

Modifikasi Headstega Berdasarkan Penyisipan Karakter

Hasmawati^{#1}, Ari Moesriami Barmawi^{#2}

*# School of Computing, Telkom University
Jl. Telekomunikasi No. 1, Terusan Buah Batu Bandung 40257 Indonesia*

¹hasmawati@telkomuniversity.ac.id

²mbarmawi@melsa.net.id

Abstract

Head steganography or Headstega is one of noiseless steganography paradigm, or Nostega. This method utilizes the email header as a media of message concealment. There are several problems that can be enhanced in Headstega, i.e. low embedding capacity and high level of suspicion. Modified Headstega based on Character Hiding uses a combination of consonant vowel to embed the secret messages into email address. The messages embedding process using four consonant vowel combination that represented one character in Indonesian language. From the experiments conducted, the results obtained that the Modified Headstega has a better performance than the Original Headstega in term of embedding capacity. Modified Headstega allows to conceal more than one character in one email address. In other words an email address consists of one or more patterns of consonant and vocal combinations. While in the previous method one email address is only able to conceal one character because each character is only represented in the first letter of the email address. In addition Modified Headstega does not cause suspicion because the cover used is the existing cover so it is not generated from the message. In contrast to the Headstega, because the cover used is generated from the message so that the pattern of the resulting cover may cause suspicion.

Keyword : Steganography, Nostega, Headstega, Character Hiding

Abstrak

Head-Steganography atau Headstega adalah salah satu metodologi steganografi yang berbasis *noiseless* atau Nostega. Metode ini memanfaatkan *header* email sebagai media penyembunyian pesan rahasia. Metode Headstega memiliki kekurangan yaitu kapasitas penyembunyian pesan yang rendah dan tingkat kecurigaan yang tinggi. Modifikasi Headstega berdasarkan penyembunyian karakter menggunakan kombinasi konsonan vokal untuk menyembunyikan pesan rahasia pada alamat email. Proses penyembunyian pesan menggunakan kombinasi empat karakter konsonan vokal yang mewakili satu karakter alfabet dalam Bahasa Indonesia. Dari percobaan yang dilakukan, hasil yang diperoleh menunjukkan bahwa metode yang diusulkan memiliki kapasitas penyisipan pesan yang lebih baik dari metode sebelumnya. Metode Modifikasi Headstega memungkinkan untuk menyisipkan lebih dari satu karakter dalam satu alamat email dengan kata lain satu alamat email terdiri dari satu atau lebih pola empat kombinasi konsonan dan vokal. Sementara pada metode sebelumnya satu alamat email hanya mampu menyisipkan satu karakter pesan karena setiap karakter pesan hanya direpresentasikan pada huruf pertama dari alamat email. Selain itu metode Modifikasi Headstega tidak menimbulkan kecurigaan karena *cover* yang digunakan adalah *cover*

yang *existing* sehingga tidak dihasilkan dari pesan. Berbeda dengan metode Headstega, dimana *cover* yang digunakan dihasilkan dari pesan sehingga pola dari *cover* yang dihasilkan dapat menimbulkan kecurigaan.

Kata kunci: Steganography, Nostega, Headstega, Penyembunyian Karakter

I. PENDAHULUAN

Untuk berbagai alasan dan keperluan orang perlu untuk berbagi informasi maupun berkomunikasi dengan orang lain. Disisi lain, informasi adalah hal yang sangat bernilai bagi setiap orang. Oleh karena itu, melindungi informasi dari pihak yang tidak bertanggung jawab menjadi hal yang sangat penting. Penyembunyian informasi dapat dilakukan salah satunya adalah menggunakan metode steganografi. Steganografi merupakan salah satu metode penyembunyian pesan rahasia berupa teks, gambar maupun video kedalam media lain. Pesan rahasia tidak dapat dideteksi kecuali dengan penerima yang dimaksudkan. Ide utama dari steganografi adalah bahwa pesan rahasia tertanam didalam *cover* sedemikian sehingga *cover* yang menyembunyikan pesan rahasia terlihat seperti *cover* yang asli. Steganografi terdiri dari dua jenis yaitu steganografi *noisy* dan *noiseless*. Konsep dasar dari steganografi *noisy* adalah dengan mengubah bit dari *cover* yang digunakan. Proses perubahan tersebut akan menghasilkan *noise* sehingga akan menimbulkan kecurigaan [1]. Sementara konsep dari steganografi *noiseless* adalah tidak mengubah bit dari *cover* yang digunakan, sehingga *cover* terlihat seperti *cover* asli. Pada 2010, Desoky mengusulkan beberapa metode berbasis steganografi *noiseless*, diantaranya adalah Listega atau List-based steganography, Headstega atau Header Steganography, Edustega, Graphstega atau Graph based steganography, Chestega atau Chess based steganography, dll. Salah satu metode pada steganografi *noiseless* adalah Headstega. Headstega menyembunyikan pesan pada *header* email yaitu pada alamat email [2].

Frekuensi penggunaan email sebagai media komunikasi menjadi motivasi utama dari Headstega untuk memanfaatkan alamat email sebagai media pembawa pesan rahasia. Headstega memiliki kapasitas penyembunyian pesan yang rendah, karena untuk menyembunyikan satu karakter ASCII diperlukan dua alamat email. Selain itu Headstega memiliki tingkat kecurigaan yang tinggi, karena alamat email yang digunakan dihasilkan berdasarkan pesan rahasia yang akan disembunyikan. Metode yang diusulkan menggunakan kombinasi konsonan vokal untuk menyembunyikan pesan rahasia pada alamat email. Menurut standar RFC (Request For Comment) struktur dari alamat email terdiri dari dua bagian, yaitu bagian lokal (sebelum tanda @) dan bagian domain (setelah tanda @) [8]. Pada penelitian ini, pesan rahasia disembunyikan pada bagian lokal alamat email (sebelum tanda @). Proses penyembunyian pesan menggunakan kombinasi empat karakter konsonan vokal. Satu pola kombinasi konsonan vokal mewakili satu karakter atau satu alfabet dalam Bahasa Indonesia. Dari hasil percobaan, metode yang diusulkan memiliki kapasitas penyisipan pesan yang lebih baik dari metode sebelumnya dan juga dapat mereduksi tingkat kecurigaan.

Untuk menghindari kecurigaan, format alamat email dan proses pengiriman email sesuai standar internasional dari RFC (*Request For Comment*). RFC atau request for comment adalah standar internasional yang mengatur format, sintaks dari suatu pesan yang dikirim antar pengguna komputer menggunakan protokol elektronik email [8]. Menurut RFC, maksimum penerima dalam satu pengiriman email adalah 100 alamat email, termasuk didalamnya kombinasi dari CC dan BCC.

II. PENELITIAN TERKAIT

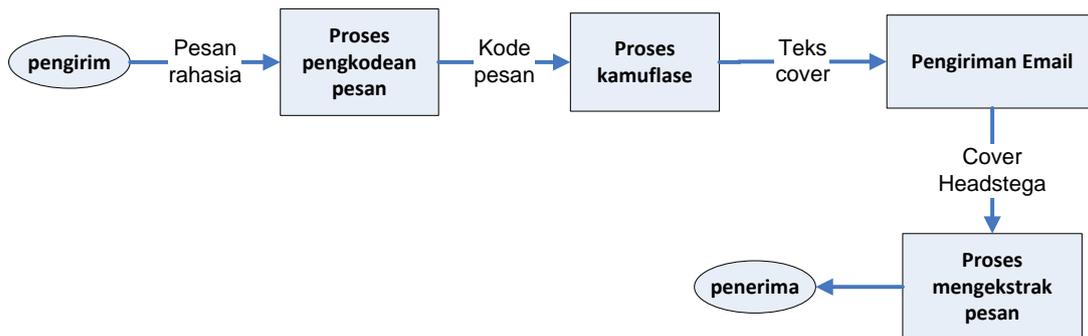
A. HEADSTEGA

Headstega memanfaatkan *header* email sebagai media pembawa pesan rahasia. Headstega diperkenalkan oleh Abderahman Desoky pada 2010. Headstega menyisipkan pesan rahasia pada karakter pertama dari alamat email berdasarkan kode steganografi [1]. Sebagai contoh, jika huruf pertama dari alamat email adalah huruf “H”, maka alamat email ini menyimpan kode steganografi yaitu “0111”. Kode steganografi dari Headstega ditunjukkan pada Tabel 1.

Tabel 1. Kode steganografi Headstega [3].

NO	Biner	Huruf	NO	Biner	Huruf
1	0000	A	14	1101	N
2	0001	B	15	1110	O
3	0010	C	16	1111	P
4	0011	D	17	0000	Q
5	0100	E	18	0001	R
6	0101	F	19	0010	S
7	0110	G	20	0011	T
8	0111	H	21	0100	U
9	1000	I	22	0101	V
10	1001	J	23	0110	W
11	1010	K	24	0111	X
12	1011	L	25	1000	Y
13	1100	M	26	1001	Z

Headstega terdiri dari tiga modul yaitu modul pengkodean pesan, modul kamufase dan modul ekstraksi pesan. Secara rinci dapat dilihat pada Gambar 1.



Gambar 1. Arsitektur Headstega [3]

Modul pertama dari arsitektur Headstega adalah modul pengkodean pesan. Pada modul ini akan ditentukan parameter yang akan digunakan untuk mengkodekan pesan kemudian mendefinisikan kode steganografi berdasarkan parameter yang dipilih. Dengan kata lain proses untuk menentukan pengelompokan bit pesan apakah dikelompokkan menjadi 4 bit, 2 bit atau lainnya. Modul kedua dari arsitektur Headstega adalah modul

kamuflase. Modul ini akan menghasilkan *cover* yang akan digunakan untuk menyisipkan pesan. Misalnya, jika empat bit yang akan disisipkan adalah "0111" yang merepresentasikan huruf H atau X, maka *cover* (alamat email) yang dihasilkan berlawanan huruf H atau X. Modul terakhir adalah modul ekstraksi pesan. Pada modul ini alamat email akan diekstrak untuk mendapatkan pesan rahasia. Sebagai contoh, alamat email yang diterima adalah "hasmawati@test.xyz", "Erisdian@test.xyz". Alamat email ini akan diekstrak berdasarkan kode steganografi. Karena karakter pertama dari alamat email menyimpan 4 bit kode steganografi (kode steganografi ditampilkan pada Tabel 1), maka huruf H pada "hasmawati@test.xyz" menyimpan kode "0111" dan huruf E pada "Erisdian@test.xyz" menyimpan kode "0100". Jika masing – masing dari 4 bit ini digabungkan maka akan diperoleh 8 bit yaitu "01110100" yang senilai dengan 116 kode ASCII dan merepresentasikan huruf "t" dalam karakter ASCII.

B. LISTEGA

Listega atau List steganografi adalah salah satu metode steganografi berbasis *noiseless* atau Nostega. Metode Listega menyisipkan pesan rahasia kedalam karakter pertama dari item list untuk menghasilkan *cover*. Konsep dasar metode Listega adalah penyamaran data kedalam list/daftar barang misalnya list buku, list musik, list peralatan komputer dll. Arsitektur Listega terdiri dari Empat modul yaitu modul penentuan domain, modul pengkodean pesan, modul kamuflase pesan dan protocol komunikasi [6].

Modul pertama dari Listega adalah modul penentuan domain. Modul ini mendefinisikan domain yang sesuai untuk mencapai tujuan steganografi. Salah satu faktor utama untuk menggunakan domain tertentu adalah penggunaan daftar. Misalnya bisnis online yang menggunakan rincian list/daftar item seperti daftar buku, daftar komponen computer, daftar CD musik, daftar DVD film dll. Modul kedua adalah modul pengkodean pesan. Pada modul ini akan ditentukan parameter yang akan digunakan untuk mengkodekan pesan kemudian mendefinisikan kode steganografi berdasarkan parameter yang dipilih. Dengan kata lain proses untuk menentukan pengelompokan bit pesan apakah dikelompokkan menjadi 4 bit, 2 bit atau lainnya. Modul ketiga dari arsitektur Listega adalah modul kamuflase. Modul ini akan menghasilkan list *cover* yang akan digunakan untuk menyisipkan pesan. Modul keempat adalah modul protocol komunikasi. Modul ini mendefinisikan bagaimana pengirim dan penerima berkomunikasi secara diam-diam, mencakup protokol rahasia untuk mengirimkan daftar list *cover* ke penerima yang dimaksud dan mendefinisikan skema bagaimana ekstraksi pesan untuk mengungkap pesan tersembunyi.

C. LIST STEGANOGRAPHY BASED ON SYLLABLE PATTERNS

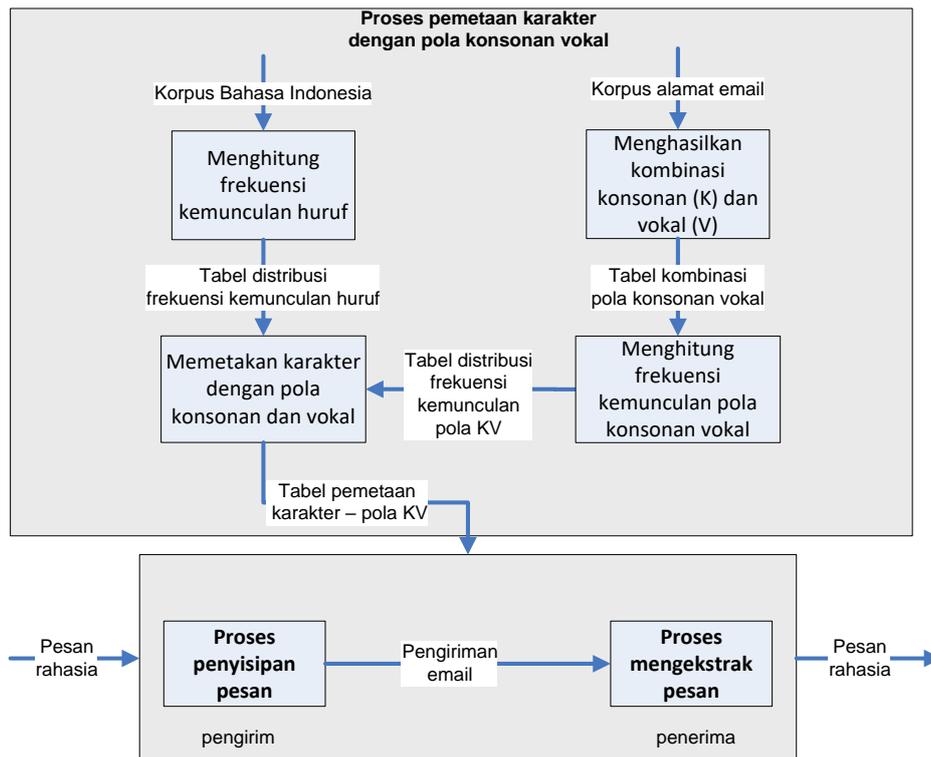
Beberapa permasalahan pada Listega, yaitu kapasitas penyisipan yang kecil, rentan menimbulkan kecurigaan yang tinggi karena hanya memakai item list yang tersisipi dan kurang tahan terhadap *noise* [7]. Penelitian lanjut dilakukan untuk mengatasi permasalahan pada Listega dengan mengusulkan metode Steganografi List berbasis pola suku kata. Konsep dasar dari metode ini adalah penggunaan pola suku kata untuk menyisipkan pesan kedalam sebuah *cover* [7]. Dalam hal ini, list ulang tahun karyawan digunakan sebagai *cover*. Inovasi lain yang dituangkan dalam riset ini adalah sebuah algoritma untuk menghasilkan list *cover* tak terfilter, yakni list *cover* yang mengandung item list yang tersisipi dan yang tidak tersisipi. Hal ini dilakukan untuk mengurangi kecurigaan pihak lain. Metode ini dapat diterapkan dalam berbagai bahasa. Hasil eksperimen dari metode ini menunjukkan hasil yang lebih baik dari metode sebelumnya, dimana kapasitas penyisipan pesan yang lebih tinggi dibandingkan metode sebelumnya.

III. METODOLOGI PENELITIAN

Modifikasi headstega berdasarkan penyisipan karakter memanfaatkan metode penyisipan karakter pada alamat email. Untuk mengimplementasikan metode ini, korpus alamat email dari salah satu perusahaan digunakan dengan jumlah kurang lebih 4.469 alamat email. Alamat email ini akan diproses sedemikian sehingga akan diperoleh kombinasi konsonan vokal dari alamat email berikut frekuensinya.

Pesan rahasia ditulis dalam Bahasa Indonesia dan hanya menggunakan karakter alfabet dan beberapa karakter spesial seperti titik, koma, dan spasi.

Arsitektur dari modifikasi headstega berdasarkan penyisipan karakter terdiri dari tiga proses yaitu proses pemetaan karakter dengan pola konsonan vokal alamat email, proses penyisipan pesan dan proses mengekstrak pesan. Detail dari metode ini dapat dilihat pada Gambar 2.



Gambar 2. Arsitektur modifikasi headstega berdasarkan penyisipan karakter.

1. Proses pemetaan karakter dengan pola konsonan vokal alamat email

Proses ini dilakukan untuk memetakan karakter dari Bahasa Indonesia dengan pola konsonan vokal alamat email. Pemetaan karakter dilakukan berdasarkan frekuensi kemunculan karakter dalam Bahasa Indonesia dan frekuensi kemunculan pola konsonan vokal dari alamat email. Oleh karena itu perlu dilakukan perhitungan distribusi kombinasi konsonan vokal dari alamat email dan distribusi kemunculan karakter dalam korpus Bahasa Indonesia. Sebelum melakukan perhitungan kombinasi konsonan vokal, terlebih dahulu dilakukan pengolahan data alamat email untuk mengetahui panjang rata-rata karakter pada bagian lokal alamat email. Berdasarkan hasil pengolahan data tersebut, diperoleh hasil bahwa panjang karakter bagian lokal alamat email terdiri dari 4 – 17 karakter. Oleh karena itu, pola kombinasi konsonan vokal adalah menggunakan 4 karakter.

Distribusi dari kombinasi konsonan vokal diperoleh dengan menghitung rata-rata jumlah kemunculan dari setiap pola kombinasi konsonan vokal dari alamat email. Sementara distribusi karakter dalam Bahasa Indonesia diperoleh dengan menghitung frekuensi kemunculan karakter dalam korpus Bahasa Indonesia. Hasil dari distribusi frekuensi kemunculan karakter dan distribusi kemunculan pola konsonan vokal dari alamat email dapat dilihat pada Tabel 2.

Tabel 2 . (a). Distribusi kemunculan pola kombinasi konsonan vokal alamat email
 (b) Distribusi kemunculan karakter dari korpus Bahasa Indoensia

NO	Pola kombinasi konsonan vokal	Prosentase kemunculan	No	Huruf	Prosentase kemunculan	No	Huruf	Prosentase kemunculan
1	KVKV	19,39%	1	A	18,12%	17	O	2,00%
2	VKVK	16,51%	2	N	10,14%	18	Y	1,35%
3	KVKK	14,33%	3	E	8,66%	19	KOMA	1,27%
4	KKVK	13,74%	4	I	7,64%	20	J	0,93%
5	VKKV	13,42%	5	R	5,80%	21	TITIK	0,81%
6	KVVK	4,43%	6	T	5,12%	22	C	0,53%
7	VKKK	3,88%	7	K	4,72%	23	SPASI	0,38%
8	KKKV	3,61%	8	S	4,56%	24	W	0,36%
9	VKVV	2,46%	9	U	4,51%	25	F	0,31%
10	VVKV	2,16%	10	M	4,27%	26	V	0,15%
11	KKVV	2,16%	11	D	3,71%	27	Z	0,04%
12	VVKK	1,93%	12	P	3,53%	28	Q	0,01%
13	KKKK	1,54%	13	G	3,28%	29	X	0,01%
14	KVVV	0,22%	14	L	3,06%			
15	VVVK	0,20%	15	B	2,66%			
16	VVVV	0,02%	16	H	2,07%			

(a)

(b)

Berdasarkan Tabel 2 (a) dan (b), distribusi karakter dari Bahasa Indonesia kemudian dipasangkan dengan distribusi pola kombinasi konsonan vokal dari alamat email, sedemikian sehingga karakter dengan frekuensi kemunculan tertinggi dipasangkan dengan pola kombinasi konsonan vokal dengan frekuensi tertinggi. Karena hanya terdapat 16 pola kombinasi konsonan vokal yang dihasilkan dari proses pengolahan korpus alamat email, sementara jumlah karakter yang akan dipasangkan terdiri dari 26 alfabet dan 3 karakter spesial, maka satu pola kombinasi konsonan vokal dipasangkan dengan dua karakter dari korpus Bahasa Indonesia. Karakter dengan frekuensi kemunculan tertinggi dipetakan dengan karakter yang memiliki frekuensi rendah dengan tetap memperhatikan frekuensi kemunculan pasangan dua karakter ini dalam korpus Bahasa Indonesia. Sedemikian sehingga pasangan dua karakter ini tidak menimbulkan ambigu pada saat merepresentasikan pesan rahasia. Hasil dari proses ini dapat dilihat pada Tabel 3.

Tabel 3. Pasangan karakter dalam Bahasa Indonesia dengan pola kombinasi konsonan vokal dari alamat email

NO	Pola kombinasi konsonan vokal	Karakter
1	KVKV	A atau X
2	VKVK	SPASI atau V
3	KVKK	N atau H
4	KKVK	E atau Q

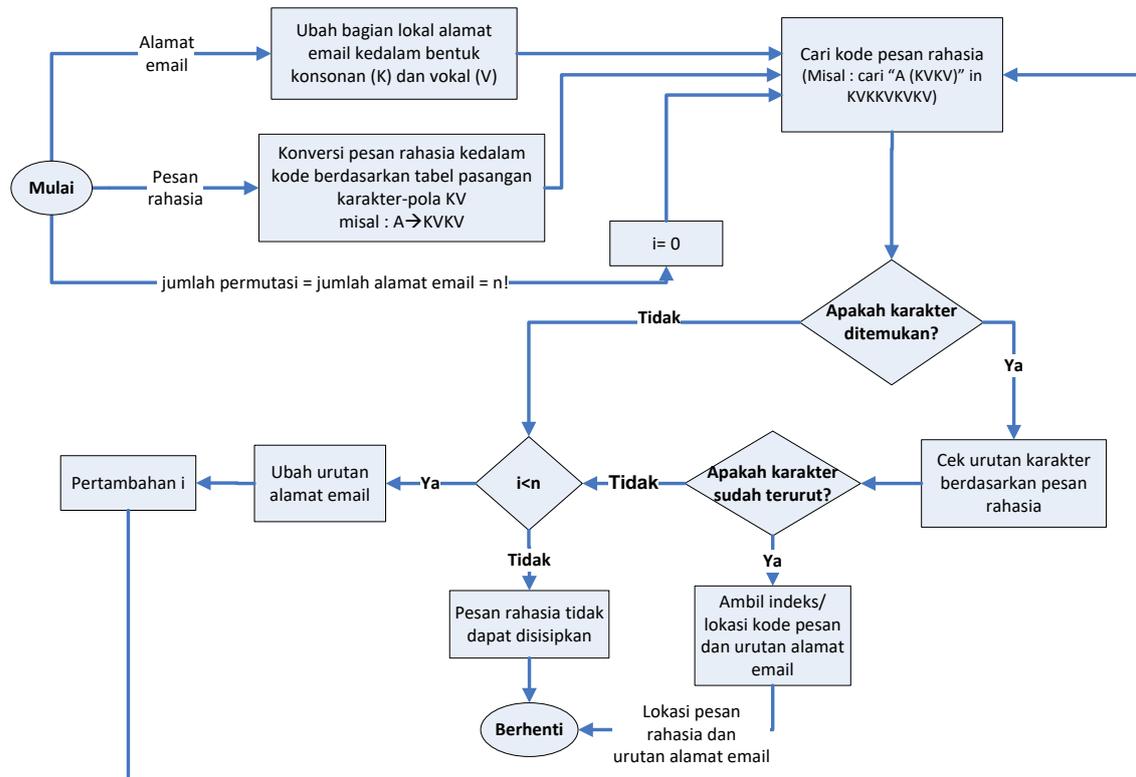
5	VKKV	I
6	KVVK	R atau Y
7	VKKK	T atau Z
8	KKKV	K atau F
9	VKVV	S atau J
10	VVKV	U atau O
11	KKVV	M atau G
12	VVKK	D atau L
13	KKKK	P atau B
14	KVVV	C
15	VVVK	W
16	VVVV	KOMA, TITIK

2. Proses penyisipan pesan

Dalam proses ini, pesan rahasia akan disisipkan kedalam alamat email berdasarkan pola konsonan vokal alamat email. Algoritma dari proses penyisipan pesan adalah sebagai berikut :

1. Pertama – tama pesan rahasia dikonversi menjadi pola konsonan vokal yang terdiri atas 4 karakter berdasarkan tabel pemetaan karakter dengan pola kombinasi konsonan vokal (tabel 3.)
2. Bagian lokal dari alamat email (sebelum tanda @) dikonversi menjadi konsonan dan vokal.
3. Dimisalkan total permutasi alamat email adalah sama dengan jumlah alamat email yang akan digunakan untuk menyisipkan pesan = $n!$.
4. Cari kode dari pesan rahasia dalam pola konsonan vokal alamat email
 - i. Jika kode pesan ditemukan, maka periksa urutan dari kode pesan apakah telah sesuai dengan urutan karakter dalam pesan rahasia.
 - a. Jika seluruh karakter pesan sudah terurut, maka indeks atau lokasi dari setiap karakter pesan dan urutan dari alamat email akan disimpan dan proses penyisipan pesan selesai.
 - b. Jika karakter pesan belum terurut, maka periksa jumlah permutasi. Jika masih terdapat kemungkinan permutasi (jumlah permutasi kurang dari total permutasi), maka ubah urutan alamat email kemudian ulangi kembali untuk mencari kode pesan dalam konsonan vokal alamat email. Jika seluruh permutasi sudah dilakukan, maka pesan rahasia ini tidak dapat disisipkan kedalam alamat email..
 - ii. Jika kode pesan tidak ditemukan, maka periksa jumlah permutasi. Jika masih terdapat kemungkinan permutasi (jumlah permutasi kurang dari total permutasi), maka ubah urutan alamat email kemudian ulangi kembali untuk mencari kode pesan dalam konsonan vokal alamat email. Jika seluruh permutasi sudah dilakukan, maka pesan rahasia ini tidak dapat disisipkan kedalam alamat email.

Detail dari proses penyisipan pesan dapat dilihat pada Gambar 3.



Gambar 3. Proses penyisipan pesan

Contoh proses penyisipan pesan adalah sebagai berikut :

Dimisalkan pesan rahasia yang akan disisipkan adalah kata “SKENARIO”. Kata skenario ini jika dikonversi kedalam pola konsonan vokal maka diperoleh hasil sebagai berikut :

S → VKVV, K → KKKV, E → KKVK, N → KVKK, A → KVKV, R → KVVK, I → VKKV, O → VVKV

Dengan menggunakan algoritma penyisipan pesan, pesan rahasia “SKENARIO” dapat disisipkan kedalam alamat email seperti yang diperlihatkan pada Tabel 4.

Tabel 4. Contoh proses penyisipan pesan.

Urutan alamat email sebelum penyisipan pesan	Alamat email	Pola konsonan vokal alamat email	Proses penyisipan pesan	Informasi tentang lokasi pesan
1	shaufiah@gmail.com	KKVVKVVK	CKV ^S VKVVKVKVKV ^K KKKVK ^E KKVK ^N K VKK ^A KVKV ^R KVV ^I KVKVKVKVKV ^I VKKVK	- Jarak antara satu pola dengan lainnya
2	rimbawh@gmail.com	KVKKVKK	KVKVKV ^O VVKVKVKVKV	3, 6, 1, 0, 0, 8, 8
3	mediana.kancana@gmail.com	KVKVVVKVKVKV V	sha ^S ufiah@gmail.com,	- Urutan alamat email setelah proses penyisipan pesan :
4	febryantisthevanie@yahoo.com	KVKKKVKVKKKVK VKVV	rimba ^K wh@gmail.com, feb ^E ryan ^N tist ^A heva ^R nie@yahoo.co	

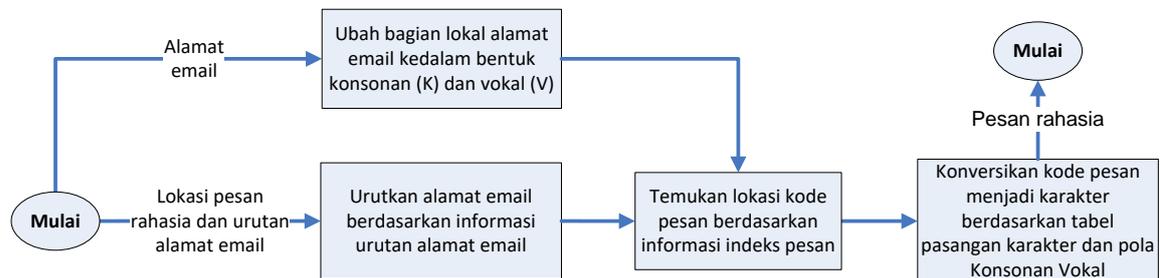
5	danakusumo@telkomuniversity.ac.id	KVKVKVKVKV	m, danakusum ^o @telkomuniversity.ac.id	1, 2, 6, 3, 4, 5
6	mbarmawi@melsa.net.id	KKVKVKVKV	, mbarmawi@melsa.net.id, med ^o iana.kancana@gmail.com	

3. Proses mengekstrak pesan

Proses ini merupakan proses utama dalam arsitektur modifikasi headstega. Dalam proses ini, alamat email yang diterima akan diekstrak untuk mendapatkan pesan rahasia yang dikirimkan. Dengan menggunakan tabel pasangan karakter dan pola kombinasi konsonan vokal (Tabel 3), dan mengetahui informasi lokasi pesan dan urutan alamat email, maka pesan rahasia dapat diekstrak kembali. Algoritma dari proses mengekstrak pesan adalah sebagai berikut :

1. Pertama-tama, bagian lokal alamat email akan dikonversi menjadi konsonan dan vokal.
Contoh : alamat email : hasmawati@telkomuniversity.ac.id → hasmawati → KVKKKVKVKV
2. Berdasarkan informasi lokasi pesan dan urutan alamat email yang diterima penerima, selanjutnya cari kode pesan tersebut dalam konsonan vokal alamat email.
3. Setelah itu, konversikan kode pesan kedalam karakter berdasarkan tabel pasangan karakter – pola konsonan vokal (Tabel 3). Pada akhirnya pesan rahasia dapat diekstrak.

Detail dari proses mengekstrak pesan rahasia dapat dilihat pada Gambar 4. Sementara contoh proses mengekstrak pesan dapat dilihat pada Tabel. 5



Gambar 4. Proses mengekstrak pesan

Tabel 5. Contoh proses mengekstrak pesan

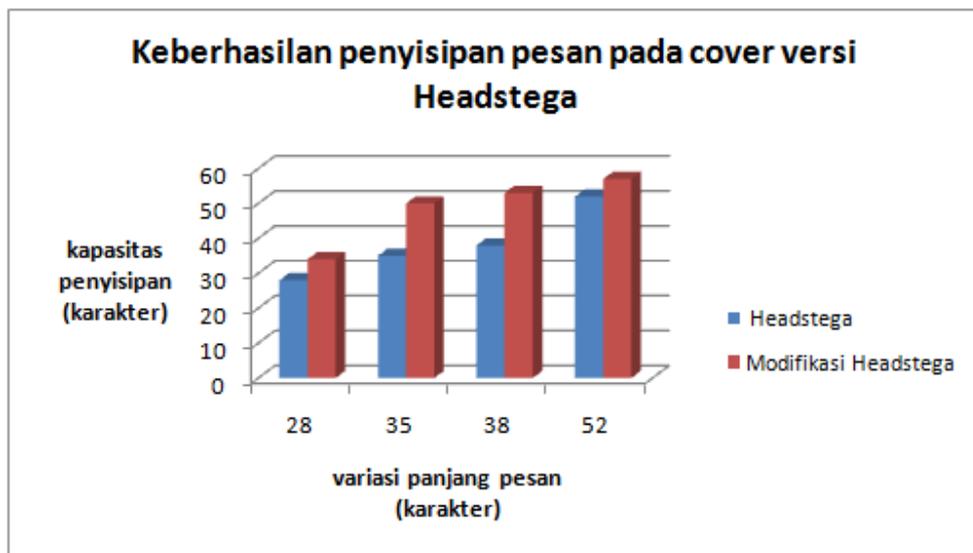
Alamat email	Informasi tentang pesan	Urutan alamat email sesuai urutan setelah pesan di encode	Pola konsonan vokal (bagian lokal) alamat email	Pesan rahasia
shaufiah@gmail.com	- Urutan alamat email setelah proses penyisipan pesan : 1, 2, 6, 3, 4, 5 - Jarak antara satu pola dengan lainnya : 3, 6, 1, 0, 0, 0, 8, 8	shaufiah@gmail.com,	CCV ^S VCVVCCVCCV ^K CCC VC ^E CCVC ^N CVCC ^A CVCV ^R CVVCVCVCVCVC ^I VCCVC CVVCVC ^O VVCVCVCCV CV	SKENARIO
rimbawh@gmail.com		rimbawh@gmail.com,		
mediana.kancana@gmail.com		febryantisthevanie@yahoo.com,		
febryantisthevanie@yahoo.com		danakusumo@telkomuniversity.ac.id, mbarmawi@melsa.net.id, mediana.kancana@gmail.		

danakusumo@telkomuniversity.ac.id		com		
mbarmawi@melsa.net.id				

IV. HASIL DAN DISKUSI

Terdapat dua percobaan utama yang dilakukan untuk membandingkan performansi dari metode Headstega dan metode Modifikasi Headstega, yaitu : percobaan penyisipan pesan menggunakan cover versi Headstega dan percobaan penyisipan pesan menggunakan cover versi modifikasi headstega.

1. Percobaan menggunakan *cover* versi Headstega.
Tujuan dari percobaan ini adalah untuk melihat kemampuan dari metode Modifikasi Headstega dalam menyisipkan pesan jika *cover* yang digunakan adalah *cover* yang dihasilkan oleh metode Headstega. Skenario yang dilakukan pada percobaan ini adalah menggunakan *cover* yang dihasilkan oleh metode Headstega untuk menyisipkan pesan menggunakan metode Headstega dan metode Modifikasi Headstega dengan beberapa variasi panjang pesan.



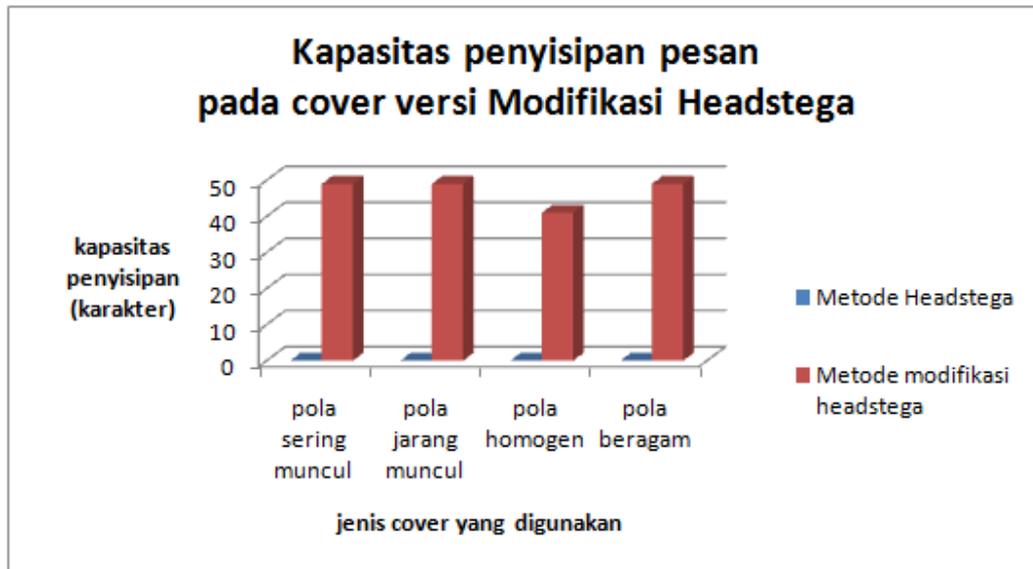
Gambar 5. Hasil percobaan menggunakan *cover* versi Headstega

Gambar 5 menunjukkan bahwa metode Modifikasi Headstega mampu menyisipkan seluruh pesan meskipun *cover* yang digunakan adalah *cover* yang dihasilkan oleh metode Headstega. Dengan menggunakan *cover* yang sama, metode Modifikasi Headstega mampu menyisipkan pesan lebih dari panjang pesan yang dapat disisipkan oleh metode Headstega. Kondisi ini terjadi karena dengan menggunakan metode Modifikasi Headstega, satu alamat email mampu menyisipkan lebih dari satu karakter sementara pada metode Headstega, satu alamat email hanya mampu menyisipkan 4 bit dari 8 bit karakter ASCII.

2. Percobaan menggunakan *cover* versi Modifikasi Headstega
Tujuan dari percobaan ini adalah untuk membandingkan kemampuan penyisipan pesan dari metode Headstega dan metode Modifikasi Headstega jika *cover* yang digunakan adalah *cover* versi metode Modifikasi Headstega. Ada empat skenario yang digunakan dalam percobaan ini. Yang pertama adalah menyisipkan pesan kedalam *cover* yang memiliki pola konsonan vokal dengan frekuensi kemunculan yang tinggi. Skenario kedua adalah menyisipkan pesan kedalam *cover* yang memiliki pola konsonan vokal dengan frekuensi yang rendah. Skenario ketiga adalah menyisipkan pesan kedalam *cover* yang memiliki pola konsonan vokal yang homogen. Skenario keempat adalah menyisipkan pesan kedalam

cover yang memiliki pola konsonan vokal yang beragam. Dengan menggunakan panjang pesan dan *cover* yang sama, kapasitas kedua metode yaitu Headstega dan Modifikasi Headstega dibandingkan.

Hasil dari percobaan menggunakan *cover* versi Modifikasi Headstega dapat dilihat pada Gambar 6.



Gambar 6. Hasil percobaan penyisipan pesan menggunakan *cover* versi Modifikasi Headstega

Gambar 6 menunjukkan bahwa metode Headstega tidak mampu untuk menyisipkan pesan jika *cover* yang digunakan adalah *cover* versi Modifikasi Headstega. Hal ini terjadi karena *cover* yang digunakan tidak dihasilkan dari pesan. Sehingga kapasitas penyisipan pesan dari metode Headstega sangat bergantung pada karakter pertama dari *cover* versi Modifikasi Headstega. Dikarenakan karakter pertama dari *cover* ini tidak sesuai dengan kode pesan pada Headstega maka metode Headstega tidak dapat menyisipkan pesan rahasia. Sementara metode Modifikasi Headstega mampu menyisipkan seluruh karakter pesan. Panjang karakter pesan dalam percobaan ini adalah 52 karakter. Dari hasil percobaan diperoleh bahwa metode Modifikasi Headstega mampu menyisipkan 49 karakter pada kondisi dimana *cover* yang digunakan memiliki pola konsonan vokal dengan frekuensi tinggi. Hasil yang sama diperoleh pada kondisi dimana *cover* yang digunakan adalah *cover* yang memiliki pola konsonan vokal dengan frekuensi rendah dan beragam. Sementara kondisi lain, pada *cover* dengan pola konsonan vokal yang beragam, metode Modifikasi Headstega hanya mampu menyisipkan 41 karakter dari 52 karakter pesan. Hasil percobaan ini menunjukkan bahwa metode Modifikasi Headstega memiliki performansi yang lebih baik dibandingkan dengan metode Headstega dalam hal kapasitas penyisipan pesan.

V. KESIMPULAN

Berdasarkan hasil eksperimen dapat disimpulkan bahwa metode Modifikasi Headstega memiliki kapasitas penyisipan pesan yang lebih baik dibandingkan metode Headstega. Kondisi ini terjadi karena metode Modifikasi Headstega memungkinkan untuk menyisipkan lebih dari satu karakter dalam satu alamat email dengan kata lain satu alamat email terdiri dari satu atau lebih pola empat kombinasi konsonan dan vokal. Sementara pada metode sebelumnya satu alamat email hanya mampu menyisipkan satu karakter pesan karena setiap karakter pesan hanya direpresentasikan pada huruf pertama dari alamat email.

Selain itu metode Modifikasi Headstega tidak menimbulkan kecurigaan karena *cover* yang digunakan adalah *cover* yang *existing* sehingga tidak dihasilkan dari pesan. Berbeda dengan metode Headstega, dimana *cover* yang digunakan dihasilkan dari pesan sehingga pola dari *cover* yang dihasilkan dapat menimbulkan kecurigaan.

DAFTAR PUSTAKA

- [1] Abdelrahman Desoky. Nostega: a novel noiseless steganography paradigm. *Journal of Digital Forensic Practice*, 2(3):132_139, 2008.
- [2] Abdelrahman Desoky. *Noiseless steganography: The key to covert communications*. CRC Press, 2012.
- [3] Abdelrahman Desoky. Headstega: e-mail-headers-based steganography methodology. *International Journal Electronic Security and Digital Forensics*, 3(4):289_310, 2010.
- [4] Agarwal, M., "Text steganographic approaches: a comparison", *International Journal of Network Security & Its Applications (IJNSA)*, Vol.5, No.1, January 2013.
- [5] Thampi, S. M., "Information hiding techniques: a tutorial review", *ISTE-STTP on Network Security & Cryptography*, LBSCE, 2004.
- [6] Desoky, A., "Listega: list-based steganography methodology", *Int. J. Inf. Secur.* 8, 4 (August 2009), 247-261, 2009.
- [7] David Martin, Ari Moesriami Barmawi. *List Steganography Based on Syllable Patterns*. The 5th International Conference on Electrical Engineering and Informatics 2015, 2015.
- [8] Standard for the format of arpa internet text messages. rfc 821, rfc 822, rfc 2822, rfc 2821. <https://www.ietf.org/rfc.1992>.
- [9] Application techniques for checking and transformation of names, rfc 3696. <https://tools.ietf.org/pdf/rfc3696.pdf>.
- [10] *Corpus Bahasa Indonesia*, Universitas Indonesia tahun 2016.
- [11] Indonesian Department of Education, "Kamus besar bahasa Indonesia" (The Great Dictionary of Indonesian Language), Fourth Edition, Gramedia Pustaka Utama Publisher, 2008.