Terbit *online* pada laman web jurnal :
http://ejournal.amikompurwokerto.ac.id/index.php/telematika/

Telematika

Terakreditasi Sinta "3" KEMENRISTEKDIKTI, No. 21/E/KPT/2018

Implementasi Keamanan Pesan pada Citra Steganografi Menggunakan Modifikasi Cipher Block Chaining (CBC) Vigenere

Hanifatus Sa'diyah[1], Vera Wati[2], Dony Ariyus[3]

[1,2,3] Magister Teknik Informatika
Universitas AMIKOM Yogyakarta
Email : hanifputri2013@gmail.com[1], verave.wati@gmail.com[2], dony.a@amikom.ac.id[3]

I N F O A R T I K E L

Sejarah Artikel:
Menerima 17 Desember 2019
Revisi 1 Februari 2020
Diterima 27 Februari 2020
Online 29 Februari 2020

Keywords:
Cryptography,
Cipher Block Chaining,
Vigenere,
LSB,
Data Security

Kata Kunci:
Cryptography,
Cipher Block Chaining,
Vigenere,
LSB,
Keamanan Data

Korespondensi:
Telepon: +62 81229883223
E-mail:
hanifputri2013@gmail.com

ABSTRACT

Internet of Things (IoT) provides easy transportation of data and information, but on the other hand, provides opportunities for cyber-terrorists and attackers to carry out attacks on data and information so that security of data and information is needed. This study aims to combine cryptographic techniques with the classical algorithm that is Vigenere Cipher and modern algorithms that Cipher Block Chaining (CBC), which will be integrated with steganographic techniques Least Significant Bit (LSB) to insert the message information on an object image to provide data security and information more. Is expected to support the various fields of digital watermark and capable of being used in the picture. Testing with 25 times the encryption and decryption process was successfully carried out 18 times and failed seven times, influenced by the size and dimensions of the image. Performance on this algorithm can accommodate both symbols, characters and numbers. However, changes in image size affect the process of decryption and encryption.

ABSTRAK

Internet of Things (IoT) menghadirkan kemudahan pertukaran data dan informasi, namun demikian di sisi lain memberikan peluang kepada *cyber-terrorist* dan penyerang untuk melakukan serangan terhadap data dan informasi sehingga pengamanan data dan informasi diperlukan. Penelitian ini bertujuan mengkombinasikan teknik kriptografi dengan algoritme klasik yaitu *Vigenere Cipher* dan algoritme modern yaitu *Cipher Block Chaining* (CBC) yang akan diintegrasikan dengan teknik steganografi *Least Significant Bit* (LSB) untuk menyisipkan pesan informasi di sebuah objek gambar sehingga memberikan keamanan data dan informasi yang lebih tinggi. Diharapkan mampu mendukung layanan berbagai bidang sehingga mampu digunakan digital *watermark* pada gambar. Hasil penelitian yang telah dilakukan menghasilkan visualisasi tidak adanya perbedaan pesan yang belum dan sudah terenkripsi. Pengujian dengan 25 kali proses enkripsi dan dekripsi berhasil dilakukan sebanyak 18 kali dan gagal sebanyak 7 kali, dipengaruhi oleh ukuran dan dimensi citra. Kinerja pada algoritme ini mampu menampung dengan baik simbol, karakter dan angka. Namun perubahan pada *size* gambar berpengaruh ketika proses dekripsi dan enkripsi.

PENDAHULUAN

Internet of Things memiliki potensi besar menawarkan berbagai jenis layanan yang mampu menyelesaikan permasalahan di kehidupan sosial maupun lingkungan bisnis, salah satu jenis layanan yang ditawarkan adalah layanan komunikasi (Atzori, dkk., 2010)(Abomhara dan Koien, 2015). Layanan komunikasi dengan IoT menghadirkan kemudahan pertukaran data dan informasi. Statistik terbaru berdasarkan *International Telecommunication Union* (ITU) mengungkapkan bahwa (ITU, 2017) lebih dari

830 juta pelanggan diseluruh dunia dan 80% populasi dunia memiliki akses ke *internet*. Hal ini membuktikan bahwa IoT memberikan kemudahan berkomunikasi.

Hadirnya IoT memberikan kemudahan berkomunikasi, namun demikian di sisi lain juga menghadirkan ancaman dan memberikan peluang kepada *cyber-terrorist* dan penyerang untuk melakukan serangan (Goutam, 2015). Serangan yang dapat mengancam data dan informasi berupa interupsi, penyadapan informasi, pencurian identitas, pelanggaran hak privasi, penyisipan virus, dan penyisipan data maupun informasi (Ijemaru, dkk., 2018)(Zou, dkk., 2016). Jumlah ancaman semakin meningkat setiap hari dengan jumlah dan kompleksitas yang tinggi (Abomhara dan Koien, 2015). Tidak hanya jumlah penyerang berpotensial yang semakin meningkat, namun jaringan yang semakin meluas dan alat yang tersedia lebih canggih, efektif dan efisien (Kizza, 2013)(Taneja, 2013). Oleh karena itu, keamanan data dan informasi diperlukan dan hal ini menjadi perhatian utama untuk memerangi adanya *cyber crime* karena meluasnya penggunaan *internet* (Zou, dkk., 2016)(Laskar dan Hemachandran, 2012). Keamanan media data dan informasi dapat disisipkan pada sebuah media, yakni dalam format gambar, audio, dan format teks file. Teknik pendekatan ini bisa menggunakan steganografi. Tujuan dari steganografi menjadikan penyembunyian informasi tanpa dicurigai perubahannya. Seperti kasus untuk legitimasi pada gambar dilakukan upaya *watermarking* untuk melindungi keaslian isi informasi dan menghindarkan dari *copyright*.

Kini teknik steganografi bisa lebih ditingkatkan dengan penggunaan kriptografi. Kedua teknik tersebut memiliki tujuan menyembunyikan informasi yang memberikan jaminan akan kerahasiaan dan integritas data (Laskar dan Hemachandran, 2012)(Raphael dan Sundaram, 2010). Steganografi merupakan jenis komunikasi tersembunyi (Laskar dan Hemachandran, 2012)(Li, dkk., 2011) yang bertujuan menyembunyikan informasi di media digital sehingga keberadaan pesan rahasia tidak terdeteksi (Laskar dan Hemachandran, 2012)(Johnson dan Mason, 1998). Teknik kriptografi merupakan teknik mengacak data (Maruf, Riadi dan Prayudi, 2015). Pada teknik kriptografi, struktur pesan akan diacak sedemikian rupa agar pesan tidak memiliki makna dan tidak dapat dipahami(Laskar dan Hemachandran, 2012)(Anderson, 1989). Proses enkripsi akan mengubah informasi dan menjadikan informasi tersebut tidak dapat dibaca (Kester, 2012)(Sinkov, 2009).

Pada dasarnya steganografi dan kriptografi memiliki perbedaan hasil dalam hal teknik penyembunyian data dan informasi. Namun demikian, kedua teknik penyembunyian informasi ini akan saling melengkapi satu sama lain (Laskar dan Hemachandran, 2012). Seberapa baik suatu pesan disembunyikan di dalam media digital, ada kemungkinan pesan tersembunyi itu ditemukan oleh pihak ketiga. Penggabungan steganografi dan kriptografi maka pengamanan pesan yang lebih baik akan tercapai dengan cara menyembunyikan keberadaan pesan yang telah terenkripsi (Laskar dan Hemachandran, 2012)(Raphael dan Sundaram, 2010)(Song dkk., 2011).

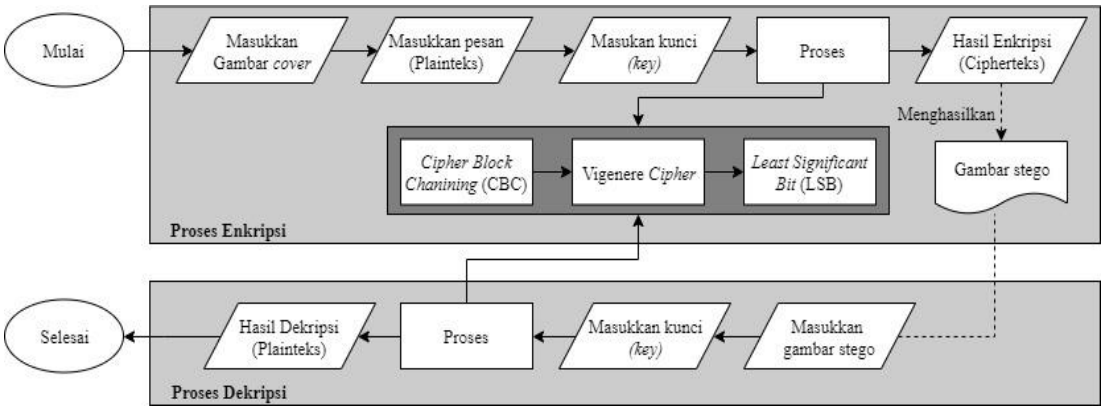
Teknik penerapan penggabungan steganografi dan kriptografi telah dikembangkan pada beberapa penelitian. Penelitian (Permana, 2018), mengamankan pesan teks menggunakan algoritme *Vigenere Cipher*. Proses mengamankan pesan dilakukan dengan cara substitusi, yaitu mengubah setiap huruf menjadi huruf lain berdasarkan kunci yang digunakan. Namun demikian, metode kasiski telah mampu memecahkan enkripsi pesan rahasia algoritme *Vigenere Cipher*. Pemecahan enkripsi ini didasari karena penggunaan kunci yang hanya terdiri dari 26 karakter kunci pada pesan sehingga dapat dengan mudah dipecahkan (Hidayat, Gerhana dan Syaripudin, 2018).

Penelitian melakukan peningkatan keamanan pesan dengan mengkombinasikan algoritme kriptografi klasik dan modern yaitu algoritme *Vigenere Cipher* dan *Cipher Block Chaining* (CBC).

Keunggulan mode operasi CBC adalah pengacakan data biner di dalam blok. Hasil enkripsi blok sebelumnya diumpan-balikkan *(feedback)* ke dalam enkripsi blok *current*, sehingga *cipher* blok yang dihasilkan sepenuhnya tergantung pada semua blok biner dari plainteks (Humendru dan Zebua, 2018). Penelitian ini mengkombinasikan hasil enkripsi *Vigenere Cipher* dan *Cipher Block Chaining* (CBC) dengan algoritme *Least Signicant Bit* (LSB) sehingga menghasilkan proteksi ganda pada keamanan pesan. Kelebihan metode ini pada pengamanan data yang tinggi, sehingga mencegah adanya serangan *stego-attack*, mempertahankan resolusi gambar agar tidak banyak berubah, dan gambar tidak mencurigakan di mata manusia yang akan diabaikan ketika ada pesan rahasia, serta mudah diimplementasikan (Kavitha, dkk., 2012). Maka dalam mendukung layanan kehidupan sosial dalam berbagai bidang, penelitian ini diharapkan mampu digunakan untuk digital *watermark.* Dimana informasi disembunyikan pada format gambar sehingga dilakukan perlindungan *copyright* meskipun dapat diakses dengan *internet* dimanapun dan kapanpun. Namun metode steganografi LSB dalam menyisipkan informasi pada gambar masih bergantung pada resolusi gambar, maka perlu peningkatan metode steganografi untuk menampung lebih banyak karakter pada informasi yang akan disisipkan.

METODE PENELITIAN

Penelitian ini akan mengkombinasikan algoritme klasik yaitu *Vigenere Cipher* dan algoritme modern *Cipher Block Chainning* (CBC). Alur kinerja dari kombinasi terdapat pada Gambar 1.



Gambar 1 Skema Proses Penyandian dan Penyisipan Pesan

Dijelaskan pada Gambar 1 skema proses penyandian dan penyisipan pesan menggunakan *Vigenere Cipher* dan *Cipher Block Chainning* (CBC) melalui 2 tahapan, yakni :

1. Proses Enkripsi

Pada proses enkripsi dimulai dari penyisipan gambar, kemudian masukan pesan asli (plainteks) dengan beberapa karakter. Pesan asli merupakan informasi yang ingin dilakukan proses enkripsi, masukkan kunci sebagai inisiasi proses. Proses enkripsi melibatkan 3 (tiga) metode, yaitu modifikasi CBC dengan *Vigenere Chiper* untuk proses kriptografi pada pesan dan pendekatan LSB sebagai proses steganografi. Jika berhasil diproses, maka akan menghasilkan informasi acak (cipherteks) dan gambar stego (gambar yang tersisipi pesan).

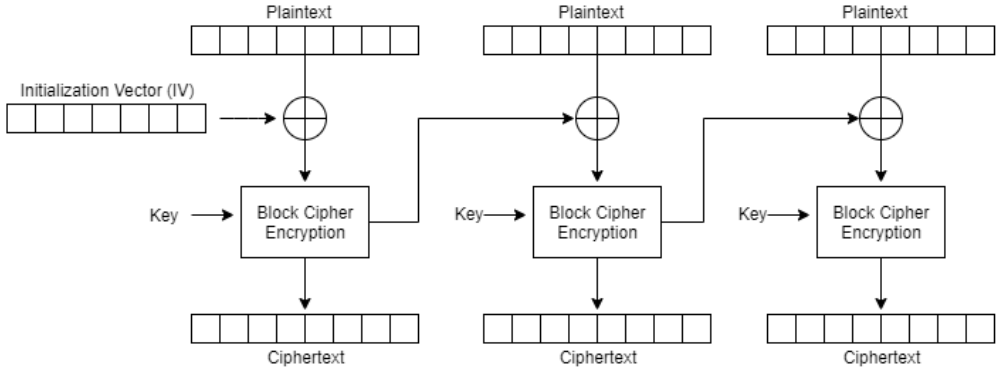
2. Proses Dekripsi

Proses dekripsi menjadi langkah dalam pengembalian pesan yang disisipi pada gambar (gambar stego) untuk kembali ke semula. Proses awal dimulai dari memasukkan gambar stego, kemudian memasukkan kunci penyandian. Dilakukan proses dengan metode yang digunakan sehingga isi pesan asli (plainteks) dapat diketahui.

Ada beberapa metode yang digunakan pada penelitian, yaitu *Cipher Block Chaining* (CBC) digunakan untuk proses kriptografi yang dimodifikasi menggunakan *Vigenere Cipher*. Proses steganografi digunakan pendekatan *Least Significant Bit* (LSB) yakni perubahan dilakukan penyisipan pada bit terakhir pada suatu gambar stego. Metode yang digunakan antara lain :

1. *Cipher Block Chaining* (CBC)

Tahapan proses enkripsi algoritme *Cipher Block Chaining* (CBC) adalah dengan cara meng-XOR-kan blok plainteks dengan *Initialization Vector* (IV). Hasil XOR yang didapat diawal kemudian akan dilakukan XOR kembali dengan menggunakan kunci sehingga menghasilkan cipherteks untuk blok pertama. Cipherteks di blok pertama selanjutkan digunakan sebagai *Initialization Vector* (IV) untuk enkripsi pada blok yang selanjutmya (Dashti, Kheradmand dan Jazi, 2016)(Lestiawan dan Purnama, 2016). Tahapan proses enkripsi dapat dilihat pada Gambar 2.

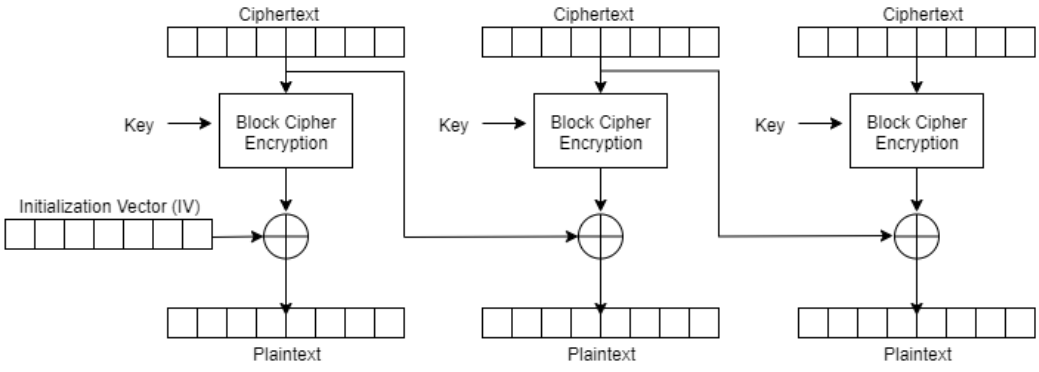


Gambar 2 Proses Enkripsi Algoritme *Cipher Block Chaining* (CBC)

Secara sistematis proses enkripsi CBC dituliskan pada persamaan 1 berikut ini.

$$C_i = E_k\ (P_i \oplus C_{i-1}), C_0 = \text{IV} \qquad (1)$$

Pada proses dekripsi algoritme *Cipher Block Chaining* (CBC) akan dilakukan hal yang sebaliknya dari proses enkripsi. Blok plainteks yang pertama akan didapatkan dengan cara meng-XOR-kan *Initialization Vector* (IV) dengan hasil dekripsi dari blok cipherteks yang pertama (Dashti, Kheradmand dan Jazi, 2016)(Lestiawan dan Purnama, 2016). Ilustrasi proses dekripsi disajikan pada Gambar 3.



Gambar 3 Proses Dekripsi Algoritme *Cipher Block Chaining* (CBC)

Secara sistematis proses dekripsi CBC dituliskan pada persamaan 2 berikut ini.

$$C_i = E_k\ (P_i \oplus C_{i-1}), C_0 = \text{IV} \qquad (2)$$

2. *Vigenere Cipher*

Vigenere Cipher dipopulerkan oleh Giovan Bellaso tahun 1553 yang kemudian telah dikembangkan oleh Blaisede Vigenere dengan menggunakan *autokey cipher*. *Vigenere Cipher* untuk proses enkripsi dan

dekripsi akan menggunakan bujur sangkar *Vigenere* (Handoko, dkk., 2019)(Senthil, Prasanthi dan Rajaram, 2013). Enkripsi *Vigenere Cipher* secara matematis dituliskan pada persamaan (3) berikut ini:

$$C_i = (P_i + K_i)\ mod\ 26 \qquad (3)$$

C_i = nilai ascii dari karakter ciphertext ke-i

P_i = nilai ascii dari karakter plaintext ke-i

K_i = nilai ascii dari karakter kunci ke-i

Sedangkan dekripsi *Vigenere Cipher* secara matematis dituliskan pada persamaan (4) berikut ini:

$$P_i = (C_i - K_i)\ mod\ 26 \qquad (4)$$

C_i = nilai ascii dari karakter ciphertext ke-i

P_i = nilai ascii dari karakter plaintext ke-i

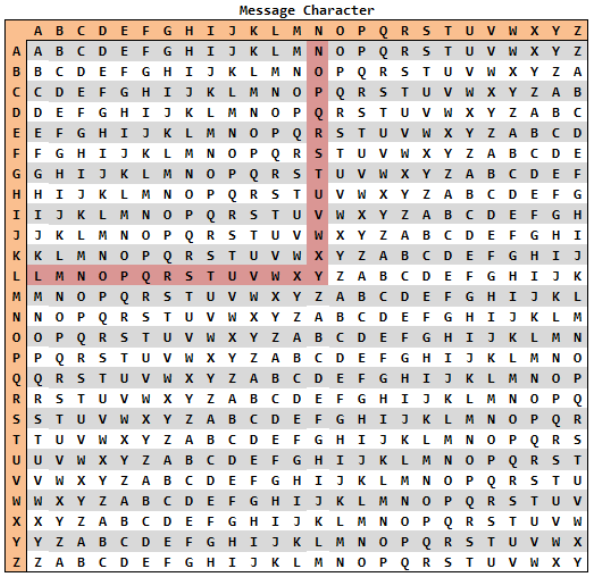
K_i = nilai ascii dari karakter kunci ke-i

Dimana nilai desimal karakter : A=0, B=1, C=2, D=3 ... Z=25

Angka module yang digunakan pada persamaan (3)(4) hanya digunakan untuk proses enkripsi dan dekripsi dengan jumlah karakter 26. Jika semua karakter ASCII digunakan untuk proses enkripsi, maka persamaan yang digunakan menggunakan modulo 256.

3. Modifikasi *Cipher Block Chaining* (CBC) dan *Vigenere Cipher*

CBC menjadi algoritme yang melibatkan nilai Inisialisasi Vektor (IV) pada blok *cipher*. Hasil enkripsi sesuai kinerja CBC pada Gambar 2 selanjutnya akan dilakukan proses enkripsi kembali dengan mengadopsi kinerja *Vigenere* dengan menggunakan persamaan (3). Sehingga proses dekripsi pun dilakukan dengan metode yang sama. Penulis memodifikasi mode *Vigenere Cipher* dengan menggunakan tabel yang mengadopsi tabel *Vigenere Cipher* seperti pada Gambar 4.



Gambar 4. Tabel Vigenere Cipher (Wikibooks, 2020)

Pada *"message character"* di isi untuk informasi (plainteks) yang akan di lakukan proses enkripsi, kemudian dicocokkan dengan kunci yaitu "key character" kemudian dilakukan titik temu hingga menghasilkan isi pesan baru dalam bentuk cipherteks. Proses bisa dipercepat dengan persamaan (3)(4) untuk proses enkripsi dan dekripsinya yang dibantu dengan module. Modifikasi penelitian yakni hasil dari CBC kemudian diproses dengan *Vigenere Cipher*. Proses ini sebagai proses kriptografi.

4. *Least Signicant Bit* (LSB)

Teknik steganografi yang umum digunakan adalah metode *Least Significant Bit* (LSB) walaupun umum dan sering digunakan karena kemudahan dalam penerapannya, namun akan sulit jika dikombinasikan dengan teknik kriptografi menggunakan populasi kunci tertentu (Syawal, Fikriansyah dan Agani, 2016). LSB merupakan salah satu algoritme yang digunakan untuk menyembunyikan pesan dalam media digital sehingga pihak lain tidak menyadari bahwa terdapat informasi rahasia dalam gambar tersebut (Song, dkk., 2011). Proses LSB bit dari gambar *cover* di ilustrasikan pada Gambar 5. Misalkan; terdapat karakter JOG dengan nilai biner 01001010 01001111 01000111.

Biner Gambar Cover							
11100100	10000001	10110100	10001111	10111100	10110111	11100000	11001100
10101010	10000110	11110111	11010100	10000000	11100101	11111111	10000011
11000011	11000000	11000001	11010001	10000111	11100000	11111110	11000000

↓

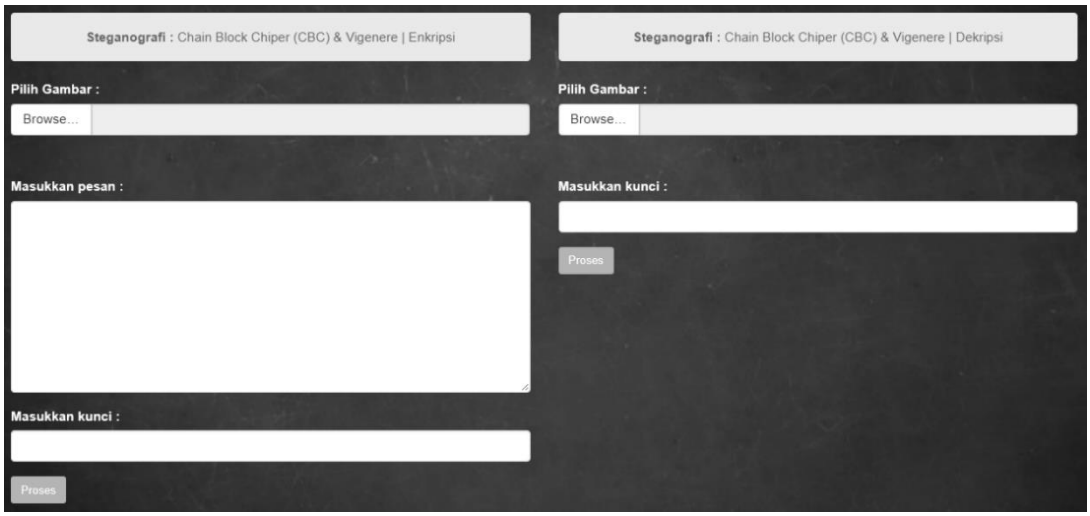
Biner Gambar Stego							
11100100	10000001	10110100	10001110	10111101	10110110	11100001	11001100
10101010	10000111	11110110	11010100	10000001	11100101	11111111	10000011
11000010	11000001	11000000	11010000	10000110	11100001	11111111	11000001

Gambar 5 Pengubahan Biner pada Gambar *Cover* ke Gambar Stego

Pada Gambar 5 nilai dari LSB dalam suatu bit terletak pada angka bit paling terakhir, dan merupakan angka yang cocok untuk diganti dengan mengubah nilai bit satu lebih tinggi atau lebih rendah dari nilai sebelumnya (Raphael dan Sundaram, 2010). Dalam penerapan algoritme CBC dan *Vigenere* yang akan diintegrasikan dengan LSB, hasil cipherteks dari CBC dan *Vigenere* diubah ke kode biner berdasarkan tabel ASCII untuk disisipkan bit terakhir pada gambar.

HASIL DAN PEMBAHASAN

Implementasi pengamanan informasi dengan teknik kriptografi modifikasi CBC dan vigenere yang kemudian dilanjutkan dengan teknik steganografi menggunakan mode Least Signicant Bit (LSB) disajikan pada Gambar 6.



Gambar 6 Desain Antar Muka Kriptografi Modifikasi CBC dan Vigenere dengan Teknik Steganografi

1. Skenario Pengujian

a. Pengujian Visual

Pengujian visual digunakan untuk memberikan perbandingan pada cover image dan stego image setelah dilakukan enkripsi maupun sebelum dilakukan enkripsi secara kasat mata. Implementasi teknik steganografi memberikan pengamanan pesan agar tidak terdeteksi secara kasat mata(Tiwari, Yadav and Mittal, 2014), sehingga diperlukan skenario pengujian visual.

Tabel 1 Skenario Pengujian Visual 1

Gambar Stego	:	
Pesan Rahasia	:	Belajar Kriptografi CBC Vigenere
Gambar *Cover*	:	

Tabel 2 Skenario Pengujian Visual 2

Gambar *Cover*	:	
Pesan Rahasia	:	Local Wisdom Indonesia is gudeg
Gambar Stego	:	

Tabel 3 Skenario Pengujian Visual 3

Gambar *Cover*	:	
Pesan Rahasia	:	Kesultanan Ngayogyakarta Hadiningrat berada di Jogja
Gambar Stego	:	

Tabel 1,2,3 menunjukkan hasil pengujian visual secara kasar mata pada gambar *cover* dan gambar stego yang menunjukkan tidak ada perbedaan pada hasil enksipsi gambar. Hasil gambar stego yang menunjukkan tidak adanya perbedaan dengan gambar *cover* mengacu pada penelitian yang memberikan perubahan keduanya tidak terlalu mencolok.

b. Pengujian Kapasitas Penyisipan Gambar

Kelebihan teknik steganografi adalah pada kapasitas data yang berhasil disisipkan atau disimpan pada gambar *cover*. Pengujian kapasitas penyisipan dilakukan untuk mengetahui seberapa besar kapasitas pesan yang dapat disisipkan pada gambar *cover*. Hal inilah yang mendasari perlunya dilakukan pengujian pada kapasitas pennyisipan pesan. Hasil pengujian kapasitasn penyisipan disajikan pada Tabel 4. berikut ini.

Tabel 4 Hasil Pengujian Kapasitas Penyisipan Gambar

No	Info Enkripsi			Info Embedd			Proses	
	Nama Gambar	Kunci	Karakter	Ukuran Awal	Ukuran Akhir	Tipe File	Enkripsi	Dekripsi
1	Doraemon.jpg	Amikom	The Avengers is a 2012 American superhero film	7,391 bytes	-	.png	Gagal	Gagal
	Doraemon.jpg	Amikom	2012567653	7,391 bytes	53,737 bytes	.png	Berhasil	Berhasil
	Doraemon.jpg	Amikom	!@#$%%$#^	7,391 bytes	53,739 bytes	.png	Berhasil	Berhasil
	Doraemon.jpg	Amikom	The Avengers is !@# American superhero film	7,391 bytes	-	.png	Gagal	Gagal
	Doraemon.jpg	Amikom	The Avengers !@# American	7,391 bytes	53,818 bytes	.png	Berhasil	Berhasil
	Doraemon.jpg	Amikom	The Ave ngers !@# 12 American	7,391 bytes	53,836 bytes	.png	Berhasil	Berhasil
	Doraemon.jpg	Indonesia jaya	The Avengers !@# 12 American	7,391 bytes	53,839 bytes	.png	Berhasil	Berhasil
	Doraemon.jpg	Indonesia jaya	The Avengers !@# 12 American film	7,391 bytes	-	.png	Gagal	Gagal
	Doraemon.jpg	!@#12	The Avengers !@# 12 Americanfilm	7,391 bytes	53,844 bytes	.png	Berhasil	Berhasil
	Doraemon.jpg	!@#12	The Avengers !@# 12 Americansuperherofilm	7,391 bytes	-	.png	Gagal	Gagal
2	Lena.jpg	Amikom	The Avengers is a 2012 American superhero film	11,782 bytes	-	.png	Gagal	Gagal
	Lena.jpg	Amikom	The Avengers is a 2012 American superhero	11,782 bytes	103,511 bytes	.png	Berhasil	Berhasil
	Lena.jpg	Amikom	The Avengers is a 2012 American superherofilm	11,782 bytes	103,529 bytes	.png	Berhasil	Berhasil
	Lena.jpg	Amikom	201256235712391723	11,782 bytes	103,455 bytes	.png	Berhasil	Berhasil
	Lena.jpg	Amikom	!@#$%^&*(__+){|":?><	11,782 bytes	103,448 bytes	.png	Berhasil	Berhasil
	Lena.jpg	amikom unggul	201256235712391723	11,782 bytes	103,455 bytes	.png	Berhasil	Berhasil
	Lena.jpg	12345	!@#$%^&*(__+){\|":?><?><:"><}(*&^%^&*^^*&^^^^%$<>:?":{}+	11,782 bytes	-	.png	Gagal	Gagal
	Lena.jpg	12345	!@#$%^&*(__+){\|":?><?><:"><}(*&^%^&*^^*&^^^^%$<>:?":{}+	11,782 bytes	-	.png	Gagal	Gagal

			!@###@@$$%^>?:"|){+_}(*&&*_					
	Lena.jpg	@#$%^ &	!@#$%^&*(__+){\|": ?><&**^$	11,782 bytes	103,479 bytes	.png	Berhasil	Berhasil
3	Monas.jpg	Amikom	The Avengers is a 2012 American superhero film	20,246 bytes	142,034 bytes	.png	Berhasil	Berhasil
	Monas.jpg	Amikom	20125623571239172 3	20,246 bytes	141,894 bytes	.png	Berhasil	Berhasil
	Monas.jpg	Amikom	!@#$%^&*(__+){|": ?><	20,246 bytes	141,920 bytes	.png	Berhasil	Berhasil
	Monas.jpg	Amikom unggul	20125623571239172 3	20,246 bytes	141,889 bytes	.png	Berhasil	Berhasil
	Monas.jpg	12345	!@#$%^&*(__+){\|": ?><?><:"><} (*&^%^&*^^*&^^^^ %$<>:?":{}+	20,246 bytes	142,088 bytes	.png	Berhasil	Berhasil
	Monas.jpg	@#$%^ &	!@#$%^&*(__+){\|": ?><?><:"><} (*&^%^&*^^*&^^^^ %$<>:?":{}+ !@###@@$$%^>?:"\|){+_}(*&&*_ !@###@@$$%^>?:"|){+_}(*&&*_	20,246 bytes	142,314 bytes	.png	Berhasil	Berhasil

Pada pengujian penyisipan pesan pada 25 kali masing-masing pada proses enkripsi dan dekripsi, telah ditemukan keberhasilan sebanyak 18 kali pada proses enkripsi dan dekripsi dan kegagalan proses sebanyak 7 kali. Pada pengujian ini modifikasi CBC *Vigenere* yang di sisipkan pada citra steganografi menemukan beberapa temuan yaitu sistem ini mampu membaca pesan karakter, angka dan simbol. Hasil inputan ketika proses enkripsi mampu memanggil citra yang berwarna dengan format .jpg namun hasil enkripsi dijadikan format .png dan dan citra tetap terjaga warnanya. Jumlah pesan, kunci dan ukuran citra berpengaruh pada proses enkripsi dan dekripsi karena dipengaruhi oleh file gambar yang terlalu kecil *size* sekitar sampai 10 KB dengan nilai lebar dan tinggi (dimensi) gambar yang terlalu kecil. Namun sejauh ini kinerja dari metode ini berkerja dengan baik dalam proses enkripsi dan dekripsi.

c. Pengujian Enkripsi dan *Embedding*

Pengujian enkripsi dan embedding dilakukan untuk menguji keberhasilan sistem dalam melakukan penyembunyian informasi dengan menggunakan modifikasi teknik kriptografi CBC dan *Vigenere Cipher* yang diintegrasikan dengan teknik steganografi *Least Signicant Bit* (LSB). Tabel 5 menunjukkan hasil pengujian enkripsi dan embedding pada sistem.

Tabel 5 Hasil Pengujian Enkripsi dan Embedding

No	Info Enkripsi			Info Embedd			Proses	
	Nama Gambar	Kunci	Jumlah Pesan	Ukuran Awal	Ukuran Akhir	Tipe File	Enkripsi	*Embedd*
1	Doraemon.jpg	Amikom	4 kata	7,391 bytes	53,818 bytes	.png	Berhasil	Berhasil
2	Lena.jpg	Amikom	4 word	13,459 bytes	103,458 bytes	.png	Berhasil	Berhasil
3	Monas.jpg	Jawa	10 word	20,246 bytes	142,057 bytes	.png	Berhasil	Berhasil

Tabel 5. menunjukkan bahwa setiap kunci yang digunakan untuk skenario uji enkripsi dan *embed* berhasil. Jumlah pesan yang disisipkan memiliki perbedaan satu dengan yang lainnya, hal ini bergantung pada ukuran bit citra yang digunakan. File gambar sebelum dilakukan enkripsi memiliki tipe file .jpg dan

setelah dilakukan enkripsi tipe file akan berubah menjadi .png dengan ukuran gambar yang berbeda sesuai dengan jumlah pesan dan kunci yang digunakan.

d. Pengujian Dekripsi dan *Extracting*

Pengujian dekripsi dan *extracting* dilakukan untuk menguji keberhasilan sistem dalam melakukan pengembalian pesan informasi rahasia menggunakan modifikasi teknik kriptografi CBC dan *Vigenere Cipher* yang diintegrasikan dengan teknik steganografi *Least Signicant Bit* (LSB). Tabel 6 menunjukkan hasil pengujian dekripsi dan *extracting* pada sistem.

Tabel 6 Hasil Pengujian Dekripsi dan Extracting

No	Info Extracting			Info Dekripsi				Proses	
	Nama Gambar	Kunci	Jumlah Pesan Awal	Ukuran Awal (bytes)	Ukuran Akhir (bytes)	Tipe File	Jumlah Pesan Akhir	Dekripsi	*Extract*
1	Doraemon.jpg	Amikom	7 kata	7,391	53,922	.png	7 kata	Berhasil	Berhasil
2	Lena.jpg	jogja	4 word	13,459	103,458	.png	4 word	Berhasil	Berhasil
3	Monas.jpg	jawa	10 word	20,246	142,057	.png	10 word	Berhasil	Berhasil

Berdasarkan pengujian yang dilakukan pada Tabel 6. menunjukkan bahwa dekripsi dan extracting yang dilakukan oleh sistem berhasil dalam melakukan pengembalian pesan informasi rahasia menggunakan modifikasi teknik kriptografi cipher block chaining dan vigenere cipher yang diintegrasikan dengan teknik steganografi Least Signicant Bit (LSB). Jumlah pesan tidak ada yang berkurang maupun terpotong, pesan dapat dikembalikan tanpa ada perubahan apapun.

KESIMPULAN DAN SARAN

Berdasarkan pada pembahasan hasil dan pengujian yang telah dilakukan pada penelitian ini, dapat ditemukan beberapa hasil, yaitu:

1. Pengujian dengan visual menghasilkan secara penglihatan mata tidak adanya perbedaan pada gambar baik yang belum disisipi pesan maupun sudah.
2. Penyisipan pesan pun dilakukan untuk menguji kinerja dari kriptografi dan penyisipan pada citranya. Hasil tersebut membuktikan jika proses yang dilakukan sebanyak 25 kali menemukan keberhasilan sebanyak 18 kali dan gagal sebanyak 7 kali. Hal tersebut dipengaruhi jumlah pesan, kunci dan ukuran citra berpengaruh pada proses enkripsi dan dekripsi karena dipengaruhi oleh file gambar yang terlalu kecil *size* sekitar sampai ±10 KB dengan nilai lebar dan tinggi (dimensi) gambar yang terlalu kecil. Namun penyisipan simbol dan karakter sudah dapat dilakukan dengan metode CBC Vigenere. Ketika enkripsi gambar memiliki pengubahan *size* dan proses dekripsi teknik Steganografi *Least Significant Bit* (LSB) mampu disisipi pesan dan dapat mengembalikan pesan ke semula.

DAFTAR PUSTAKA

Abomhara, M. and Koien, G. (2015) 'Cyber Security and the *Internet* of Things : Vulnerabilities , Threats , Intruders Cyber Security and the *Internet* of Things : Vulnerabilities , Threats , Intruders', *Journal of Cyber Security*, 4(May), pp. 65–88. doi: 10.13052/jcsm2245-1439.414.

Anderson, R. (1989) 'Cryptanalytic Properties Of Short Substitution', *Taylor & Francis*, XIII(1), pp. 61–72. doi: 10.1080/0161-118991863772.

Atzori, L., Iera, A. and Morabito, G. (2010) 'The *Internet* of Things : A survey', *Computer Networks ELSEVIER*. Elsevier B.V., 54(15), pp. 2787–2805. doi: 10.1016/j.comnet.2010.05.010.

Dashti, A., Kheradmand, H. A. and Jazi, M. D. (2016) 'Comparison Of Three Modes Of Cryptography

Operation For Providing Security and Privacy Based on Important Factors', *Information Technology & Electrical Engineering*, 5(3), pp. 7–12.

Goutam, R. K. (2015) 'Importance of Cyber Security', *International Journal of Computer Applications*, 111(7), pp. 14–17.

Handoko, L. B. *et al.* (2019) 'Digital Signature Pada Citra Menggunakan Rsa Dan Vigenere Cipher Berbasis Md5', *SIMETRIS*, 10(1), pp. 357–366.

Hidayat, M. H., Gerhana, Y. A. and Syaripudin, U. (2018) 'Kombinasi Algoritme Kriptografi Vigenere Chiper dan Hill Cipher untuk Penyandian Pesan Rahasia pada Metode Steganografi', *INSIGHT*, 1(1), pp. 125–131.

Humendru, F. and Zebua, T. (2018) 'Implementation of Triple Transposition Vegenere Cipher Algorithm and Cipher Block Chaining for Encoding Text', *International Journal of Informatics and Computer Science*, 2(1), pp. 26–31.

Ijemaru, G. K. *et al.* (2018) 'Security Challenges of Wireless Communications Networks : A Survey Security Challenges of Wireless Communications Networks : A Survey', *International Journal of Applied Engineering Research*, 13(8), pp. 5680–5692.

ITU (2017) 'The world in 2017: ICT facts and figures', *International Telecomummication Union*, July.

Johnson, N. F. and Mason, G. (no date) 'Exploring Steganography: Seeing the Unseen', *IEEE, Computing Practices*, 31(2), pp. 26–34.

Kavitha *et al.* (2012) 'Steganography Using Least Signicant Bit Algorithm', *International Journal of Engineering Research and Applications (IJERA)*, 2(3), pp. 338–341.

Kester, Q. (2012) 'A Cryptosystem Based on Vigenère Cipher with Varying Key', *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1(10), pp. 108–113.

Kizza, J. M. (2013) *Guide to Computer Network Security*. Springer.

Laskar, S. A. and Hemachandran, K. (2012) 'Secure Data Transmission Using Steganography And Encryption', *International Journal on Cryptography and Information Security (IJCIS)*, 2(3), pp. 161–172. doi: 10.5121/ijcis.2012.2314.

Lestiawan, H. and Purnama, R. D. O. (2016) 'Pengamanan Dokumen Teks Menggunakan Algoritme Kriptografi Mode Operasi Cipher Block Chaining (CBC) Dan Steganografi Metode End Of File (EOF)', *Techno.com*, 15(1), pp. 22–31.

Li, B. *et al.* (2011) 'A Survey on Image Steganography and Steganalysis', *Journal of Information Hiding and Multimedia Signal Processing*, 2(2), pp. 142–172.

Maruf, F., Riadi, I. and Prayudi, Y. (2015) 'Merging of Vigenére Cipher with XTEA Block Cipher to Encryption Digital Merging of Vigenére Cipher with XTEA Block Cipher to Encryption Digital Documents', *International Journal of Computer Applications*, 132(1), pp. 27–33. doi: 10.5120/ijca2015907262.

Permana, A. A. (2018) 'Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode', *Jurnal Al-Azhar Indonesia Seri Sains Dan Teknologi*, 4(3), pp. 110–115.

Raphael, A. J. and Sundaram, D. V. (2010) 'Cryptography and Steganography – A Survey', *Int. J. Comp. Tech. Appl*, 2(3), pp. 626–630.

Senthil, K., Prasanthi, K. and Rajaram, R. (2013) 'A Modern Avatar of Julius Ceasar and Vigenere Cipher', *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 13–15. doi: 10.1109/ICCIC.2013.6724170.

Sinkov, A. (2009) *Elementary Cryptanalysis: A Mathematical Approach*. Second Edi. United States of America: The Mathematical Association of Amerika.

Song, S. *et al.* (2011) 'A Novel Secure Communication Protocol Combining Steganography and Cryptography', *Elsevier Inc, Advanced in Control Engineering and Information Science*, 15, pp. 2767–2772. doi: 10.1016/j.proeng.2011.08.521.

Syawal, M. F., Fikriansyah, D. C. and Agani, N. (2016) 'Implementasi Teknik Steganografi Menggunakan

Algoritme Vigenere Cipher Dan Metode LSB', *Jurnal TICOM*, 4(3), pp. 91–99.

Taneja, M. (2013) 'An Analytics Framework to Detect Compromised IoT Devices using Mobility Behavior', *International Conference on ICT Convergence (ICTC) IEEE*, pp. 38–43.

Tiwari, A., Yadav, S. R. and Mittal, N. K. (2014) 'A Review on Different Image Steganography Techniques', *International Journal of Engineering and Innovative Technology (IJEIT)*, 3(7), pp. 121–124.

Wikibooks (2020) *Visual Basic for Applications*.

Zebua, T. (2015) 'Pengamanan Data Teks Dengan Kombinasi Cipher Block Chaining dan LSB-1', *Seminar Nasional Inovasi dan Teknologi (SNITI)*, 2015(September), pp. 85–89. Available at: sniti.info.

Zou, Y. *et al*. (2016) 'A Survey on Wireless Security : Technical Challenges , Recent Advances , and Future Trends', *Proceedings of the IEEE*, 104(9), pp. 1727–1765.