Teknik "*Snap and Share*" pada Aplikasi Steganografi Berbasis Android

Achmad Aditya A. U[#1], Nazori AZ[#2]

[#]*Magister Ilmu Komputer, Universitas Budi Luhur*

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, 12260

[1]achmad.aditya@gmail.com

[2]nazori@budiluhur.ac.id.com

***Abstraksi*— Belakangan muncul aplikasi steganografi yang berbasis Android, namun aplikasi tersebut belum memanfaatkan fitur-fitur yang telah tersedia di sistem operasi Android. Seluruh perangkat bergerak, dalam hal ini *smartphone* dan tablet yang berbasis Android, sudah dilengkapi dengan kamera digital. Kamera digital ini dapat digunakan untuk membuat *cover-image* namun belum dimanfaatkan. *Cover-image* biasanya mengambil citra yang sudah ada, biasanya dari Internet. Sedangkan hasil stego-image pun hanya disimpan, jika ingin mengirimkan hasil stego-image maka harus membuka aplikasi lain semisal email *client* atau web mail jika ingin dikirim melalui email, Facebook atau Twitter bila ingin mengirim lewat kedua *social media* tersebut. Teknik "*Snap and Share*" digunakan untuk memasukkan penggunaan kamera digital langsung untuk membuat *cover-image*, dan metode untuk menyebarkan stego-image ke dalam aplikasi steganografi sehingga aplikasi steganografi ini bisa dilakukan secara *real-time*. Hasilnya adalah melalui teknik "*Snap and Share*" ini aplikasi steganografi dapat dilakukan secara *real-time* untuk membuat *cover-image* dan mengirimkan stego-image.**

Kata kunci: snap and share,* steganografi, pesan rahasia, stego-image, *cover-image,* kamera digital, android, perangkat bergerak, *real-time

Abstract*— *Recently, Android based steganography applications has been developed. Unfortunately, they are not taking advantage of Android's tools. Every Android's smartphones or tablets are embedded with digital camera. This digital can be used to create a cover-image, but it has not been developed. The cover-image is usually made by using an available image from the Internet. The stego-image usually only be saved, if we want to share or send the stego-image we will open another application, such as email client or web mail, or social media like Facebook or Twitter. "Snap and Share" technique is used to embed the advantage of digital camera to create cover-image,and the sharing method of stego-image into steganography application, so it can be done in real-time. By using "Snap and Share" technique it can be done in real-time to create cover-image and share the stego-image.

Keywords: snap and share, steganography, secret message, stego-image,digital camera, android, mobile devices, real-time

I. PENDAHULUAN

Saat ini perangkat bergerak seperti *smartphone* dan tablet telah menjadi bagian dalam kehidupan sehari-hari. Penggunaan perangkat bergerak tersebut bukan lagi sekedar untuk menelepon dan mengirimkan pesan singkat melalui SMS, tapi jauh lebih banyak lagi. Seperti menangkap gambar melalui kamera digital yang kini selalu tersemat dalam perangkat bergerak dan mengirimkannya melalui email, MMS, maupun aplikasi lain yang saat ini sudah sangat populer seperti Facebook, Twitter, Instagram, dan lain-lain.

Dari sekian banyak sistem operasi untuk perangkat bergerak tersebut, sistem operasi Android memuncaki dalam hal jumlah penggunanya. Ada ratusan juta perangkat bergerak di lebih dari 190 negara di seluruh dunia menggunakan Android sebagai platformnya. Hal ini menjadikan Android sebagai sistem operasi *mobile* terbesar dan mempunyai pertumbuhan pengguna tercepat. Sehingga banyak aplikasi dibuat untuk memenuhi kebutuhan pengguna Android.

Keamanan yang merupakan hal yang sangat penting ketika seorang pengguna berkomunikasi dengan pengguna lain pada media seperti internet. Internet menawarkan kemudahan dalam berkomunikasi secara cepat tanpa dibatasi ruang dan waktu. Ketika seseorang menginginkan pesannya hanya dapat dibaca oleh pengguna yang ia maksudkan, maka ia harus memikirkan bagaimana pesan rahasia tersebut dapat dengan aman diterima dan hanya dibaca oleh pengguna tersebut.

Banyak kasus terjadi mengenai penyadapan informasi hingga informasi tidak sampai ke penerima karena dicegat oleh pihak-pihak yang menginginkan informasi tersebut. Sehingga dibuatlah mekanisme pengamanan pesan rahasia dengan menyisipkannya melalui suatu media digital seperti citra, video, teks, maupun suara. Mekanisme pengamanan pesan rahasia ini adalah steganografi.

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Dengan Steganografi maka pemilik data dapat

menyembunyikan informasi hak ciptanya seperti identitas pembuat, tanggal dibuat, hingga pesan kepada seseorang. Steganografi ini menyembunyikan informasi ke dalam berbagai jenis data seperti: gambar, audio, video, teks atau file biner.

Steganografi itu sendiri dianggap sebagai seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan yang telah ada sejak lama. Tujuan penyembunyian pesan rahasia berbeda-beda dari zaman ke zaman, walaupun ada tujuan yang masih digunakan hingga saat ini. Di masa lalu, orang-orang menggunakan tato tersembunyi atau tinta tak terlihat untuk menyampaikan isi steganografi. Hari ini, teknologi jaringan dan komputer menyediakan cara yang lebih mudah untuk menggunakan steganografi. Istilah steganografi pun melebar termasuk penyembunyian data digital dalam berkas/berkas (*file*) komputer. Pada umumnya, pesan steganografi disisipkan pada media lain seperti citra, artikel, daftar belanjaan, atau pesan-pesan lainnya. Pesan rahasia ini menyatu atau disamarkan dengan media yang disisipinya.

Dalam prakteknya, sebenarnya pesan yang disembunyikan akan membuat perubahan tipis terhadap data digital yang disisipinya. namun karena perubahan itu sulit dilihat dengan mata, maka data tersebut tidak akan menarik perhatian dari orang yang tidak berhak untuk membaca pesan tersebut.

Steganografi memanfaatkan media digital untuk menyisipkan pesan rahasia melalui kode biner pada media digital tersebut. Pesan rahasia yang disisipkan ke dalam media digital sedikit banyak akan mengubah tampilan maupun ukuran filenya. Dalam hal ini media digital yang digunakan adalah citra digital. Berkomunikasi dengan saling mengirimkan foto atau citra antar pengguna saat ini sudah semakin populer.

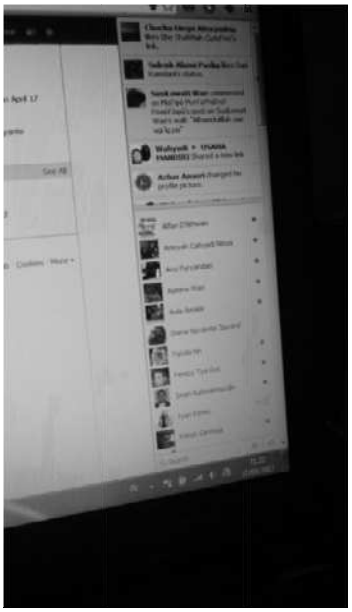
Banyak aplikasi yang memfasilitasi pengguna untuk dengan mudah saling bertukar citra atau foto. Steganografi memungkinkan seseorang untuk menyisipkan pesan rahasia ke dalam citra lalu mengirimkannya ke pengguna yang ia inginkan tanpa diketahui oleh orang lain walaupun orang lain mengetahui proses pengiriman dan penerimaan citra tersebut. Namun, jika citra digital yang digunakan merupakan citra umum yang bisa didapat dengan mudah di internet, maka akan timbul kecurigaan dari orang lain jika ia memiliki citra yang sama namun berbeda dalam hal ukuran atau tampilan citra tersebut. Sehingga prinsip pertama dalam steganografi yaitu tidak menimbulkan kecurigaan akan terlanggar. Lebih jauh lagi, resiko terbacanya pesan rahasia yang disisipkan pada citra tersebut -pada pembahasan selanjutnya disebut stego-image- akan meningkat.

Dalam membuat steganografi ada dua kriteria yang harus diperhatikan, yaitu:

- *Fidelity*. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. pihak ketiga tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
- *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*). karena tujuan steganografi adalah penyembunyian pesan, maka sewaktu-waktu pesan rahasia didalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Aplikasi pengamanan pesan rahasia menggunakan steganografi awalnya dikembangkan hanya untuk komputer atau laptop. Namun seiring semakin dibutuhkannya komunikasi yang cepat dan fleksibel karena meningkatnya teknologi perangkat bergerak, maka komunikasi pesan rahasia juga diharapkan bisa dilakukan dengan cepat, mudah tanpa mengurangi aspek keamanan pesan tersebut. Belakangan ini telah dikembangkan aplikasi steganografi untuk perangkat bergerak seperti handphone dan tablet.

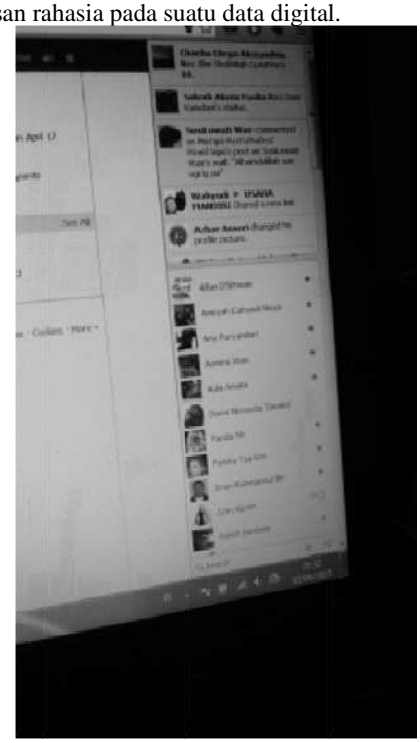
Namun, aplikasi yang dikembangkan ini hanya sekedar menyisipkan pesan rahasia ke dalam citra yang sudah ada. Sementara aspek peningkatan keamanan dengan membuat cover-image sendiri dan pengiriman stego-image melalui berbagai cara belum menjadi perhatian penting. Aplikasi steganografi yang ada hanya memanfaatkan citra yang sudah ada untuk dijadikan *cover-image*, lalu cukup menyimpan stego-image-nya. Jika ingin mengirimkan stego-image kepada orang lain, maka harus membuka aplikasi lain di luar aplikasi steganografi tersebut. Selain itu, citra yang digunakan untuk disisipkan pesan rahasia, atau *cover-image* masih menggunakan citra umum dari Internet sehingga aspek keamanan pesan rahasia masih belum maksimal.



Gbr. 1 *Cover Image* dari Kamera Digital

Secara kasat mata, gambar 1 di atas dan gambar 2 di bawah tidak ada bedanya. Tapi jika digunakan aplikasi pengolah gambar bisa diketahui perbedaan melalui warna jika kedua gambar diperbesar hingga beberapa kali. Prioritas utama dari

Steganografi adalah bagaimana orang lain tidak menyadari bahwa ada pesan rahasia pada suatu data digital.

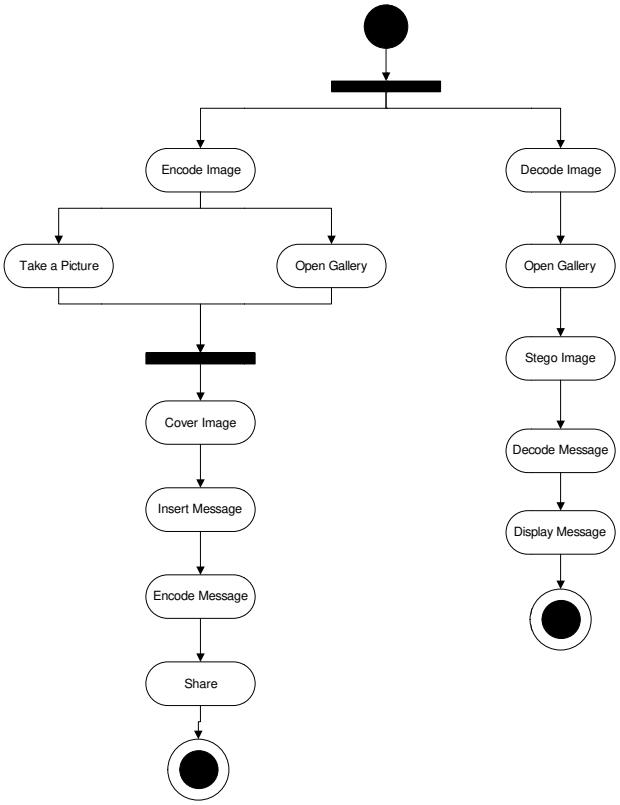


Gbr. 2 Stego Image

Pada penelitian ini, diajukan teknik pengamanan pesan rahasia steganografi pada perangkat bergerak berbasis Android dengan teknik "*Snap and Share*", yaitu sebuah teknik yang memasukkan penggunaan kamera digital sebagai sarana yang ada pada setiap perangkat bergerak berbasis Android untuk membuat *cover-image* sendiri, dan metode untuk menyebarkan stego-image secara langsung ke dalam aplikasi steganografi.

Sebuah program steganografi dibutuhkan untuk melakukan hal-hal implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan, seperti menemukan kelebihan bit dalam dokumen yang dapat digunakan untuk menyembunyikan pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyembunyikan data dan melakukan penyembunyian data dalam bit yang telah dipilih sebelumnya.

Terdapat dua langkah dalam sistem steganografi yaitu proses penyembunyian dan pengambilan data dari media yang disisipi. Penyembunyian data dilakukan dengan mengganti bit-bit data di dalam segmen gambar dengan bit-bit data rahasia. Metode yang paling sederhana adalah metode modifikasi LSB (*Least Significant Bit Modification*). Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (*Most Significant Bit* atau MSB) dan bit yang paling kurang berarti (*Least Significant Bit* atau LSB).



Gbr. 3 Alur Aplikasi

II. PENELITIAN TERKAIT

Tinjauan studi yang dijadikan acuan dalam melakukan penelitian ini mengacu pada beberapa penelitian terkait yang telah dilakukan sebelumnya yaitu sebagai berikut.

1) Penelitian lain yang dilakukan oleh Ritesh Pratap Singh dan Neha Singh [1] yang mengembangkan aplikasi steganografi dengan menggunakan platform MATLAB untuk kemudian bisa dikirim melalui Multimedia Messaging Service (MMS). Teknik yang digunakan adalah CDMA Spread Spectrum, yaitu teknik penyisipan pesan dalam citra dengan mengksploitasi sifat korelatif aditif dari pola Pseudo-Random Noise yang diterapkan pada sebuah citra. Teknik ini menyebarkan setiap bit pesan secara acak di seluruh cover-image, sehingga meningkatkan kapasitas penyimpanan pesan.

Hasil penelitian ini adalah dengan menggunakan teknik algoritma CDMA *Spread Spectrum* bisa meningkatkan kapasitas penyimpanan pesan pada citra tanpa mengubah kualitas citra secara berarti. Selain itu keamanan pesan juga tetap tinggi karena menggunakan teknik penyebaran bit secara acak, sehingga sulit dideteksi. Namun, teknik pengambilan *cover-image* masih menggunakan citra yang sudah ada dan media pengiriman stego-image masih menggunakan MMS sehingga untuk mengirimkan lewat teknik lain harus

membuka aplikasi lain, selain itu hanya terbatas antar *mobile phone.*

2) Penelitian untuk mengamankan pesan rahasia dengan steganografi melalui MMS dengan teknik kriptografi *Elliptic Curve* dilakukan oleh Prof. B.N. Jagdale, Prof. R.K. Bedi dan Sharmishta Desai [2]. *Elliptic Curve Criptography* (ECC) adalah sebuah *public key* dari kriptografi. ECC menawarkan keamanan yang setara dengan teknik kriptografi lain semisal RSA dan DH, namun ECC memiliki ukuran kunci yang lebih kecil, sehingga lebih cepat dalam komputasi. Selain itu ECC juga sangat rendah dalam mengkonsumsi memori dan *bandwidth*, sehingga sangat cocok untuk perangkat mobile.

Hasil penelitian, teknik ECC sangat sesuai untuk pengamanan pesan pada perangkat bergerak, karena tidak membutuhkan resource yang besar, namun hasil stego-image hanya dapat dikirimkan melalui MMS dan untuk mengirimkan lewat teknik lain, harus membuka aplikasi lain. Selain itu cover-image didapat dari citra yang sudah ada, tanpa bisa membuat sendiri melalui kamera.

3) Penelitian mengenai pengembangan aplikasi untuk steganografi sebelumnya telah dilakukan oleh Wesam S. Bhaya [3]. Pada aplikasi yang dikembangkan ini, steganografi dilakukan pada *Simple Message Service* (SMS) pada *mobile phone*. Penyisipan dilakukan dengan mengganti *font* dari *font* yang ada pada setiap perangkat, yaitu *System Font* dan *Proportional Font. Font* pengganti ini mempunyai bentuk yang mirip dengan *font* yang telah ada, dan tidak dapat ditemukan perbedaannya secara kasat mata. Pesan yang disisipkan berupa satu karakter per satu *font.* Aplikasi ini dikembangkan dengan pemrograman *Java 2 Micro Edition* (J2ME).

4) Hasil dari penelitian ini adalah penerima tidak dapat membuka pesan rahasia bila tidak mengetahui kunci pembukanya. Aspek keamanan telah terpenuhi di dalam aplikasi ini, namun pesan rahasia masih terbatas dilakukan dengan SMS.

5) Penelitian lain mengenai pengembangan keamanan melalui steganografi pada mobile phone juga telah dilakukan oleh Yogendra Kumar Jain, Roopesh Kumar, dan Pankaj Agarwal [4]. Aplikasi yang dikembangkan ini juga mengirimkan hasil citra steganografinya melalui MMS. Algoritma yang digunakan adalah *Discrete Cosine Transform* (DCT) dan *Tiny Encription Algorithm* (TEA). *Discrete Cosine Transform* merepresentasikan sebuah citra dari penjumlahan sinusoida dari magnitude dan frekuensi yang berubah-ubah. Sifat dari DCT adalah mengubah informasi citra yang signifikan dikonsentrasikan hanya pada beberapa koefisien DCT. DCT menghitung kuantitas bit-bit citra dimana pesan tersebut disembunyikan didalamnya. Algoritma TEA merupakan algoritma penyandian *block cipher* yang dirancang untuk penggunaan memori yang seminimal mungkin dengan kecepatan proses yang maksimal. Sistem penyandian TEA menambahkan fungsi matematik berupa penambahan dan pengurangan sebagai operator pembalik selain XOR. Hal ini dimaksudkan untuk menciptakan sifat non-linearitas. Pergeseran dua arah (ke kiri dan ke kanan) menyebabkan semua bit kunci dan data bercampur secara berulang ulang.

Hasil penelitian tersebut menyebutkan keamanan dari pesan yang disisipkan lebih tinggi, karena pesan dienkripsi terlebih dahulu baru disisipkan ke dalam citra. Dari aspek keamanan pesan rahasia memang lebih terjaga dengan adanya enkripsi di awal, namun citra yang digunakan mengambil citra yang sudah ada, tanpa menggunakan citra sendiri yang diambil melalui kamera. Selain itu kemudahan dalam mengirimkan stego-image baru sebatas melalui MMS.

6) Penelitian lainnya tentang steganografi dilakukan juga oleh S. Mohanapriya [5]. Di dalam aplikasi yang dibuat ini, steganografi dilakukan dengan teknik *Discrete Cosine Transform* (DCT) dan algoritma F5, dan hasilnya bisa disebarkan melalui *Multimedia Messaging Service* (MMS). Algoritma F5 secara acak menyisipkan bit-bit yang terpilih oleh koefisien DCT dan membuat matriks penyisipan yang akan meminimalkan perubahan oleh pesan yang disisipkan dengan panjang tertentu.

Hasil penelitian tersebut adalah bahwa keamanan pesan rahasia yang disisipkan sudah melalui keamanan berlapis dengan dua teknik keamanan, sehingga sangat sulit untuk dipecahkan. Namun, stego-image tersebut hanya bisa dikirimkan melalui MMS yang terbatas hanya untuk citra berukuran maksimal 300KB. Sehingga kemudahan dalam membuat cover-image dan mengirimkan stego-image masih belum maksimal.

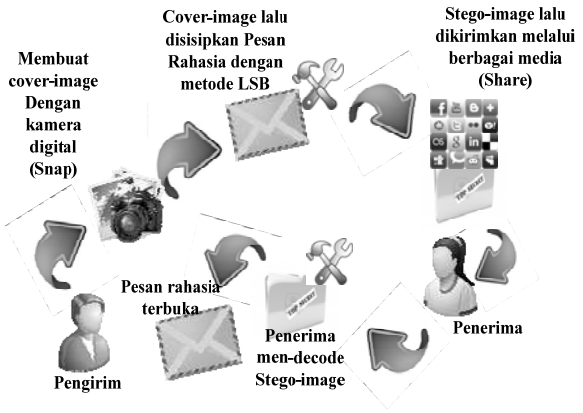
7) Penelitian mengenai pengembangan steganografi melalui aplikasi berbasis Android telah dilakukan oleh Rosziati Ibrahim dan Law Chia Kee [6]. Sistem yang dikembangkan mengamankan citra dengan steganografi lalu dikirimkan melalui *Multimedia Messaging Service* (MMS) dan email. Aplikasi ini menambahkan tambahan keamanan berupa *password* atau *key* pada citra stego. Algoritma yang digunakan adalah Huffman Encoder, dimana teknik ini memendekkan karakter jika karakter tersebut berulang sehingga pesan menjadi lebih pendek, namun jika karakter yang dipakai di dalam pesan tidak berulang, maka pesan yang disimpan menjadi lebih panjang. Bahasa pemrograman yang digunakan dalam aplikasi ini adalah Java dan *Extensible Markup Language* (XML).

Hasil penelitian menyebutkan bahwa proses stegano pada sebuah citra yang diambil bisa melalui kamera digital yang tersemat dalam perangkat dan mengirimkannya melalui MMS atau email telah berhasil dilakukan. Aspek keamanan pesan telah ditingkatkan melalui penggunaan kamera digital, namun kemudahan dalam mengirimkan stego-image baru hanya sebatas melalui MMS dan email.

III. IMPLEMENTASI

Teknik *"Snap and Share"* adalah sebuah teknik yang sering digunakan dalam dunia fotografi dan internet. *Snap* berarti melakukan pengambilan citra dengan cepat melalui kamera digital. Sedangkan *share* adalah melakukan pengiriman atau penyebaran suatu data kepada orang lain. Teknik "*Snap and Share*" dapat dikatakan sebagai teknik mengambil citra dengan cepat melalui kamera digital lalu dengan mudah menyebarkan atau mengirimkan citra tersebut.

Pada penelitian ini teknik "*Snap and Share*" merupakan inti dari alternatif solusi guna menyelesaikan permasalahan penelitian yang dituangkan dalam rumusan masalah. Perancangan teknik "*Snap and Share*" nantinya akan diimplementasikan pada perangkat bergerak berbasis Android menggunakan bahasa pemrograman Java. Gambar 3 di bawah ini memberikan gambaran yang jelas mengenai teknik "*Snap and Share*" yang akan diimplementasikan.



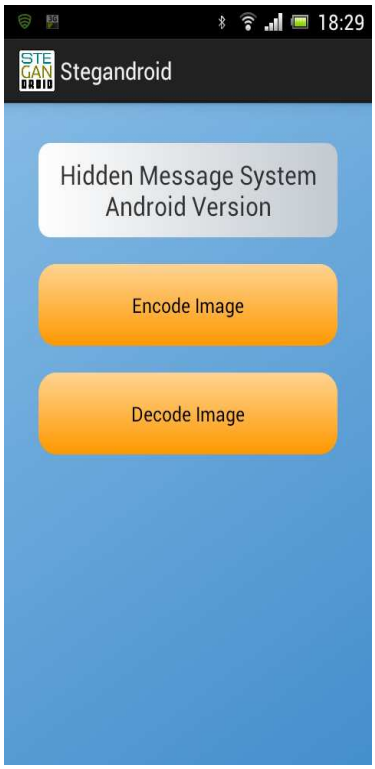
Gbr. 4 Proses teknik "*Snap and Share*" dalam aplikasi steganografi yang dikembangkan

Secara singkat perancangan teknik "*Snap and Share*" digambarkan pada gambar di atas dapat dijelaskan sebagai berikut. Pengirim dan penerima adalah pengguna yang akan saling berkomunikasi pesan rahasia dimana pengirim akan mengirimkan pesan rahasia di dalam sebuah citra melalui steganografi kepada penerima. Untuk dapat saling berkomunikasi maka masing-masing pengguna harus memasang aplikasi ini pada perangkat bergerak miliknya. Pertama, pengirim membutuhkan cover-image, sebuah citra yang akan menjadi media penampung pesan rahasia.

Pengirim mengaktifkan fungsi kamera digital melalui aplikasi ini, lalu menjepret atau snap, selanjutnya pengirim menyisipkan pesan rahasia ke dalam foto tersebut. Pesan rahasia akan disisipkan melalui metode LSB ke dalam foto atau citra. Terakhir, pengirim bisa langsung membagikan atau share citra yang sudah disisipi pesan rahasia atau stego-image melalui berbagai media seperti email, MMS, *Bluetooth, Social Media, Instant Messaging*, dan lain-lain tanpa harus keluar dari aplikasi atau menjalankan aplikasi lain.

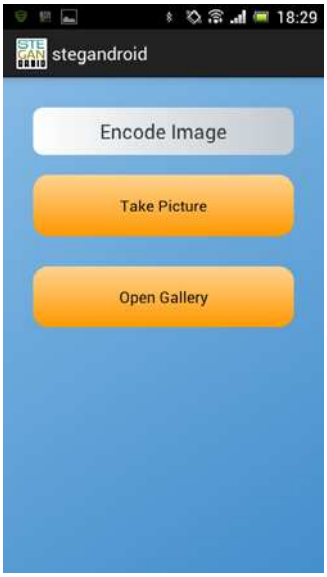
Sementara penerima, setelah menerima atau mengunduh stego-image dari pengirim, dapat langsung men-*decode* pesan rahasia di dalamnya dan dapat langsung melihat isinya.

Ketika aplikasi dijalankan, pertama kali yang muncul adalah halaman utama yang berisi menu pilihan. Ada pilihan *encode* dan *decode*. Bila pengirim ingin mengirimkan pesan rahasia, maka ia harus memilih encode untuk memulainya. Lihat gambar 5.



Gbr. 5 Layar Menu Utama

Setelah pengirim menekan tombol *encode*, maka akan muncul layar *encode image*. Disini pengirim akan membuat atau mengambil *cover-image*. Jika citra belum ada, maka pengirim bisa membuatnya melalui kamera digital. Untuk mengaktifkannya pengirim bisa langsung menekan tombol *take a picture*. Namun, jika citra yang akan dijadikan *cover-image* sudah ada, maka pengirim bisa mengambilnya di *gallery* dengan menekan tombol *open gallery*. Ditunjukkan pada gambar 6 di bawah.



Gbr. 6 Membuat Cover Image

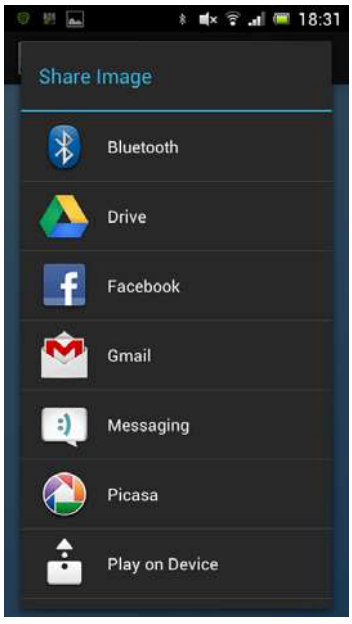
Setelah pengirim membuat atau mengambil citra sebagai *cover-image*, maka selanjutnya pengirim menyisipkan pesan rahasia yang akan disisipkan melalui metode LSB oleh sistem. Seperti gambar 7 di bawah ini.

Gbr. 7 *Inserting Secret Message*

Terakhir, pengirim dapat langsung menyebarluaskan atau share hasil steganografi tersebut dengan menekan tombol share. Seperti ditunjukkan pada gambar 8.

Gbr. 8 *Sharing Stego Image*

Hasil steganografi atau stego-image, citra yang di dalamnya telah berisi pesan rahasia dapat di-*share* dengan berbagai macam metode, seperti *Bluetooh, Drive, Facebook, Twitter, Gmail, Messaging (MMS), Whatsapp,* dan masih banyak media lain tergantung aplikasi yang dipasang pada setiap perangkat. Hal ini ditunjukkan pada gambar 9.

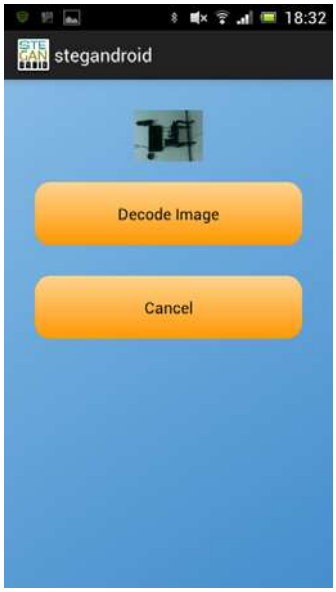


Gbr. 9 Berbagai cara untuk Share Stego Image

Ketika pengguna ingin membaca pesan rahasia yang ia dapatkan, atau si penerima. Maka dari halaman utama pada gambar 5 ia harus memilih *decode image*. Akan muncul tampilan seperti pada gambar 10 di bawah.

Gbr. 10 Memilih Stego Image

Penerima diminta untuk memasukkan stego-image yang telah ia terima. Setelah itu barulah akan muncul tombol *decode* seperti pada gambar 11 di bawah ini.



Gbr. 11 *Decoding Image*

Setelah tombol decode ditekan, maka akan muncullah pesan rahasia, seperti yang ditunjukkan pada gambar 12 di bawah ini.

Gbr. 12 Tampilan Pesan Rahasia

IV. KESIMPULAN

Steganografi merupakan salah satu bentuk komunikasi dengan pesan rahasia. Steganografi banyak digunakan oleh pihak militer atau intelijen dalam berkomunikasi satu sama lain. Namun tidak sedikit pula masyarakat umum yang menggunakan steganografi untuk kepentingan pribadi. Hal ini dikarenakan kebutuhan untuk berkomunikasi secara rahasia melalui jaringan publik seperti internet yang sangat rentan untuk disadap atau diketahui oleh orang lain. Aplikasi steganografi banyak dikembangkan yang berbasis desktop, dan belakangan sudah ada aplikasi steganografi yang dikembangkan untuk perangkat bergerak seperti *handphone* atau tablet. Hal ini memudahkan untuk melakukan komunikasi secara rahasia tersebut. Tetapi aplikasi steganografi yang dikembangkan belum memperhatikan sisi kemudahan berkomunikasi, karena aplikasi tersebut hanya melakukan penyisipan pesan rahasia, tanpa didukung untuk pembuatan *cover-image* dan pengiriman stego-imagenya.

Dalam penelitian yang telah dilakukan maka kesimpulan yang diperoleh adalah bahwa dengan teknik "*Snap and Share*" yang diterapkan ke dalam aplikasi steganografi pada perangkat bergerak berbasis Android, dapat meningkatkan proses berkomunikasi pesan rahasia menjadi real-time dengan tidak membutuhkan aplikasi lain untuk dijalankan.

DAFTAR PUSTAKA

[1] Ritesh Pratap Singh and Neha Singh, *Steganography in Multimedia Messaging Service of Mobile Phones Using CDMA Spread Spectrum*, AKGEC Journal of Technology, vol. 1, 2008.

[2] Prof. B.N. Jagdale, Prof. R.K. Bedi, Sharmishta Desai, *Securing MMS with High Performance Elliptic Curve Criptography*, International Journal of Computer Application, vol. 8, Oktober 2010.

[3] Wesam S. Bhaya, *Text Hiding in Mobile Phone Simple Message Service Using Fonts*, Journal of Computer Science 7, 2011.

[4] Yogendra Kumar Jain, Roopesh Kumar and Pankaj Agarwal (2011), *Securing Data Using Jpeg Image over Mobile Phone*, Global Journal of Computer Science and Technology, Volume 11, Issue 13, Version 1.0, August 2011.

[5] S. Mohanapriya, *Design and Implementation of Steganography Along with Secured Message Services in Mobile Phones*, International Journal of Emerging Technology and Advanced Engineering, vol. 2, Mei 2012.

[6] Rosziati Ibrahim and Law Chia Kee (2012), *MoBiSiS: An-Android based Application for Sending Stego Image through MMS*, ICCGI 2012 : The Seventh International Multi-Conference on Computing in the Global Information Technology (2012).