	180	G		
	B	188	B		
	R	185	R	184	1
158	G	150	G		
	B	190	B		
	R	202	R	203	1
149	G	199	G		
	B	205	B		
	R	188	R	189	1
252	G	125	G		
	B	199	B		
211	R	205	R	204	1
	G	189	G		

CITRA COVER			CITRA STEGANO		MSE
Pixel Target	**Warna**	**Decimal**	**Warna**	**Desimal**	**$(Red_{Cover} - Red_{Stegano})^2$**
	B	125	B		
	R	150	R	151	1
26	G	190	G		
	B	202	B		
	R	199	R	199	0
209	G	205	G		
	B	189	B		
	R	125	R	124	1
248	G	150	G		
	B	190	B		
	R	202	R	203	1
143	G	199	G		
	B	205	B		
	R	188	R	189	1
150	G	125	G		
	B	150	B		
	R	222	R	222	0
13	G	200	G		
	B	205	B		
	R	155	R	154	1
244	G	199	G		
	B	180	B		
	R	188	R	189	1
75	G	125	G		
	B	150	B		
	R	222	R	223	1
18	G	200	G		
	B	205	B		
	R	155	R	154	1
73	G	199	G		
	B	180	B		
	R	188	R	189	1
240	G	185	G		
	B	150	B		
	R	190	R	190	0
7	G	202	G		
	B	199	B		
	R	205	R	205	0
142	G	188	G		
	B	125	B		
	R	199	R	198	1
133	G	205	G		
	B	200	B		
	R	205	R	204	1
236	G	155	G		
	B	199	B		
	R	180	R	180	0
195	G	188	G		
	B	185	B		
	R	150	R	151	1
10	G	190	G		
	B	202	B		
	R	199	R	198	1
193	G	205	G		
	B	188	B		
	R	125	R	124	1
232	G	188	G		
	B	125	B		
127	R	150	R	151	1

CITRA COVER			CITRA STEGANO		MSE
Pixel Target	**Warna**	**Decimal**	**Warna**	**Desimal**	**$(Red_{Cover} - Red_{Stegano})^2$**
	G	222	G		
	B	200	B		
	R	205	R	204	1
134	G	155	G		
	B	199	B		
	R	180	R	180	0
253	G	188	G		
	B	185	B		
	R	150	R	151	1
228	G	190	G		
	B	202	B		
	R	199	R	199	0
59	G	205	G		
	B	188	B		
	R	125	R	125	0
2	G	199	G		
	B	125	B		
	R	150	R	150	0
57	G	222	G		
	B	200	B		
	R	205	R	204	1
224	G	155	G		
	B	199	B		
	R	180	R	181	1
247	G	188	G		
	B	185	B		
	R	150	R	150	0
126	G	205	G		
	B	200	B		
	R	205	R	205	0
117	G	155	G		
	B	199	B		
	R	180	R	181	1
220	G	188	G		
	B	185	B		
	R	199	R	199	0
179	G	205	G		
	B	188	B		
	R	125	R	125	0
250	G	150	G		
	B	222	B		
	R	200	R	200	0
177	G	205	G		
	B	155	B		
	R	199	R	198	1
216	G	180	G		
	B	188	B		
	R	185	R	185	0
111	G	150	G		
	B	205	B		
	R	155	R	154	1
118	G	199	G		
	B	180	B		
	R	188	R	188	0
237	G	185	G		
	B	150	B		
	R	190	R	190	0
212	G	202	G		
	B	199	B		

BIOSTech: Bulletin of Computer Science and Information Technology
Vol 1, No 2, Juni 2023
Hal: 72-86
Available Online at https://journal.grahamitra.id/index.php/biostech

CITRA COVER			CITRA STEGANO		MSE
Pixel Target	**Warna**	**Decimal**	**Warna**	**Desimal**	**$(Red_{Cover} - Red_{Stegano})^2$**
	R	151	R	150	1
43	G	120	G		
	B	111	B		
			Total MSE Antara Pixel =		46

Sehingga dapat dihitung :

$$MSE = \frac{\text{Total MSE antara Pixel Red}}{\text{Resolusi}} = \frac{46}{80} = 0{,}575$$

$$PSNR = 10 * \text{Log}_{10}\left(\frac{Nilai\ Maximum\ Citra^2}{\sqrt{MSE}}\right)$$

$$PSNR = 10 * \text{Log}_{10}\left(\frac{222^2}{\sqrt{0{,}575}}\right)$$

PSNR = 48,129db

Berdasarkan perhitungan MSE dan PSNR, diketahui bahwa error (MSE) yang terjadi pada citra stegano yang menyebabkan perbedaannya dengan citra cover hanya sebesar 0,575 dengan distorsi (PSNR) kualitas citra stegano sebesar 48,129db. Hal ini terjadi karena perubahan hanya tejadi pada nilai elemen warna merah (red) pada setiap pixel. Berdasarkan nilai tersebut, maka disimpulkan bahwa perubahan yang terjadi pada citra cover (citra asli) tidak signifikan terlihat serta memiliki nilai kualitas karena nilai error (MSE) yang rendah dan nilai distorsi (PSNR) yang tinggi (>40db).

3. Proses Ekstraksi

Tahapan ini, bit ciphertext yang telah disisipkan dengan metode redundant pattern encoding, akan dipisahkan dari stegano image yang dihasilkan dari proses embedding. Proses ini diawali mentransformasikan citra stegano menjadi nilai-nilai diskrit, kemudian melakukan proses pembangkitan bilangan acak seperti yang dilakukan pada proses dekripsi. Proses pembangkitan sejumlah bilangan acak tetap dilakukan dengan metode LCM dengan nilai-nilai parameter LCM yang sama. Pembangkitan bilangan acak ini dilakukan untuk mendapatkan kembali posisi pixel target penyembunyi biner-biner ciphertext.

a. Proses pemisahan bit ciphertext dilakukan dengan mengambil setiap bit terakhir (LSB) elemen warna merah (Red) dari citra stegano image, seperti terlihat pada tabel di bawah ini.

Tabel 9. Proses ekstraksi bit Stegano Image

Stegano Image				Bit cipher
Pixel target	**Warna**	**Dec**	**Biner**	
	Red	203	11001011	1
66	Green	102	01100110	
	Blue	100	01100100	
	Red	211	11010011	1
121	Green	105	01101001	
	Blue	101	01100101	
	Red	222	11011110	0
32	Green	100	01100100	
	Blue	111	01101111	
	Red	199	11000111	1
55	Green	180	10110100	
	Blue	188	10111100	
	Red	185	10111001	1
190	Green	150	10010110	
	Blue	190	10111110	
	Red	202	11001010	0
181	Green	199	11000111	
	Blue	205	11001101	
	Red	189	10111101	1
28	Green	125	01111101	
	Blue	150	10010110	
	Red	222	11011110	0
243	Green	200	11001000	
	Blue	205	11001101	
	Red	151	10010111	1
58	Green	105	01101001	
	Blue	111	01101111	
241	Red	145	01101111	1

Stegano Image				Bit cipher
Pixel target	**Warna**	**Dec**	**Biner**	
	Green	130	10000010	
	Blue	155	10011011	
Dilakukan hingga didapatkan 80 bit biner dari ciphertext				
	Red	150	10010110	0
43	Green	120	01111000	
	Blue	111	01101111	

b. Bit-bit ciphertext yang telah diambil dari citra stegano akan dikelompokkan menjadi 8 bit setiap kelompok kemudian dikonversi menjadi desimal, sehingga akan didapatkan ciphertext dalam bentuk kode ASCII.

Tabel 10. Konversi biner ke ASCII

Biner	Desimal	Char
11011010	218	Ú
11010010	210	Ò
11010000	208	Đ
11010101	213	Õ
11100110	230	æ
11011001	217	Ù
10101000	168	¨
10010011	147	“
10010111	151	—
10010000	144	□

4. Proses Dekripsi

Terakhir adalah proses dekripsi, merupakan proses mengembalikan pesan asli (plaintext) dari ciphertext yang didapatkan dari hasil ekstraksi.

a. Proses dekripsi berdasarkan algortima one time pad dilakukan dengan ketentuan rumus dekripsi OTP yaitu :
Pi = (Ci - Ki) mod 256
Keterangan rumus :
Pi = Plaintext
Ci = Ciphertext
Ki = Key (kunci)

b. Dalam proses dekripsi ini key yang digunakan adalah key yang sama digunakan pada proses enkripsi yaitu “gmbtxrwado”. Sehingga didapatkan nilai ASCII dari ciphertext dan key seperti pada tabel di bawah ini.

Tabel 11. Nilai ASCII

Char	Nilai ASCII	Key	Nilai ASCII
Ú	218	g	103
Ò	210	m	109
Đ	208	b	98
Õ	213	t	116
æ	230	x	120
Ù	217	r	114
¨	168	w	119
“	147	a	97
—	151	d	100
□	144	o	111

c. Sesuai dengan rumus dekripsi maka ditentukannya plaintext dengan proses dekripsi sebagai berikut :
P (1) = (218 - 103) mod 256 = 115 (s)
P (2) = (210 - 109) mod 256 = 101 (e)
P (3) = (208 - 98) mod 256 = 110 (n)
P (4) = (213 - 116) mod 256 = 97 (a)
P (5) = (230 - 120) mod 256 = 110 (n)
P (6) = (217 - 114) mod 256 = 103 (g)
P (7) = (168 - 119) mod 256 = 49 (1)
P (8) = (147 - 97) mod 256 = 50 (2)
P (9) = (151 - 100) mod 256 = 51 (3)
P (10) = (144 - 111) mod 256 = 33 (!)

d. Setelah proses dekripsi berhasil maka akan didapatkan kode plaintext yaitu :

Tabel 12. Hasil dekripsi algoritma OTP

Ciphertext	Key	Plaintext
Ú	g	s
Ò	m	e
Đ	b	n
Õ	t	a
æ	x	n
Ù	r	g
¨	w	1
“	a	2
—	d	3
□	o	!

4. KESIMPULAN

Berdasarkan analisa yang telah dilakukan pada bab sebelumnya, disimpulkan beberapa hal terkait penelitian ini sebagai berikut Pengamaan data teks berdasarkan metode One Time Pad (OTP) dilakukan dengan mengkombinasikan karakter kunci dengan karakter pesan yang diamankan, sehingga cara ini menyebabkan terjadinya duplikasi atau perulangan penggunaan karakter kunci yang sama. Konsep ini pengamanan seperti ini akan sangat mudah dipecahkan oleh penyerang dengan menggunakan metode pemecahan kunci, salah satunya adalah metode kasiki. Pengkombinasian algoritma OTP yang merupakan salah satu teknik kriptografi dengan metode Redudant Pattern Encoding (RPE) yang merupakan salah satu metode steganografi mampu meningkatkan keterjaminan keamanan pesan rahasia atau penting, karena pesan rahasia diamanakan dengan dua teknik yang berbeda. Penyembunyian bit ciphertext pada citra digital berdasarkan metode RPE pada pixel yang acak. Hal inilah yang menambah kerumitan untuk mengetahui posisi penempatan bit ciphertext pada citra. Berdasarkan pengujian sampel yang dilakukan dalam penelitian ini, diperoleh bahwa citra stegano yang dihasilkan tidak memiliki perbedaan yang signifikan dengan citra asli (cover) yang ditunjukkan dengan nilai MSE hanya 0,575 dan nilai PSNR adalah 48,129db yang menunjukkan tingkat kualitas citra stegano lebih baik.

REFERENCES

[1] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, “Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard,” Inform. Mulawarman J. Ilm. Ilmu Komput., vol. 10, no. 1, p. 20, 2016, doi: 10.30872/jim.v10i1.23.
[2] N. E. Saragih, “Implementasi Algoritma One Time Pad pada Pesan,” J. Ilm. MATRIK, vol. Vol.20 No., no. 3, pp. 31–40, 2018.
[3] Sumandri, “Studi Model Algoritma Kriptografi Klasik dan Modern,” Semin. Mat. dan Pendidik. Mat. UNY, pp. 265–272, 2017.
[4] M. Irawan, “Penggunaan Steganografi dengan Metode End of File (EOF) pada Digital Watermarking,” J. Teknol. Inf. Komput., vol. 2, no. 1, pp. 36–42, 2013.
[5] D. A. Setyawan, “Data dan Metode Pengumpulan Data Penelitian,” Metodol. Penelit., pp. 9–17, 2013.
[6] K. Harianto, “Penerapan Interpolasi Lanjar Terhadap Piksel Gambar Digital yang,” SATIN - Sains dan Teknol. Inf., 2014.
[7] M. A. Maricar and O. Widyantara, “Pemampatan Citra Pas Foto dengan Menggunakan Algoritma Kompresi Joint-Photograpic Experts Group (JPEG) dan Principal Component Analysis (PCA),” Maj. Ilm. Teknol. Elektro, vol. 17, no. 1, p. 102, 2018, doi: 10.24843/mite.2018.v17i01.p14.
[8] H. Santoso and M. Z. Siambaton, “APLIKASI PENGAMANAN EKSTENSI FILE MENGGUNAKAN KRIPTOGRAFI ONE TIME PAD (OTP) DAN ELLIPTIC CURVE CRYPTOGRAPHY (ECC),” vol. 5, no. 1, pp. 22–38, 2020.
[9] R. F. Sannawira and A. S. Purnomo, “Penyisipan Citra Pesan Ke Dalam Citra Berwarna Menggunakan Metode Least Significant Bit dan Redundant Pattern Encoding,” Informatics J., vol. 1, no. 1, pp. 39–46, 2016, [Online]. Available: www.eepis-its.edu/uploadta/downloadmk.php?id=1216.
[10] D. Rofifah, “済無No Title No Title No Title,” Pap. Knowl. . Towar. a Media Hist. Doc., pp. 12–26, 2020.
[11] G. M. Male, Wirawan, and E. Setijadi, “Analisa Kualitas Citra Pada Steganografi untuk Aplikasi e-Government,” Pros. Semin. Nas. Manaj. Teknol. XV, pp. 1–9, 2012.
[12] A. Ilmiah, “Modifikasi Kriptografi One Time Pad (OTP) Menggunakan Padding Dinamis dalam Pengamanan Data File Modifikasi Kriptografi One Time Pad (OTP) Menggunakan Padding Dinamis dalam Pengamanan Data File,” 2014.
[13] E. F. Nugraha, “Meningkatkan Kapasistas Pesan yang disisipkan dengan Metode Redundant Pattern Encoding,” 2010.