SISTEM KEAMANAN PADA PENGIRIMAN DATA INFORMASI DINI TSUNAMI BERBASIS ANDROID PADA PIHAK BERWENANG SECARA NASIONAL

SECURITY SYSTEM IN SENDING TSUNAMI DATA EARLY INFORMATION BASED ON ANDROID TO NATIONAL AUTHORITIES

Wiko Setyonegoro
Pusat Penelitian dan Pengembangan Badan Meteorologi Klimatologi dan Geofisika
*e-mail***:** wiko.setyonegoro@bmkg.go.id
Ryan Zulham Ramadhani
Program Pascasarjana Magister Ilmu Komputer Universitas Budi Luhur
*e-mail***:** ryanzulham@gmail.com

Naskah diterima: 25-04-2016, direvisi: 27-06-2016, disetujui: 28-06-2016

Abstrak

Indonesia terletak di kawasan yang memiliki potensi tsunami. Informasi mengenai tsunami yang akan terjadi wajib diberikan pada pejabat wilayah yang diprediksi akan terkena dampak bencana tsunami agar segera mempersiapkan diri untuk mengevakuasi warganya. Mekanisme pemberian informasi ini ke tiap daerah terdampak perlu memperhatikan sistem keamanan sistem komunikasinya karena jika data dan informasi jatuh ke pihak yang tidak berwenang dapat menyebabkan stabilitas keamanan daerah penerima informasi terganggu. Untuk, itu tujuan penelitian ini ialah membuat aplikasi sistem komunikasi data informasi dini tsunami yang terenkripsi pada android antara BMKG dan penerima pesan yang berwenang. Metode penelitian ini menggunakan teknik steganografi dengan menggunakan metode LSB (*Least Significant Bit*) metode enkripsi *Caesar chipper* pada aplikasi android. Hasil penelitian menunjukkan bahwa aplikasi android yang dirancang dengan teknik staganografi dan penyisipan password md5 dapat mengirimkan pesan privasi/rahasia pada media atau data-data digital yang dikirimkan dari BMKG untuk pejabat yang berwenang terhadap informasi dini tsunami tanpa terbaca oleh pihak yang tidak berwenang.

Kata Kunci*:* sistem keamanan data*,* steganografi*, LSB, caesar chipper,* enkripsi

Abstract

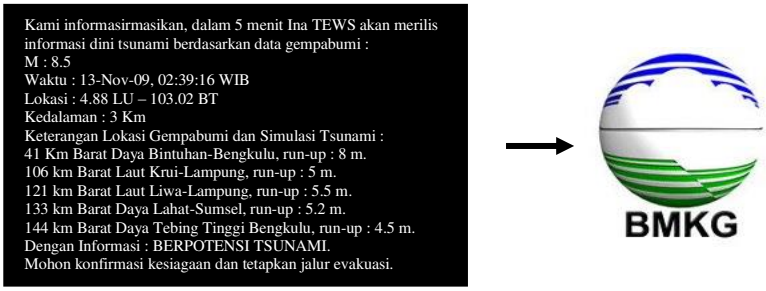
Indonesia is located in a tsunami risk zone. Information regarding an impending tsunami must be given to government officials of areas where the tsunami had been predicted in order to immediately preparing evacuation of their citizens. The mechanisms of providing this information to each affected areas should take into account of the information systems security of the Indonesia's Meteorology, Climatology and Geophysics Agency (BMKG) because if the data and information should fall into the wrong hands, it could disturb the stability and security of the area. Accordingly, this research aims to develop a tsunami early warning communication system application encripted in Android between BMKG and authorized parties. This research uses steganography technique with LSB (Least Significant Bit) Caesar cipher

encryption method on Android app. The results showed that the Android application designed using steganography and md5 password insertion technique could send a private/secret message or digital data from BMKG to media or authorised authorities in charge of tsunami alert information without being read by unauthorized parties.

***Keywords** : Data security system,* steganography*, LSB, caesarchipper , encryption*

PENDAHULUAN

Bencana tsunami yang bersumber dari lantai samudra (*seafloor*) yang terjadi akibat kejadian gempa bumi akan menimbulkan gelombang massa air laut ke segala arah hingga sampai ke pesisir pantai (Setyonegoro, 2011). Sampai dengan saat ini, gempa bumi belum dapat diprediksi (Wallansha dan Setyonegoro, 2015), akan tetapi terjadinya tsunami sudah dapat dilakukan prediksi perambatan gelombangnya setelah gempa bumi yang terjadi dengan koordinat di dasar samudra (Setyonegoro dkk, 2015).



(a) Pesan Text Rahasia (b) Gambar Logo BMKG

Gambar 1. (a) Pesan text data (*.txt) yang disisipkan pada, (b) gambar logo BMKG sebagai Informasi Dini Potensi Tsunami. Dikirimkan oleh BMKG secara rahasia pada pimpinan BNPB, POLRI, TNI, PUSDALOBS, BPBD. Dengan banyak kriteria dari potensi tsunami, maka komunikasi singkat atas persetujuan dari beberapa pejabat BMKG yang berpengalaman di bidangnya antara BMKG Pusat dan Stasiun di Daerah wajib terjaga keamanannya sebelum informasi dini dirilis online oleh Ina TEWS-BMKG. (Sumber : Gempa Terkini BMKG, 2016).

Sebelum terjadi tsunami, masih dapat diprediksi dan dilakukan pemberian informasi peringatan dini bagi area yang terprediksi akan berpotensi berdampak tsunami. Peringatan dini adalah serangkaian kegiatan pemberian peringatan sesegera mungkin kepada masyarakat tentang kemungkinan terjadinya bencana pada suatu tempat oleh lembaga yang berwenang (PP No.21 Tahun 2008). Sebagai contoh, untuk Negara Indonesia, suatu badan yang bertugas memberikan informasi dini mengenai potensi tsunami adalah BMKG. Untuk prosedur di internal BMKG sebelum informasi warning tsunami dikeluarkan, pejabat BMKG berwenang akan mendapat prosedur izin singkat bagi operator untuk melakukan *commit* pada informasi warning tsunami via *Decission Support System* (DSS). Ina-TEWS BMKG menyusun alat sederhana bagi para pengambil keputusan dan para pemangku kepentingan (*stakeholder*) di tingkat daerah yang terlibat dalam pelaksanaan peringatan dini terhadap Tsunami di tingkat komunitas di Indonesia (Spahn, 2006).

Sistem peringatan dini yang terpusat pada masyarakat adalah merupakan suatu sistem yang peringatannya diberikan tepat pada waktunya dan dapat dimengerti oleh individu dan masyarakat yang menghadapi risiko bencana, termasuk panduan tentang bagaimana mereka bertindak apabila ada peringatan serta mengambil tindakan untuk

menghindari atau mengurangi bencana yang mengancam.

Informasi peringatan dini tsunami harus segera didistribusikan kepada instansi lain yang berwenang baik di dalam negeri maupun negara tetangga yang terprediksi akan mengalami dampak serupa. Hal ini menjadikan informasi potensi tsunami menjadi teramat penting bagi area yang diprediksi terdampak tsunami. Dalam prosedur hukum sistem keamanan nasional, hal ini terkait dengan informasi ekstrem yang dapat menjadikan warga panik dan stabilitas nasional politik dan keamanan terganggu jika seandainya informasi yang didistribusikan tidak valid atau menjadi isu yang salah di kalangan penduduk terdampak tsunami.

Berdasarkan Permen Kominfo. No. 20 tahun 2006, tentang peringatan dini tsunami atau bencana lainnya melalui lembaga penyiaran di seluruh Indonesia, pasal 6 Ayat 2 menyebutkan bahwasannya," pihak-pihak yang menyalahgunakan peringatan dini tsunami atau bencana lainnya yang berakibat menggangu ketertiban umum dan atau meresahkan masyarakat dapat dikenakan sanki pidana sesuai dengan ketentuan peraturan perundang-undangan yang berlaku". Hal itu menekankan bahwa peringatan dini yang dalam hal ini bencana tsunami harus berada pada jalur komunikasi yang tepat.

Komunikasi informasi peringatan dini tsunami melalui jalur yang tidak tepat dan tidak aman dapat mengakibatkan kebocoran informasi yang akhirnya memicu kepanikan Perkasa (2016) dan keresahan dalam masyarakat (Aditya, 2014; Rahman, 2013). Bahkan berita bohong (hoax) juga dapat tersebar (Prasetya, 2014; Rahman, 2013) sehingga pemerintah sering mengingatkan kepada masyarakat untuk meminta informasi hanya kepada lembaga resmi Nugroho (2016). Oleh sebab itu, jalur komunikasi peringatan dini perlu dilewatkan melalui pesan rahasia. Pesan rahasia pemerintahan ini menjadi penting untuk dijalankan, terkait deteksi steganogram untuk mendukung *E-Government* (Bahrawi dkk, 2013).

Dalam melakukan proses *steganografi* pada data digital terdapat banyak cara yang dapat dilakukan, salah satunya adalah dengan menggunakan metode *Least Significant Bit* dan metode *Creamer* untuk melakukan penyembunyian data pada media digital tersebut Ariyus (2009), dan aplikasi Enkripsi SMS menggunakan metode Blowfish Wahyu (2010). Metode ini menjamin keutuhan media sehingga tidak merusak media asli meskipun telah disisipi data rahasia Win (2015). Selain itu, metode ini merupakan metode yang mudah dimplementasikan pada data-data digital seperti gambar dan video (Bander, 1996).

Atas dasar inilah metode LSB (*Least Significant Bit*) dan Metode Enkripsi Caesar merupakan metode *steganografi* yang penulis pilih. Studi kasus desain pada penelitian ini mengangkat tema aplikasi android pada data privasi/rahasia komunikasi informasi dini tsunaanmi yang perlu dienkripsi untuk menjaga stabilitas keamanan nasional.

Beberapa data terkait Informasi tsunami yang diamankan adalah sebagai berikut:

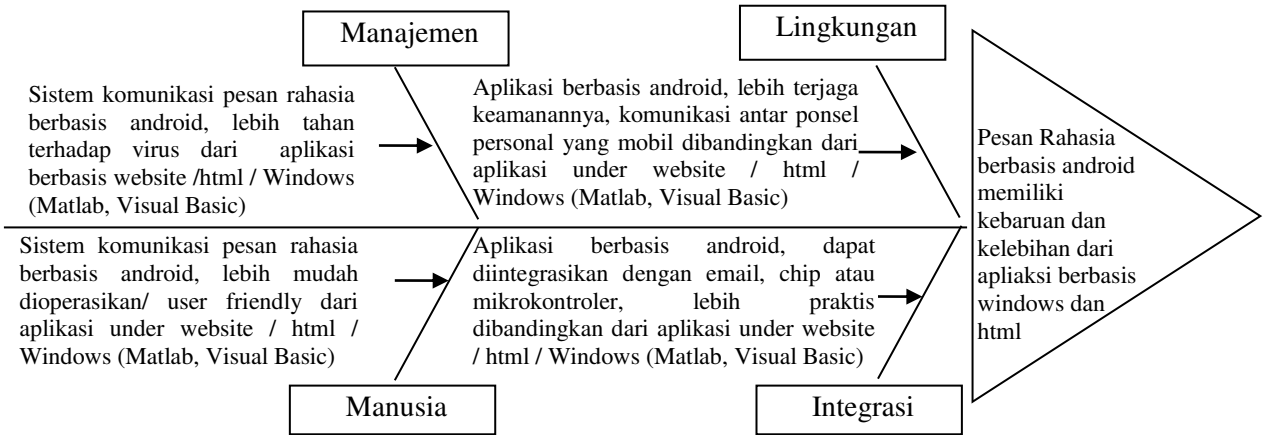
1. Informasi prediksi tsunami pada area terdampak tsunami.
2. Ketinggian gelombang tsunami yang akan tiba di garis pantai.
3. Informasi prediksi luapan/inundasi tsunami yang akan menggenangi area terdampak tsunami.
4. Rekomendasi jalur evakuasi bagi tiap-tiap sub perbatasan area yang terdampak tsunami.
5. Simulasi tingkat korban jiwa akibat luapan tsunami (inundasi) berdasarkan data populasi penduduk yang diprediksi terdampak tsunami.

Kelima data tersebut perlu dijaga kerahasiaannya karena dapat terjadi kepanikan bila

data tersebut sampai pada pihak yang tidak berwenang atau tersebarnya informasi yang salah terutama pada media internet dan TV yang dikemas untuk kehangatan informasi. Kepanikan tersebut akan menyebabkan reaksi berantai. Kepanikan warga dalam mengevakuasi diri ke tempat yang lebih tinggi untuk menghindari tsunami yang akan terjadi secara bersamaan, terburu-buru dalam satu waktu sehingga dapat menyebabkan jalur transportasi padat, timbulnya kekacauan akibat kepanikan warga akan adanya bencana tsunami (Gambar 2).

Dari bahasan-bahasan pada latar belakang tersebut maka dapat disimpulkan beberapa masalah yang menjadi pokok bahasan penulisan ini yang dapat diterapkan dalam penulisan ini. Masalah yang dapat ditemui, antara lain ialah sebagai berikut.

a. Bagaimana proses penerapan metode LSB pada media digital/ gambar ?
b. Bagaimana penyisipan dengan metode enkripsi Caesar dan pengambilan data pada media penampung.



Gambar 2. Diagram sebab akibat - Fishbone pada penggambaran State of The Art dari kebaruan penelitian dengan metode LSB dan Enkripsi Caesar Chiper dari penelitian terdahulu.

c. Apakah keamanan sistem komunikasi data ini akan berpengaruh positif bagi pengiriman informasi dini tsunami dengan urutan prosedur penerimaan informasi bagi pejabat/petugas yang berwenang memutuskan apakah informasi tersebut akan diteruskan ke masyarakat atau petugas setempat memiliki cara lain/kesempatan untuk mengatur jalur evakuasi bagi warganya agar tidak menimbulkan kepanikan penduduk pada area yang diprediksi terdampak tsunami

Tujuan dari penulisan ini ialah membuat aplikasi android dengan teknik *steganografi* untuk menjaga kerahasiaan data berupa dengan menyisipkan pesan text yang pada media gambar BMP/ JPG 24 bit dengan metode LSB (*Least Significant Bit*) menggunakan metode enkripsi *Caesar Chiper.*

Dalam penelitian ini akan dibatasi permasalahan-permasalahan yang ada sehingga cakupannya tidak begitu melebar. Batasan masalah dalam penelitian ini ialah sebagai berikut.

a. Media yang digunakan untuk disisipkan *watermark* berupa data gambar dengan format BMP/JPG 24 bit.
b. Data *watermark* yang digunakan berupa data berupa gambar lain dengan dimensi seper delapan dari media yang digunakan dan dengan format yang sama yaitu BMP/JPG 24 bit.
c. Jika data yang digunakan adalah dalam data *watermark* dengan *file* dengan format cirta digital, *file* itu harus diubah menjadi citra 2 warna.
d. Metode yang digunakan untuk proses penyisipan yaitu metode *Least Significant Bit* (LSB) dan enkripsi Caesar

Chiper.

e. Aplikasi penelitian dititikberatkan pada penyisipan atau penggunaan metode LSB pada media digital berupa gambar dalam sistem komunikasi data antar negara yang diprediksi terdampak tsunami.

Manfaat penelitian ini ialah sebagai berikut.

a. Aplikasi yang lebih mudah digunakan (*user friendly*) pada *smartphone* android dengan menggunakan data digital berupa gambar dengan format BMP/ JPG 24 bit.
b. Hasil uji coba penelitian ini dapat digunakan sebagai media verifikasi untuk penelitian lebih lanjut dalam pengembangan *prototipe*.

Penelitian ini yang menggunakan metode LSB untuk melakukan steganografi pada media digital dengan menggunakan aplikasi android telah dilakukan sebelumnya, diantaranya penelitian yang dikembangkan oleh Juanda (2009) dari Universitas Teknik Informatika Gunadarma dengan tema penelitian "Aplikasi steganografi pada audio MP3 dengan menggunakan metode LSB". Perbedaan penelitian Juanda (2009) dengan penelitian ini ialah pada software *tools* dan objek penyisipan yang dipilih.

Penelitian Juanda (2009) yang menggunakan media penampung adalah file dengan format MP3, sedangkan media penampung yang digunakan dalam penelitian ini adalah file gambar dengan format BMP/JPG 24 bit. Selain media yang digunakan, penelitian Juanda (2009) menggunakan Java sebagai alat bantu pemrosesan data, sedangkan pada penelitian ini menggunakan alat bantu android berbasis linux sebagai media pemprosesnya.

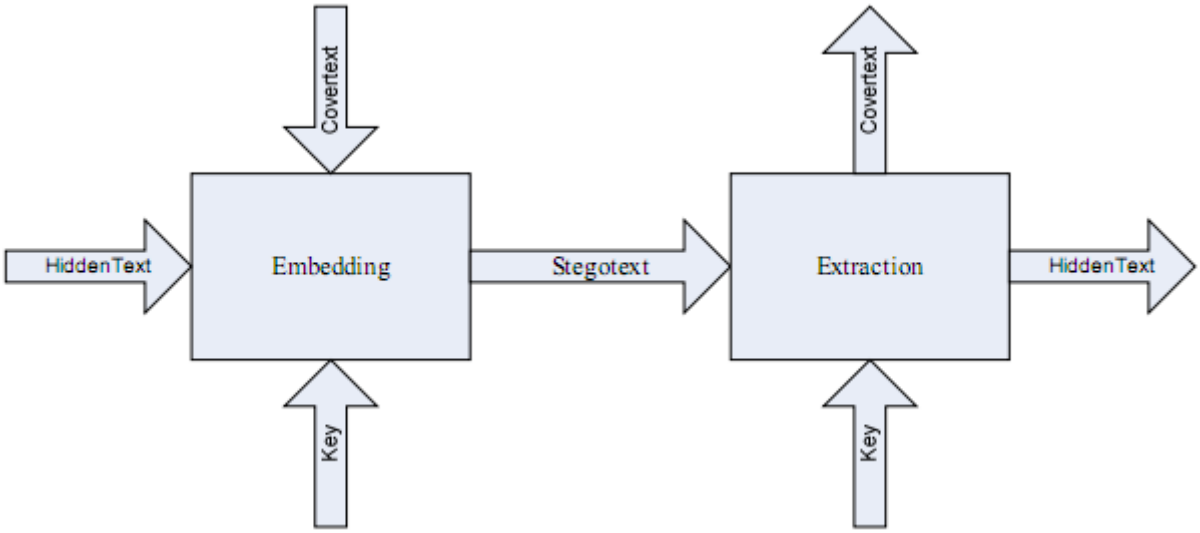
Penelitian lainnya yang mempunyai tema yang sama dengan penelitian (Septiani, 2012) berjudul "Aplikasi *watermarking* pada *mobile device* dengan menggunakan J2ME". Dan penelitian teknik steganografi dengan metode LSB dan diimplementasikan dengan menggunakan alat bantu Java (Hermawan, 2004). Selain itu aplikasi ditujukan kepada para pengguna mobile sehingga digunakan J2ME sebagai alat bantu pemproses (Kristian, 2010). Pada penelitian kali ini metode yang dilakukan diuji coba dilakukan dengan metode LSB dan ditambahkan dengan teknik enkripsi Caesar Chiper.

Kata steganografi berasal dari bahasa Yunani yaitu *steganos* yang berarti 'tersembunyi' atau 'terselubung' dan *graphein* yang berarti 'menulis' sehingga kurang lebih artinya adalah 'menulis tulisan yang tersembunyi atau terselubung' (Kettle & Sellars, 1996). Prinsip dasar keamanan data dengan menyembunyikannya melalui proses enkripsi sehingga orang lain tidak dapat membacanya (Alatas Putri, 2009; R.T. Michael, 2000).

Steganografi sudah dikenal oleh bangsa Romawi sekitar 2500 tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi. Bangsa Romawi mengenal steganografi dengan menggunakan tinta tak-tampak untuk menulis pesan. Tinta tersebut terbuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis, tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Konsep dari steganografi adalah menyembunyikan pesan dalam media lain sehingga pesan tidak dapat diterjemahkan secara langsung (Munir, 2004), dalam *steganografi* dikenal beberapa istilah sebagai berikut.

a. *Hidden Text*, merupakan pesan yang disembunyikan.
b. *Covert text*, merupakan media yang digunakan untuk menampung pesan.
c. *Stego text*, merupakan media yang sudah disisipkan pesan.
d. *Stego key*, merupakan kunci yang digunakan untuk menyisipkan pesan maupun membaca pesan (Gambar 3).



Gambar 3. Ilustrasi teknik penyisipan data dengan steganografi.

Akurasi algoritma steganografi seperti yang ditunjukkan pada Gambar 3 dapat dinilai dari beberapa faktor yaitu :

a) *Imperectibility*. Keberadaan pesan rahasia dalam media penampung tidak terdeteksi oleh inderawi. Misalnya, jika *covertext* berupa citra, penyisipan pesan membuat citra *stegotext* sukar dibedakan oleh mata dengan *covertext*-nya (Morkel et al, 2005). Jika *covertext* berupa audio (misalnya berkas *file* mp3, wav, midi dan lainnya), indra telinga tidak dapat mendeteksi perubahan pada *file stegotext*-nya (gambar 3).
b) *Fidelity.* Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan itu tidak dapat dipersepsi oleh inderawi. Misalnya, jika *covertext* berupa citra, penyisipan pesan dapat membuat citra *stegotext* sukar dibedakan oleh mata dengan citra *covertext*-nya. Jika *covertext* berupa audio (misalnya berkas *file* mp3, wav, midi dan sebagainya), audio *stegotext* tidak rusak dan indera telinga tidak dapat mendeteksi perubahan pada *file stegotext*-nya.
c) *Recovery*. Pesan yang disembunyikan harus dapat diungkapkan kembali (*reveal*) karena tujuan steganografi ialah *data hiding.* Dengan itu sewaktu-waktu pesan rahasia di dalam *stegotext* harus dapat diambil kembali untuk digunakan lebih lanjut.

File Image BMP/JPG 24 Bit merupakan format *file* yang digunakan untuk menyimpan data yang gambar, di mana *file* dengan format ini dapat mendukung format warna *monochrome* hingga *true color*. File dengan format BMP/JPG menyimpan warna dengan sistem RGB (*Red, Green, and Blue*), di mana format warna inilah yang nantinya akan diproses lebih lanjut untuk menghasilkan gambar dengan dengan penyisipan *text*.

Metode LSB (*Least Significant Bit*) digunakan dalam teknik steganografi dikarenakan tergolong mudah dalam penerapannya. Dasar dari metode ini adalah bilangan berbasiskan biner atau dengan kata lain angka 0 dan angka 1. Karena data digital merupakan susunan antara angka 0 dan satu proses penerapannya menjadi mudah. Lebih lanjut lagi, metode ini berhubungan erat dengan ukuran 1 bit dan ukuran 1 *byte*. 1 *byte* data dapat dikatakan terdiri dari 8 bit data. Di mana bit pada

posisi paling kanan lah yang disebut dengan bit pada posisi LSB (*Least Significant Bit*). Teknik steganografi dengan menggunakan metode LSB adalah teknik dimana kita mengganti bit pada posisi LSB pada data dengan bit yang dimiliki oleh data yang akan disembunyikan. Karena bit yang diganti hanyalah bit yang paling akhir, meskipun data telah berubah, kita tetap tidak akan bisa mengenalinya karena media stego yang dihasilkan hampir sama persis dengan media sebelum disisipi oleh data yang ingin disembunyikan Gunawan (2007).

Untuk ilustrasi proses penyisipan pesan dengan menggunakan metode ini dapat dilihat pada Gambar 4.

```
00100111  11101001  11001000  00100111  11001000  11101001
11001000  00100111
```

Gambar 4. Data biner asli sebelum disisipkan perubahan bit.

Dari data pada Gambar 3 akan disisipkan suatu pesan rahasia yang berupa data biner dengan nilai bit (01001000) maka data atau media penampung akan menjadi seperti yang ditunjukkan pada Gambar 5.

```
00100110  11101001  11001000  00100110  11001001  11101000
11001000  00100110
```

Gambar 5. Data biner setelah disisipkan nilai pada setiap bit.

Dari penjelasan di atas dapat disimpulkan bahwa metode LSB hanya mengganti satu nilai dari posisi LSB pada setiap bit data pada media penampung data yang akan disembunyikan dengan satu bit data dari text atau data yang akan disembunyikan. Karena bit yang diganti adalah bit dengan nilai paling kanan, media yang dihasilkan hampir sama persis dengan media aslinya.

Android adalah sistem operasi berbasis *Linux* yang dirancang untuk perangkat seluler layar sentuh seperti telepon pintar dan komputer tablet. Android awalnya dikembangkan oleh Android, Inc., dengan dukungan finansial dari Google, yang kemudian dibelinya pada tahun 2005. Sistem operasi ini dirilis secara resmi pada tahun 2007, bersamaan dengan didirikannya *Open Handset Alliance*, konsorsium dari perusahaan-perusahaan perangkat keras, perangkat lunak, dan telekomunikasi yang bertujuan untuk memajukan standar terbuka perangkat seluler. Ponsel Android pertama mulai dijual pada bulan Oktober 2008.

Aplikasi Android dikembangkan dalam bahasa pemrograman Java dengan menggunakan kit pengembangan perangkat lunak Android (SDK). SDK ini terdiri dari seperangkat perkakas pengembangan, termasuk *debugger*, perpustakaan perangkat lunak, *emulator handset* yang berbasis QEMU, dokumentasi, kode sampel, dan tutorial. Didukung secara resmi oleh lingkungan pengembangan terpadu (IDE) Eclipse, yang menggunakan plugin *Android Development Tools* (ADT). Perkakas pengembangan lain yang tersedia di antaranya ialah Native Development Kit untuk aplikasi atau ekstensi dalam C atau C++, *Google App Inventor*, lingkungan visual untuk pemrogram pemula, dan berbagai kerangka kerja aplikasi web seluler lintas platform. Dalam rangka menghadapi penyensoran internet di Republik Rakyat Cina, perangkat Android yang dijual di RRC umumnya disesuaikan dengan layanan yang disetujui oleh negara.

Dalam kriptografi Munir (2004), metode *Caesar Chipper* berarti sandi *Caesar*, atau sandi geser. Kode *Caesar* atau Geseran *Caesar* adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dengan setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Misalnya, jika menggunakan geseran 3, W akan menjadi Z, I menjadi L, dan K menjadi N sehingga teks terang "wiki" akan menjadi

"ZLNL" pada teks tersandi. Nama *Caesar* diambil dari Julius Caesar, jenderal, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya.

Langkah enkripsi oleh sandi *Caesar* sering dijadikan bagian dari penyandian yang lebih rumit, seperti sandi *Vigenère*, dan masih memiliki aplikasi modern pada sistem ROT13. Pada saat ini, seperti halnya sandi substitusi alfabet tunggal lainnya, sandi *Caesar* dapat dengan mudah dipecahkan dan praktis tidak memberikan kerahasiaan bagi pemakainya Namiesyva (2007).

Cara kerja sandi ini dapat diilustrasikan dengan membariskan dua set alfabet; alfabet sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci). Misalnya sandi Caesar dengan kunci 3, adalah sebagai berikut:

Alfabet Biasa:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabet Sandi:
DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut, digunakan cara sebaliknya. Contoh penyandian sebuah pesan ialah sebagai berikut (tabel 1).

Teks terang: kirim pasukan ke sayap kiri

Teks tersandi: NLULP SDVXNDQ NH VDBDS NLUL

Tabel 1 Pola Pergeseran Sandi

Geseran yang Digunakan	Calon Teks Terang
0	exxegoexsrgi
1	dwwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrmlac
23	haahjrhavujl
24	gzzgiqgzutik

Proses penyandian (enkripsi) dapat secara matematis menggunakan operasi modulus dengan mengubah huruf-huruf menjadi angka, A = 0, B = 1,..., Z = 25. Sandi (E_n) dari "huruf" x dengan geseran *n* secara matematis dituliskan dengan,

$$E_n(x) = (x + n) \mod 26. \quad (1)$$

Sedangkan pada proses pemecahan kode (dekripsi), hasil dekripsi (D_n) adalah

$$D_n(x) = (x - n) \mod 26. \quad (2)$$

Setiap huruf yang sama digantikan oleh huruf yang sama di sepanjang pesan sehingga sandi Caesar digolongkan kepada *substitusi monoalfabetik*, yang berlawanan dengan *substitusi polialfabetik*.

Proses membaca teks tersandi menjadi teks terang disebut dekripsi. Sandi *Caesar* dapat dipecahkan bahkan jika seseorang hanya memiliki teks tersandi tanpa mengetahui nilai geserannya. Jika pihak pemecah sandi hanya mengetahui bahwa substitusi monoalfabetik digunakan dalam suatu sandi, sandi tersebut dipecahkan dengan cara analisis frekuensi.

Setiap bahasa memiliki huruf yang sering digunakan atau jarang digunakan.

Misalnya huruf *a* sering sekali digunakan dalam bahasa Indonesia, dan *q* atau *x* jarang sekali muncul. Setiap bahasa memiliki pola frekuensi tertentu, yang menunjukkan frekuensi relatif dari penggunaan huruf-huruf dalam bahasa tersebut. Pola frekuensi huruf dalam bahasa Inggris ditunjukkan dalam gambar.

Pola frekuensi huruf-huruf dalam bahasa Inggris. Pola ini memiliki sifat tertentu, misalnya "lonjakan" pada e, atau tiga bar tinggi pada r-s diikuti 6 batang rendah pada u-z. Jika pemecah kode menghitung frekuensi huruf pada teks tersandi, karakteristik khusus pada grafik di samping tentu masih ada pada teks tersandi, hanya saja posisinya telah digeser. Misalkan sang pemecah kode menemukan lonjakan di C, serta tiga batang tinggi berturut-turut diikuti enam batang rendah berturut-turut dimulai dari O, bisa ditebak bahwa sandi tersebut menggunakan geseran 5 ke kiri. Kesimpulannya kita dapat mendekripsi teks tersandi dengan menggeser setiap huruf sandi 2 posisi ke kanan.

Cara kedua lebih mudah dan dapat dilakukan jika sang pemecah sandi mengetahui bahwa pengirim sandi menggunakan sandi Caesar. Sandi tersebut akan dipecahkan dengan menggunakan *brute force attack*, yaitu mencoba kedua puluh enam kemungkinan geseran yang digunakan. Biasanya hanya satu dari kedua puluh enam kemungkinan ini yang dapat dibaca, Misalnya suatu teks tersandi "EXXEGOEXSRGI".

Pada tabel 1 ditunjukkan hasil percobaan yang dilakukan, dan hanya satu hasil yang dapat dibaca, yaitu *attackatonce*. Hal ini berarti pesan yang disandikan adalah pesan berbahasa Inggris "*attack at once*", yang berarti ‘serang sekarang juga’.

Dengan kemajuan komputer dan teknologi informasi, kedua cara tersebut dapat dijalankan dengan mudah dan cepat sehingga saat ini sandi Caesar sama sekali tidak berguna untuk menyembunyikan atau menyandikan dokumen-dokumen atau perintah-perintah penting dan rahasia.

METODE

Dalam penulisan penelitian steganografi dengan menggunakan metode LSB dan enkripsi *Caesar Chipper* pada media digital dengan media penyisipan berupa gambar dengan keterangan sebagai berikut (Chen, 2000).

a) Metode penyisipan text dengan ukuran seperdelapan dari media yang akan disisipi, yaitu gambar. Dengan format gambar yang sama yaitu format BMP/JPG 24 bit. Format 24 bit dipilih karena pada kondisi ini gambar belum terkompresi. Selanjutnya gambar tersebut dikompresi ke format PNG.
b) Program yang digunakan dalam metode berkaitan dengan penggunaan alat bantu aplikasi android berbasis linux.
c) Metode yang digunakan dalam penggunaan steganografi adalah penggunaan metode yang berdasarkan pada LSB dan enkripsi *Caesar Chiper*.
d) Proses extraksi pesan, hanya berkaitan dengan pengambilan data gambar atau pesan rahasia yang dimasukkan dengan menggunakan applikasi ini. Extraksi tidak dapat digunakan apabila gambar rahasia dimasukkan dengan aplikasi lain.
e) Pada aplikasi tidak terdapat media atau perantara yang digunakan dalam melakukan pengujian data untuk tingkat ketahanan data stego terhadap proses konversi atau perubahan citra.

penelitian juga menetapkan beberapa variabel yang digunakan, yaitu :

a) ukuran gambar yang bervariasi besarnya
b) format gambar yang dipilih yaitu format BMP/JPG 24 bit.
c) jumlah bit yang akan disisipkan yang bergantung pada jumlah bit data penampung.

Penelitian ini juga menggunakan berbagai macam data, khususnya data kuantitatif yang berupa indek warna dari gambar digital yang digunakan sebagai objek penelitian ini. Dengan rujukan bahwa proses steganografi adalah penyisipan pesan dalam satu media ke media lain (Rojali dkk, 2012). Dalam penelitian ini, pesan itu berupa indek angka dari media gambar yang akan di proses. Selain itu data kuantitatif lainnya berkaitan dengan ukuran gambar dan kedalaman gambar.

Penelitian ini menggunakan data kualitatif yang berkaitan dengan format gambar yang digunakan. Format yang digunakan adalah format PNG terkompresi dengan tujuan agar hasil yang tercapai bisa maksimal.

Data primer yang digunakan dalam penelitian ini ialah gambar digital berformat BMP/JPG 24 bit yang dikompresi ke format PNG. Data inilah yang kemudian akan digunakan sebagai data primer untuk melakukan uji coba teknik LSB dan enkripsi *Caesar Chipper* pada steganografi.

Data sekunder yang digunakan ialah data data literatur yang berkaitan dengan teknik dan uraian atau pengertian tentang berbagai kata kunci yang mendukung penulisan ini. Data sekunder berupa artikel artikel tentang teknik LSB, steganografi, ataupun *watermarking* yang diperoleh dari media internet. Selain itu, data sekunder lainnya ialah data yang berkaitan dengan kriteria keberhasilan dari steganografi ataupun *watermarking* itu sendiri. Hal tersebut didukung oleh data mengenai berbagai penggunaan metode LSB dalam berbagai media digital beserta semua yang berkaitan dengan metode ini.

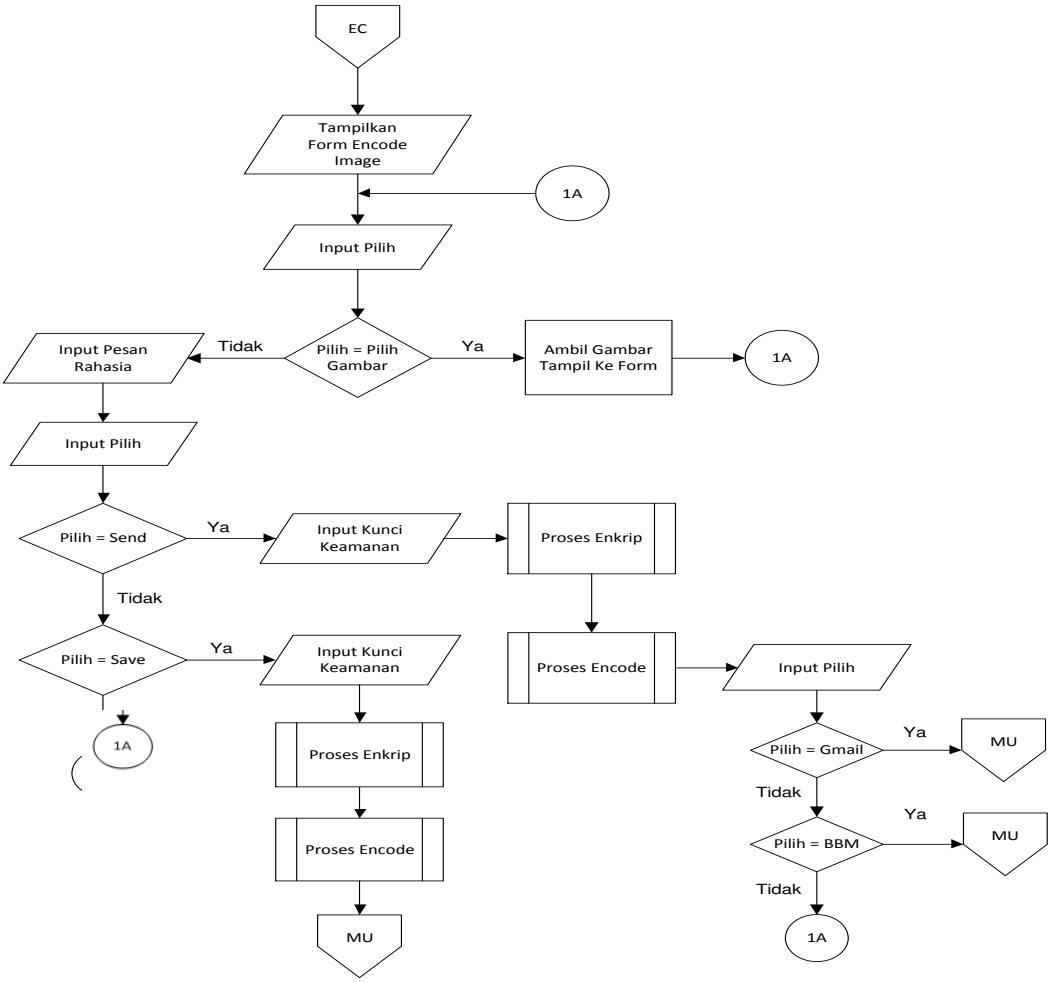
Data dikumpulkan melalui proses studi literatur tentang berbagai variabel yang berada pada penulisan penelitian. Studi literatur itu juga berasal dari studi dari berbagai artikel dengan tema yang sama yang dapat diperoleh dari media informasi internet. Selain itu data diperoleh dari berbagai buku dengan tema yang sama dengan judul penelitian.

HASIL DAN PEMBAHASAN

Rancangan Algoritma

Teknik pembuatan algorithma steganografi dengan menggunakan metode LSB 2bit dan enkripsi *Caesar Chipper* dan dengan menggunakan aplikasi Android ini diawali dari proses penentuan medium. Medium yang dipakai ialah file dengan format BMP/JPG 24 bit lalu dikompresi ke format PNG. Alasan dipilihnya file dengan format PNG ialah sangat eratnya struktur format file BMP/JPG dengan metode yang digunakan yaitu metode LSB. Untuk data yang ingin disembunyikan atau stego key, applikasi, data dapat berupa apa saja. Namun, dalam hal ini data yang akan diambil untuk dijadikan stego text dalam penulisan kali ini adalah file gambar juga. File yang digunakan sebagai *stego text* haruslah mempunyai ukuran seperdelapan dari ukuran lebar ataupun ukuran tinggi dari gambar yang akan dijadikan penampung/ wadah/ media penyisipan. Dan, ukuran maksimum dari gambar adalah tidak lebih dari 1 Mb.

Dibandingkan dengan penelitian Asep Juanda (2009), aplikasi penyisipan pesan berbasis Matlab, Win (2015) dan aplikasi penyisipan pesan berbasis visual basic, ukuran maksimum dapat berukuran lebih besar, atau lebih banyak jumlah abjad yang dapat disisipkan. Namun, aplikasi berbasis android ini lebih praktis karena *mobile* dan dapat dibawa secara personal oleh pimpinan departemen yang berwenang untuk mengetahui segera potensi tsunami ini. Penelitian ini menekankan bahwa kecepatan komunikasi akan lebih menjadi prioritas, dibandingkan dengan jumlah ukuran pesan yang akan dikirim.



Gambar 6. Algoritma *flowchart encode* gambar mengunakan aplikasi android.

Algoritma Penyisipan Data

Metode yang digunakan dalam proses penyisipan bit data kedalam *byte* citra penampung adalah dengan meng-gunakan teknik penyisipan pada LSB (*Least Significant Bit*), penyisipan LSB dilakukan dengan memodifikasi bit terahkir dalam satu *byte* (8 Bit) data.

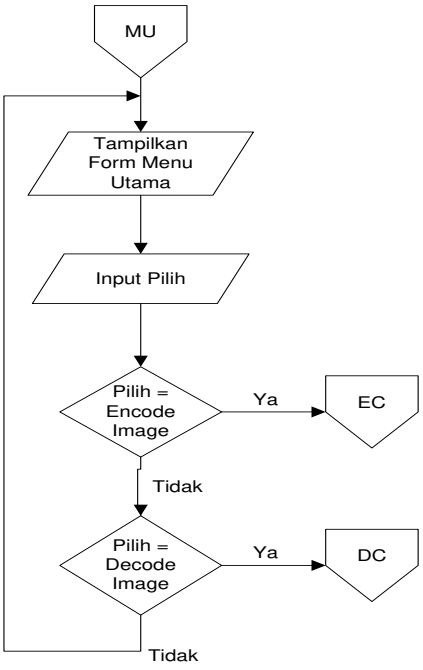
Proses penggantian ini hanya akan mengakibatkan nilai *byte* asli berubah kurang satu ataupun lebih satu. Sehingga kualitas akan hampir sama seperti saat sebelum dimodifikasi. Seperti yang kita ketahui bahwa *file* gambar dengan format warna RGB mempunyai 3 elemen warna dasar yaitu elemen Merah (*Red*) , Hijau (*Green*), dan Biru (*Blue*). Setiap elemen warna diwakili oleh indeks untuk setiap *pixel* atau bagian terkecil dari citra digital (gambar 6).

Ketiga nilai elemen indeks inilah yang akan dijadikan sebagai objek modifikasi atau sebagai media penampung pada proses penyisipan data. Proses penyisipan data diawali dengan proses pembacaan data penampung, dan kemudian diikuti dengan proses pembacaan data yang akan disisipkan.

Data dalam format BMP/JPG mempunyai karakteristik warna RGB maka dari itu dilakukan proses pembuatan atau pengkonversian dari gambar dengan banyak warna atau RGB menjadi gambar dengan format hitam putih, proses ini dilakukan untuk gambar atau medium yang akan disisipkan.

Untuk gambar atau media penampung digunakan proses pembacaan indeka untuk setiap unsur warnanya. Untuk langkah selanjutnya, dilakukan proses mengganti untuk masing-masing bit LSB pada setiap unsur warna pada media penampung dengan bit yang ada pada media stego atau *stego key* nya.

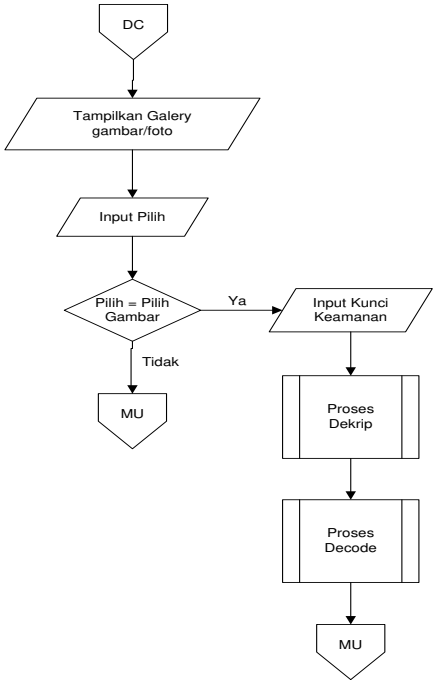
Hal itu merupakan proses pengulangan yang dilakukan dari *pixel* pertama dari media penampung hingga *pixel* terakhir dari media penampung (gambar 7).



Gambar 7. Algoritma *flowchart* menu utama mengunakan aplikasi android.

Proses diakhiri dengan penulisan data berupa media citra digital dengan format yang sama dengan media penampung, tetapi dengan data yang telah dirubah pada setiap LSB pixelnya.

Mulai - Input Gambar Penampung (*.bmp / *jpg) – Gambar penampung dikompres ke *png - Input Media Data Rahasia “Text” - Lebar = 1/8 dari Lebar Gambar Penampung Tinggi = 1/8 - Tinggi Gambar Penampung Lebar & tinggi = Kriteria - Tidak - Gambar Data Rahasia = Citra Hitam Putih atau 2 Warna Convert Citra Menjadi Monochome - Proses Pemisahan Indek Warna Media Penampung - AA Menganti Setiap Bit LSB pada data penampung dengan Bit Data Rahasia (Stego Key) - Citra hasil dengan Steganografi – Selesai (Gambar 6).



Gambar 8. Algoritma *flowchart decode* gambar mengunakan aplikasi android.

Algoritma Pengambilan Data

Pengambilan data pada media yang telah disisipi data rahasia berarti proses pengambilan data setiap dari setiap LSB pada media penampung. Untuk setiap bit data yang diambil pada media penampung, akan diterjemahkan ke dalam satuan *byte*, kemudian akan diterjemahkan untuk dapat dihasilkan citra stego yang dapat dimengerti.

Karena pada proses citra stego yang dimasukan adalah citra dengan format monochrome, hasil dari proses pengambilan data adalah citra dengan format monochrome. Proses pengambilan data dimulai dengan memasukkan input data yang telah mengandung pesan rahasia. Data yang berupa gambar ini kemudian akan dipecah berdasarkan indeksnya, yaitu berdasarkan elemen warnanya.

Dalam hal ini elemen warna yang dimaksudkan adalah elemen warna RGB. Karena nilai LSB pada setiap piksel elemen

RGB adalah sama, kita hanya menggunakan salah satu elemen saja. Proses berlanjut dengan proses penyusunan kembali bit menjadi satu ukuran *btye* (8 bit), dengan ukuran 1 *byte* pada proses penyusunan ini ialah berarti 1 *pixel* media data rahasia.

Proses berulang hingga semua data pada media elemen media penampung telah diterjemahkan. Hasil yang didapatkan adalah *file* data rahasia yang telah kita sisipkan sebelumnya. Mulai Input Data Gambar (RGB BMP) - Proses Ekstraksi Pesan Mulai Dari *Pixel* pertama sampai pixel terakhir - Simpan Hasil Data (Dengan Menyusun hasil dari proses ekstraksi - Tampilkan Gambar / pesan Rahasia – Selesai (Gambar 8).

Algoritma Substitusi Menggunakan Enkripsi Caesar Chipper

Caesar Chipper merupakan salah satu algoritma *chipper* tertua dan paling diketahui dalam perkembangan ilmu kriptografi. *Caesar chipper* merupakan salah satu jenis *chipper* substitusi yang membentuk *chipper* dengan cara melakukan penukaran karakter pada *plaintext* menjadi tepat satu karakter pada *chippertext*. Teknik seperti ini disebut juga sebagai *chipper* abjad tunggal.

Algoritma kriptografi *Caesar Chipper* sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini, melakukan pergeseran terhadap semua karakter pada plainteks dengan nilai pergeseran yang sama. Adapun langkah-langkah yang dilakukan untuk membentuk chiperteks dengan *Caesar Chipper* adalah sebagai berikut.

1. Menentukan besarnya pergeseran karakter yang digunakan dalam membentuk *ciphertext* ke *plaintext*.
2. Menukarkan karakter pada *plaintext* menjadi *chippertext* dengan berdasarkan pada pergeseran yang telah ditentukan sebelumnya.

Berikut adalah contoh penggunaan *Caesar Chipper* dengan besar pergeseran sebesar 3 karakter. Dengan nilai pergeseran tersebut, didapat tabel pergeseran nilai *Caesar Chipper* sebagai berikut :

Tabel Subtitusi :

pi : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

ci : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Contoh proses penggunaan *Caesar Chipper* :

Pesan :

INI ADALAH KATA SANDI YANG BENAR

Hasil enkripsi :

LQL DGDODK NDWD VDQGL BDQJ EHQDU

Apabila penerima mendeskripsikan pesan diatas menggunakan tabel subtitusi diatas maka hasilnya :

INI ADALAH KATA SANDI YANG BENAR

Kelemahan

Kelemahan menggunakan algoritma *Caesar chipper* adalah sebagai berikut.

1. Tingkat keamanannya rendah, dikarenakan jumlah kuncinya hanya 26 kunci saja.
2. Teknik pemecahan kata kunci tersebut dapat dilakukan dengan cara melakukan pengecekan terhadap semua kunci yang ada yang berjumlah 26 tersebut.

Algoritme Substitusi Menggunakan *Chipper Key*

Algoritma *chipper key* merupakan metode yang menggunakan sebuah kata sebagai kata kunci yang disubtitusikan

kedalam abjad. Dimana pesan yang akan disampaikan sama namun menggunakan kata kunci yang tidak sama.

Contoh proses penggunaan *chipper key* :

Pesan :

AWAS VIRUS BERBAHAYA

1. Menggunakan kata kunci : PALSU

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	A	L	S	U	B	C	D	E	F	G	H	I	J	K	M	N	O	Q	R	T	V	W	X	Y	Z

Pesan	A	W	A	S	V	I	R	U	S	B	E	R	B	A	H	A	Y	A
Enkripsi	P	W	P	Q	V	E	O	T	Q	A	U	O	A	P	D	P	Y	P

Kelebihan :

- Kemungkinan untuk mendapatkan kata kunci sulit.
- Jika kata kunci diubah,subtitusi semua abjad akan berubah

Kelemahan :

- Pada akhir abjad seperti V, W, X, Y, Z tidak berubah
- Terdapat karakter yang sama
- Kata kunci yang terlalu singkat/pendek.

2. Menggunakan kata kunci : Komputer

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K	O	M	P	U	T	E	R	A	B	C	D	F	G	H	I	J	L	N	Q	S	V	W	X	Y	Z

Pesan	A	W	A	S	V	I	R	U	S	B	E	R	B	A	H	A	Y	A
Enkripsi	K	W	K	N	V	A	L	S	N	O	U	L	O	K	R	K	Y	K

Kelebihan :

- Kata kunci yang digunakan tidak terlalu singkat/pendek
- Sulit memdapatkan kata kunci
- Tidak meiliki karakter yang sama

Kelemahan :

- Kata kunci yang digunakan terlalu umum
- Pada akhir abjad tidak berubah
- Kata kunci yang digunakan hanya satu kata

3. Menggunakan kata kunci : PORT USB

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	O	R	T	U	S	B	A	C	D	E	F	G	H	I	J	K	L	M	N	Q	V	W	X	Y	Z

Pesan	A	W	A	S	V	I	R	U	S	B	E	R	B	A	H	A	Y	A
Enkripsi	P	W	P	M	V	C	L	Q	M	O	U	L	O	P	A	P	Y	P

Kelebihan :

- Menggunakan Lebih dari satu kata kunci
- Kata kunci yang digunakan sulit ditebak
- Kata kunci yang berbeda karakter

Kelemahan :

- Kata kunci singkat
- Akhiran abjad tidak berubah

4. Menggunakan kata kunci : SULIT YAH

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	U	L	I	T	Y	A	H	B	C	D	E	F	G	J	K	M	N	O	P	Q	R	V	W	X	Z

Pesan	A	W	A	S	V	I	R	U	S	B	E	R	B	A	H	A	Y	A
Enkripsi	S	V	S	P	R	B	N	Q	O	U	T	N	U	S	H	S	X	S

Kelebihan :

- Hanya terdapat dua karakter yang sama dalam abjad yakni : H , Z .
- Sulit menerka kata kuncinya

Kekurangan :

- Meski telah memakai dua kata yang tidak umum tetapi kata kuncinya terlalu singkat

5. Menggunakan kata kunci : ZEBRA

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	E	B	R	A	C	D	F	G	H	I	J	K	L	M	N	O	P	Q	S	T	U	V	W	X	Y

Pesan	A	W	A	S	V	I	R	U	S	B	E	R	B	A	H	A	Y	A
Enkripsi	Z	V	Z	Q	U	G	P	T	Q	E	A	P	E	Z	F	Z	X	Z

Kelebihan :

- Tidak memiliki karakter yang sama pada abjad
- Kata kunci yang digunakan tidak umum

Kekurangan :

- Kata yang digunakan sebagai kata kunci terlalu singkat.

Gambar 9. Tampilan ikon aplikasi steganografi beserta tampilan menu utama setelah program dibuka.

Gambar 10. Tampilan menu input dengan melakukan pencarian pada direktori data input berupa gambar logo BMKG yang akan disisipkan pesan *text* informasi dini tsunami.

Berikut ini merupakan beberapa contoh hasil *running* dari teknik steganografi berbasis android. Pada aplikasi tersebut diasumsikan bahwa tiap petugas wilayah terdampak tsunami telah diberikan aplikasi untuk melakukan *decoding* yang dalam hal ini membuka pesan privasi atau rahasia (gambar 9).

Aplikasi yang diberikan sudah termasuk *password* dari pihak admin BMKG untuk membuka pesan rahasia/privasi yang telah dikirimkan. Pada gambar 9 dilakukan *encoding* oleh pihak BMKG.

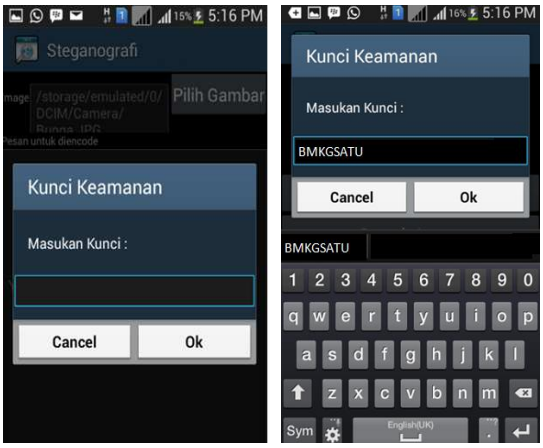
Pada gambar 10, dengan melakukan klik pada *encode image* maka akan muncul

tampilan menu input pemilihan gambar pada gambar 10. Ujicoba dilakukan pada OS android v4.2.2 (Jelly Bean) berbasis linux menggunakan *smartphone* tipe Samsung Grand Duos I9082. Format input dapat beraneka ragam, tetapi besar maksimum *file* gambar yang akan dijadikan media penyisipan berada dibawah 1 Mb.

Gambar 11. Tampilan setelah gambar telah ditetapkan sebagai media penyisipan. Setelah itu dilakukan pengisian pesan yang akan dikirimkan oleh petugas BMKG.

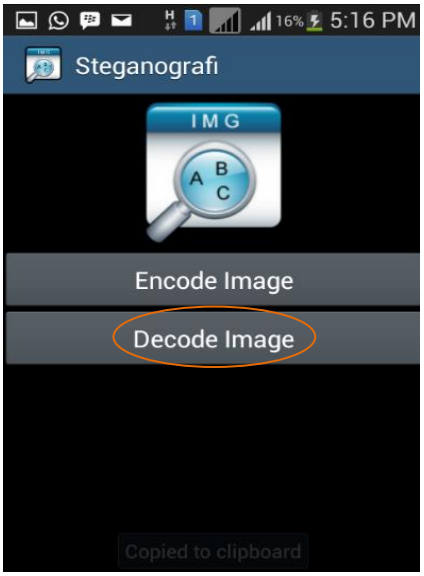
Dalam aplikasi ini digunakan *password* dalam melakukan proses *encode* yang akan digunakan pada saat *decoding*. *Password* yang dibuat diubah dalam bentuk md5 untuk menambah tingkat keamanan (Gambar 11).

Pesan yang dikirim tersimpan dalam folder khusus pada petugas yang telah menerima pengiriman pesan. Kemudian Petugas membuka hasil pengiriman tadi dengan melakukan klik pada *decode image* (gambar 9). Kemudian tampil menu pemilihan gambar pada *aplikasi smartphone* milik petugas (gambar 10).

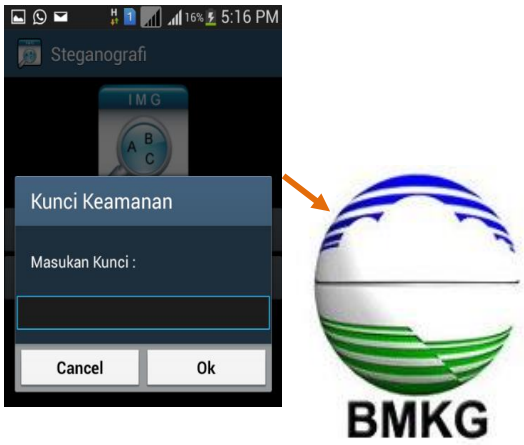


Gambar 12. Tampilan untuk konfirmasi masukkan *password* bagi petugas penerima

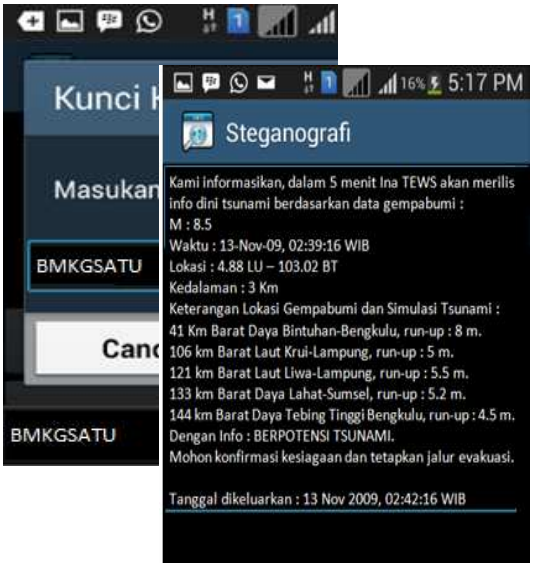
Setelah dilakukan klik pada gambar yang berada pada folder khusus tersebut maka aplikasi meminta *password* sebagai pesan rahasia / privasi agar tidak setiap orang mengetahui password untuk membuka pesan rahasia tersebut (Gambar 13).



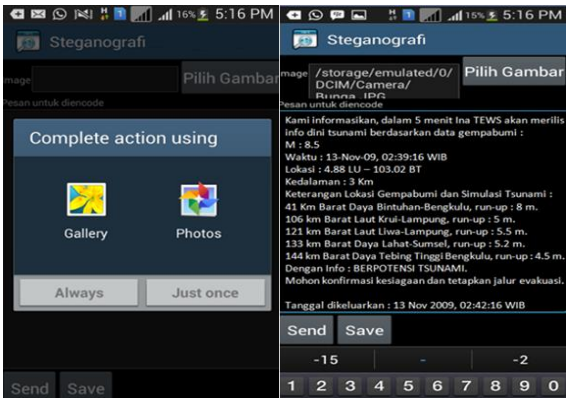
Gambar 13. Langkah selanjutnya, pejabat wilayah terdampak tsunami membuka pesan dengan melakukan *decode* dari pesan



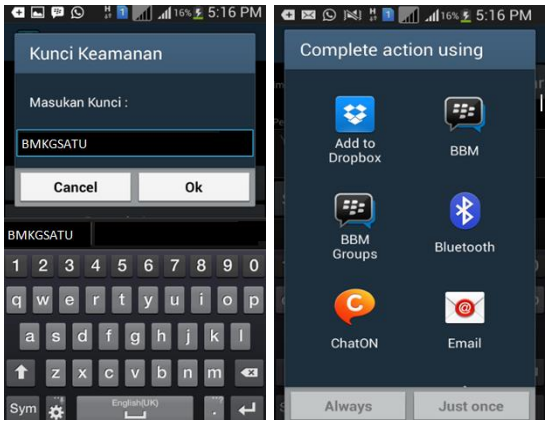
Gambar 14. Tampilan untuk membuka pesan rahasia yang telah terkirim pada aplikasi android dari *smartphone* milik petugas



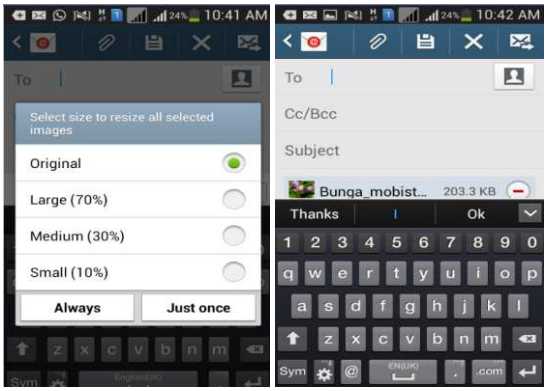
Gambar 15. Setelah input password petugas dapat membaca pesan rahasia informasi dini gempabumi



Gambar 16. Tampilan untuk memulai mengirimkan pesan gambar yang sudah disisipi pesan *text* melalui email. Membuka file dan menyisipkan pesan *text* pada gambar



Gambar 17. Tampilan konfirmasi *password* sebelum mengirimkan media pengiriman pesan gambar yang sudah disisipkan *text* tadi



Gambar 18. Tampilan kirim gambar menggunakan email

Gambar 19**.** Tampilan Inbox pada email dari pesan gambar yang telah dikirimkan oleh aplikasi android

Pengiriman informasi dini gempabumi melalui aplikasi android yang terenkripsi dapat diterima melalui *email* petugas/pejabat yang berwenang. Dengan

demikian jika sistem android tengah bermasalah atau rusak, peran android dapat digantikan dengan email ataupun Bluetooth dan dropbox (Gambar 16, gambar 17 dan gambar 18).

Berikut algoritma yang menjelaskan bagaimana urutan berjalannya aplikasi dari menu utama pada aplikasi sampai dengan menampilkan pesan privasi. Di bawah ini dijelaskan terdapat dua pilihan menu di menu utama, diantaranya Menu *Encode Image* dan Menu *Decode Image* (gambar 14 s.d gambar 19).

1. Tampilkan Menu Utama,
2. Input Pilih
3. If Pilih=Encode Image then
4. Tampilkan Form Encode Image
5. Else
6. Menuju ke baris 2
7. End if
8. Else if Pilih=Decode Image then
9. Tampilkan Form Decode Image
10. Else
11. Menuju ke baris 2
12. End if

Algoritma *Encode Image*

Algoritma di bawah ini menjelaskan proses berjalannya form *Encode Image* pada program aplikasi steganografi metode *LSB*. Untuk urutan proses yang lebih jelas dapat dilihat di bawah ini.

1. Tampilkan Form *Encode Image*
2. Input Pilih
3. If Pilih=Pilih Gambar then
4. Proses Ambil Data Tampil Ke Form
5. Menuju ke baris 2
6. Input Text Rahasia
7. Else if Pilih=Send then
8. Tampilkan Popup Kunci Keamanan
9. If Pilih = OK
10. Proses enkrip
11. Baca Setiap Pixel File Citra
12. Beri Kunci Keamanan Sebelum Pesan
13. Proses encode
14. Else
15. Menuju ke baris 2
16. End if
17. End if

Algoritma *Decode Image*

Algoritma di bawah ini menjelaskan proses berjalannya form *Decode Image* pada program aplikasi steganografi metode *LSB*. Untuk urutan proses yang lebih jelas dapat dilihat di bawah ini.

1. Tampilkan Form Galery Gambar
2. Input Pilih
3. If Pilih= Pilih Gambar
4. Proses Ambil Data Tampil Ke Form
5. Tampilkan Popup Kunci Keamanan
6. If Pilih = OK
7. If Kunci Keamanan = Kunci Keamanan Sebelum Pesan
8. Proses dekrip
9. Proses decode
10. Else
11. Tampilkan Pesan “Gambar Ini tidak terdeteksi pesan rahasia”
12. End If
13. Else
14. Tampilkan Menu Utama
15. End if

KESIMPULAN

Teknik steganografi yang menggunakan metode penyisipan data text dengan metode LSB (*Least Significant Bit*) dan yang menggunakan metode enkripsi *Caesar chipper* pada aplikasi android yang dilakukan bertahap menurut algoritma perancangan/desain program, bahwa pesan privasi/rahasia pada media atau data-data digital yang dikirimkan oleh BMKG sebagai pengirim informasi dini tsunami, akan sampai kepada pihak yang berwenang dengan valid. Dengan demikian pengumuman informasi dini dan evakuasi terhadap warga terdampak tsunami dapat dijalankan sesuai arahan yang jelas dari pimpinan/pejabat yang berwenang.

Uji coba penyisipan LSB dilakukan

dengan memodifikasi bit terahkir dalam satu *byte* (8 Bit). JPG dapat dilakukan *encode* dari pengirim dan *decode* dari penerima dengan menggunakan *password* yang dibuat dan diubah dalam bentuk md5 untuk menambah tingkat keamanan/ kerahasiaan pesan informasi dini potensi tsunami.

Dari hasil penelitan ini, aplikasi dapat dikembangkan dan diterapkan untuk mendukung keamanan informasi dini potensi yang elibatkan integrasi komunikasi antar departemen yang terkait.

DAFTAR PUSTAKA

Aditya. *Isu Gempa dan Tsunami Meresahkan*. *2014*. (http://bengkulueksprss. com/isu-gempa-dan-tsunami-meresahkan/), diakses 23 Juni 2016.

Ariyus, Dony. *Keamanan Multimedia, Penerapan Steganografi dalam Berbagai Bidang Multimedia.* Penerbit Andi Offset, Skripsi Amikom Yogyakarta. 2009.

Asep Juanda. *Penggunaan Metode LSB Dalam Melakukan Steganografi Pada Media Gambar Digital Dengan Menggunakan Matlab.* Skripsi Universitas Teknik Informatika Gunadarma. 2009.

Bahrawi. Eko Setijadi dan Wirawan. *Deteksi Steganogram Untuk Mendukung E-Government.* Prosiding Seminar Nasional Manajemen Teknologi XVII Program Studi MMT-ITS, Fakultas Teknologi Industri Surabaya. ISBN : 978-602-97491-6-8. 2013.

Bander, D. Gruhi, N. A. L. *Techniques For Data Hiding.* Ibm Systems Journal, Vol 35, Nos 3&4, 199. Doi: 0018-8670.1996.

Gunawan, Paul. *Studi dan Analisis Mengenai Teknik Steganalisis Terhadap Pengubahan LSB Pada Gambar: Enhanced LSB dan Chi-square.* Departemen Teknik Informatika ITB, 2007.

Hermawan, Benny. *Menguasai Java 2 & Object Oriented Programming. Perpustakaan Digital Universitas Negeri Malang.* 2004.

Kettle, B. & Sellars, N. *The development of student teachers' practical theory of teaching,* Teaching and Teacher Education, 12, pp. 1-24. 1996.

Kristian Bayu. *Aplikasi Enkripsi SMS Pada Telepon Selular Berbasis J2ME Dengan Metode Vigere Cipher*, Universitas Diponegoro Semarang Prasetyo. 2010.

Munir, Rinaldi. *Steganografi dan Watermaking.* Departemen Teknik Informatika ITB. 2004.

Munir, Rinaldi. *Kriptografi.* Diktat kuliah IF5054 Prodi IF – STEI. 2006.

Morkel, T., Eloff, J.H.P., Olivier, M.S. *An Overview of Image Steganography.* Information and Computer Security Architecture (ICSA) Research Group.2005.

Namiesyva. *Kriptografi Sebagai Media Pembelajaran Dalam studi Matematika Tingkat Sekolah,*. Bandung : ITB. 2007.

Nugroho B, G. *Jokowi Minta Masyarakat Hanya Cari Informasi yang Resmi Soal Gempa. 2016.* (http://news.detik.com/berita/3156985/jokowi-minta-masyarakat-hanya-cari-informasi-yang-resmi-soal-gempa, diakses tanggal 3 Maret 2016.

Patty R. Rahman. *Kepala BPBD Pastikan Isu Tsunami di Ambon Tak Benar. 2013.* (http://edukasi.kompas.com/read/2013/11/25/1120275/Kepala.BPBD.Pastikan.Isu.Tsunami.di.Ambon.Tak.Benar), diakses 23 Juni 2016).

Prasetya, D. *Kapolres ancam pidanakan penyebar isu tsunami di Serang. 2013*.

(http://www.merdeka.com/peristiwa/kapolres-ancam-pidanakan-penyebar-isu-tsunami-di-serang.html), diakses 23 Juni 2016.

Putri, Alatas. *Implementasi Teknik Steganografi Dengan Metode Lsb Pada Citra Digital. Tugas Akhir.* Jurusan Sistem Informasi, Fakultas Ilmu Komputer & Teknologi Informasi, Universitas Gunadarma, 2009.

Rojali, Afan Galih Salman, Teddy Nugraha. *Program Aplikasi Steganografi Menggunakan Metode Spread Spectrum Pada Perangkat Mobile Berbasis Android*. . ComTech. 762-773.Vol.3 No. 2 Desember 2012.

Septiani, M. *Aplikasi watermarking pada mobile device dengan menggunakan J2ME. Repository online,* Skripsi Universitas Gunadharma. 2012.

Setyonegoro W. *"Tsunami Numerical Simulation Applied to Tsunami Early Warning System Along Sumatra Region",* Jurnal Meteorologi dan Geofisika. ISSN 1411-3082, Vol.12.No.1, Hal : 21-32. 2011.

Setyonegoro W, dkk. "*Validasi Pemodelan* Tsunami *Berdasarkan Software L-2008 Menggunakan Data Sumber Gempabumi USGS, IRIS, CMT, dan GFZ untuk Studi Kasus Tsunami Nias 28 Maret 2005*". Jurnal Meteorologi dan Geofisika, ISSN 1411-3082, Vol. 16 No. 1, hal : 25-36. 2015.

Spahn, Vidiarina Harald, Iskandar Leman, Usdianto Benny. *"Checklist for Developing Early Warning Systems".* EWC III Third International Conference on Early Warning "From Concept To Action",Bonn, Jerman. 27 – 29 Maret 2006.

Surya Perkasa. *Gempa 8,3 SR, Warga Padang Panik Mengungsi ke Tempat Tinggi.* 2016. (http://news.metrotvnews.com/read/2016/03/02/492967/gempa-8-3-sr-warga-padang-panik-mengungsi-ke-tempat-tin), diakses 23 Juni 2016.

Wahyu Galih. *Aplikasi Enkripsi SMS Menggunakan Metode Blowfish.* Teknik Informatika PENS-ITS Surabaya. 2010.

Wallansha R dan Setyonegoro W. "*Skenario Tsunami Menggunakan Data Parameter Gempabumi Berdasarkan Kondisi Batimetri (Studi Kasus : Gempabumi Maluku 28 Januari 2004)*". Jurnal Segara Kementerian Kelautan dan Perikanan (KKP), ISSN : 1907-0659, Vol. 11 No. 2, hal : 159-168. 2015.

Win, Junaidi. *Algoritma Hill Chiper Untuk Enkripsi Data Teks Yang Digunakan Untuk Steganografi Gambar Dengan Metode Lsb (Least Significant Bit).* Pelita Informatika Budi Darma, Volume : IX, Nomor: 3, **ISSN :** 2301-9425. 2015.

Permen Kominfo. No. 20, Tahun 2006. Tentang : Peringatan Dini Tsunami atau bencana lainnya Melalui Lembaga Penyiaran di Seluruh Indonesia. Pasal 6 Ayat 2. 2006.