

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

TESIS



Oleh:

Achmad Aditya Ashadul Ushud

1111601256

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2013

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

TESIS

Diajukan sebagai salah satu persyaratan
untuk mendapatkan gelar Magister Ilmu Komputer (MKom)



Oleh:

Achmad Aditya Ashadul Ushud
1111601256

PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR

JAKARTA

2013



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Achmad Aditya Ashadul Ushud
NIM : 1111601256
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Topik/Judul Tesis : Teknik "*Snap and Share*" pada Aplikasi
Steganografi Berbasis Android

Jakarta, 22 Agustus 2013

Tim Penguji

Tanda Tangan

Ketua,
Dr. Moedjiono, M.Sc

Anggota,
Ir. Wendi Usino, M.Sc, MM, Ph.D

Pembimbing,
Dr. Ir. Nazori AZ, M.T

Ketua Program Studi

Dr. Ir. Nazori AZ, M.T

ABSTRAK

Berkomunikasi dalam dunia maya merupakan suatu hal yang biasa dilakukan. Ada kalanya komunikasi dilakukan secara rahasia dengan mengirimkan pesan rahasia kepada orang tertentu. Dalam hal ini, keamanan menjadi faktor terpenting untuk mengamankan pesan rahasia sehingga hanya dapat dibaca oleh orang yang diinginkan. Steganografi menawarkan keamanan pesan yang disisipkan pada berbagai media, salah satunya media citra. Sayangnya kemudahan dalam berkomunikasi melalui steganografi saat ini belum maksimal. Komunikasi dilakukan hanya melalui *pc* atau *laptop* dan belum secara *real-time*. 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

In the internet, communicating is usual activity. Sometimes conversations is done by sending secret messages to a certain person. In this case, security being the most important factor for securing a secret message that can only be read by those who desired. Steganography offers secure message which is inserted on a variety of media, one of them is image. Unfortunately, communicating through steganography application has not an easy task. Communication is done only through the pc or laptop based application and not real-time. 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*

KATA PENGANTAR

Assalamu'alaikum Warahamtullahi Wabarakatuh.

Segala puji hanya untuk dan kepada Allah swt, yang memberikan kekuatan, izin dan pertolongan, hingga akhirnya tesis yang berjudul "TEKNIK "SNAP AND SHARE" PADA APLIKASI STEGANOGRAFI BERBASIS ANDROID" ini dapat diselesaikan. Dalam penyusunan tesis ini, penulis ingin menyampaikan ucapan terima kasih kepada:

1. Allah swt, atas segala rahmat, izin dan pertolongan-Nya dalam proses penyusunan ini dari awal hingga akhir.
2. Kedua orang tua, Ariful Fuadhi dan Sumartini, yang telah banyak berjasa dengan memberikan bantuan dan dukungan penuh.
3. Titin Fatimah, selaku istri tercinta yang tak henti-hentinya memberikan motivasi dan energi.
4. Azka Athallah Asadul Usud dan Aghniya Izza Naura, yang dengan caranya sendiri dalam memberikan keceriaan, semangat, dan tujuan.
5. Bapak Dr. Ir. Nazori AZ, MT, selaku pembimbing yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini.
6. Bapak Dr. Moedjiono, M.Sc, selaku Direktur Program Pascasarjana yang telah memberikan saran dan masukan dalam penyusunan naskah akhir tesis ini.
7. Serta semua pihak yang tidak dapat dituliskan satu persatu.

Sebagai seorang manusia yang selalu memiliki kekurangan, penulis menyadari bahwa naskah akhir tesis ini masih banyak kekurangan. Oleh karena itu demi menyempurnakan naskah tesis ini, segala bentuk saran dan kritik mohon dapat dikirimkan melalui *e-mail* ke alamat achmad.aditya@gmail.com.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Jakarta, Agustus 2013

Achmad Aditya A U

DAFTAR ISI

	Halaman
ABSTRAK	i
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Masalah Penelitian	3
1.2.1 Identifikasi Masalah	3
1.2.2 Pembatasan Masalah	4
1.2.3 Rumusan Masalah	4
1.3 Tujuan dan Manfaat Penelitian	4
1.3.1 Tujuan Penelitian	4
1.3.2 Manfaat Penelitian	5
1.4 Tata Urut Penulisan	5
1.5 Daftar Pengertian	6
BAB II LANDASAN PEMIKIRAN	7
2.1 Tinjauan Pustaka	7
2.1.1 Kamera Digital	7
2.1.2 Steganografi	8

2.1.3 Teknik " <i>Snap and Share</i> "	14
2.1.4 <i>Least Significant Bit</i>	14
2.1.5 Steganalisis	16
2.1.6 Java	16
2.2 Tinjauan Studi	17
2.3 Tinjauan Obyek Penelitian	23
2.3.1 Perangkat Keras	23
2.3.2 Perangkat Lunak	24
2.4 Pola Pikir	26
2.5 Hipotesis	27
BAB III LANDASAN PEMIKIRAN	28
3.1 Metode Penelitian	28
3.2 Metode Pengumpulan Data	28
3.3 Instrumentasi	28
3.4 Teknik Analisis Data	29
3.5 Langkah-langkah Penelitian	29
3.5.1 Perumusan Masalah	30
3.5.2 Studi Kepustakaan	30
3.5.3 Memformulasikan Hipotesis	31
3.5.4 Perancangan dan Pengembangan Sistem	31
3.5.5 Algoritma Sistem yang dikembangkan	31
3.5.6 <i>Flowchart</i> Sistem yang dikembangkan	32
3.5.7 Pengujian dan Analisis	33

3.5.8 Rencana Implementasi	33
3.5.9 Penarikan Kesimpulan	33
3.6 Jadwal Penelitian	33
BAB IV ANALISIS, INTERPRETASI, DAN IMPLIKASI PENELITIAN	35
4.1 Analisis Sistem	35
4.1.1 <i>Actor</i>	35
4.1.2 <i>Use Case Diagram</i>	35
4.1.3 <i>Activity Diagram</i>	41
4.2 Perancangan Sistem	43
4.2.1 Perancangan Teknik " <i>Snap and Share</i> "	43
4.2.2 Perancangan Layar Aplikasi	45
4.3 Implementasi Sistem	50
4.3.1 Spesifikasi Perangkat Keras	50
4.3.2 Spesifikasi Perangkat Lunak	50
4.3.3 Implementasi Program	51
4.4 Pengujian Sistem	58
4.4.1 Pengujian <i>Black Box</i>	58
4.5 Implikasi Penelitian	61
4.6.1 Aspek Sistem	61
4.6.2 Aspek Manajerial	62
4.6.2 Aspek Penelitian Lanjutan	62
4.6 Rencana Implementasi	64

BAB V PENUTUP	66
5.1 Kesimpulan	66
5.2 Saran	66
5.3 Rencana Implementasi	67
DAFTAR PUSTAKA	68
LAMPIRAN	70
LAMPIRAN I KODING PROGRAM	70
LAMPIRAN II RIWAYAT HIDUP	89



DAFTAR GAMBAR

Gambar	Halaman
I-1 Pengiriman dan <i>Market Share</i> Sistem Operasi <i>Smartphone</i>	1
II-1 Proses Pengambilan Citra Melalui Kamera Digital	8
II-2 Contoh Gambar Sebelum disisipi Pesan	9
II-3 Contoh Gambar Setelah disisipi Pesan	10
II-4 Citra Biner	11
II-5 Representasi Citra Biner	11
II-6 Citra <i>Grayscale</i>	12
II-7 Citra Berwarna	12
II-8 Ilustrasi Dasar Konsep Steganografi	13
II-9 Bit pada MSB dan LSB	14
II-10 Pola Pikir	26
III-1 Langkah-langkah Penelitian	30
III-2 <i>Flowchart</i> Sistem yang dikembangkan	32
IV-1 <i>Encode Message Use Case Diagram</i> Aplikasi	37
IV-2 <i>Decode Message Use Case Diagram</i> Aplikasi	38
IV-3 <i>Activity Diagram</i> Aplikasi	41
IV-4 <i>Sequence Diagram</i> Pengirim	42
IV-5 <i>Sequence Diagram</i> Penerima	42
IV-6 Proses Teknik " <i>Snap and Share</i> " dalam Aplikasi	44
IV-7 Rancangan Layar Halaman Utama	45
IV-8 Rancangan Layar <i>Encode Image</i>	46

IV-9	Rancangan Layar <i>Insert Message</i>	47
IV-10	Rancangan Layar <i>Share</i>	47
IV-11	Rancangan Layar <i>Media Share</i>	48
IV-12	Rancangan Layar <i>Decode</i>	48
IV-13	Rancangan Layar <i>Decode Image</i>	49
IV-14	Rancangan Layar Pesan Rahasia	49
IV-15	Tampilan Halaman Utama	52
IV-16	Tampilan <i>Encode</i>	53
IV-17	Tampilan <i>Encode Message</i>	54
IV-18	Tampilan Proses <i>Share</i>	55
IV-19	Tampilan Pilihan <i>Share</i>	55
IV-20	Tampilan <i>Decode</i>	56
IV-21	Tampilan <i>Decode Image</i>	57
IV-22	Tampilan Pesan Rahasia	57

DAFTAR TABEL

Gambar	Halaman
II-1 Ringkasan Penelitian Terkait	20
III-1 Jadwal Penelitian	34
IV-1 <i>Encode Message Use Case</i> Aplikasi	37
IV-2 <i>Decode Message Use Case</i> Aplikasi	39
IV-3 Spesifikasi perangkat Keras	50
IV-4 Spesifikasi perangkat Lunak	51
IV-5 Hasil Pengujian <i>Black Box</i> Proses Pengambilan Citra	58
IV-6 Hasil Pengujian <i>Black Box</i> Proses <i>Encode</i>	59
IV-7 Hasil Pengujian <i>Black Box</i> Proses <i>Share</i>	60
IV-8 Hasil Pengujian <i>Black Box</i> Proses <i>Decode</i>	61
IV-9 Rencana Implementasi	64

DAFTAR LAMPIRAN

	Halaman
LAMPIRAN I KODING PROGRAM	70
LAMPIRAN II RIWAYAT HIDUP	89



DAFTAR PUSTAKA

- [Cory 2013] Cory Janssen. *Share*, 2013. <http://www.techopedia.com/definition/24839/information-sharing>. (Diakses 14 Juli 2013).
- [DCZone 2011] Sybill. *How Digital Camera Works as Explained Simply*, 2011. <http://idigitalphotography.blogspot.com/2011/09/how-digital-camera-works-as-explained.html/>. (Diakses 14 Juli 2013).
- [Eiji 2011] Eiji Kawaguchi, *Invitation to BPCS Steganography*, 2011, <http://datahide.com/BPCSe/index.html>, (Diakses 18 Juni 2013).
- [Houghton 2000] Houghton Mifflin, *Gadget*, 2000, <http://www.thefreedictionary.com/gadget>, (Diakses 17 Juni 2013).
- [Ingrid 2012] Ingrid Lunden, Gartner: *Android Accounted For 72% Of Smartphone Sales In Q3, Overall Sales Of Mobile Handsets Down 3%*, 2012, <http://techcrunch.com/2012/11/14/gartner-samsung-widens-its-lead-over-apple-in-smartphones-in-q3-but-overall-sales-of-mobile-handsets-down-3/>, (Diakses 17 Juni 2013).
- [Jagdale 2010] Prof. B.N. Jagdale, Prof. R.K. Bedi, Sharmishta Desai, *Securing MMS with High Performance Elliptic Curve Cryptography*, International Journal of Computer Application, vol. 8, Oktober 2010.
- [Merriam-Webster 2000] Merriam-Webster, *Definition of Steganography*, 2000, <http://www.merriam-webster.com/dictionary/steganography>, (Diakses 18 Juni 2013).
- [Mohanapriya 2012] 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.
- [Namita 2010] Namita Tiwari and Dr. Madhu Shandilya, *Evaluation of Various LSB based Methods of Image Steganography on GIF File Format*, International Journal of Computer Applications, vol. 6, September 2010.
- [Niels 2001] Niels Provos, *First Steganographic Image in The Wild*, 2001, <http://www.citi.umich.edu/u/provos/stego/abc.html>, (Diakses 18 Juni 2013).
- [Niels 2002] Niels Provos and Peter Honeyman, *Detecting Stegaraphic Content on the Internet*, Proceeding of the Network and Distributed System Symposium, San Diego, CA, February 2002.