

**PENGEMBANGAN SISTEM OTENTIKASI DI
APLIKASI BERBASIS *ANDROID* DENGAN PENERAPAN
GAMBAR *DIGITAL* SEBAGAI *PASSWORD***

TESIS



**Oleh :
Didit Dwi Permadi
1411601550**

**PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2017**

**PENGEMBANGAN SISTEM OTENTIKASI DI
APLIKASI BERBASIS *ANDROID* DENGAN PENERAPAN
GAMBAR *DIGITAL* SEBAGAI *PASSWORD***

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)



**Oleh :
Didit Dwi Permadi
1411601550**

**PROGRAM STUDI MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCA SARJANA
UNIVERSITAS BUDI LUHUR
JAKARTA
2017**



**PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PERNYATAAN

Nama Mahasiswa : Didit Dwi Permadi
NIM : 1411601550
Konsentrasi : Rekayasa Komputasi Terapan
Program Studi : Magister Ilmu Komputer
Fakultas/Program : Pascasarjana

menyatakan bahwa Tesis yang berjudul:

**PENGEMBANGAN SISTEM OTENTIKASI DI APLIKASI BERBASIS
ANDROID DENGAN PENERAPAN GAMBAR DIGITAL SEBAGAI
PASSWORD**

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 24 Januari 2017



(Didit Dwi Permadi)



PROGRAM STUDI MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Didit Dwi Permadi
NIM : 1411601550
Konsentrasi : Rekayasa Komputasi Terapan
Program Studi : Magister Ilmu Komputer
Topik/ Judul Tesis : Pengembangan Sistem Otentikasi Di Aplikasi
Berbasis *Android* Dengan Penerapan
Gambar *Digital* Sebagai *Password*

Jakarta, Februari 2017

Tim Penguji

Tanda tangan

Ketua,

(Dr., M. Syafrullah, M.Kom., M.Sc.)

Anggota,

(Utomo Budiyanto, M.Kom., M.Sc.)

Pembimbing Utama,

(Dr., Ir. Nazori AZ, M.T.)

Ketua Program Studi

(Dr., M. Syafrullah, M.Kom., M.Sc.)

ABSTRAK

Keamanan data informasi rahasia pada *platform mobile* telah menjadi topik permasalahan utama untuk para pengembang aplikasi. Hal tersebut dapat dicapai dengan cara menyediakan sistem otentikasi yang baik. Salah satu teknik otentikasi yaitu melalui penggunaan *password* berbasis tekstual. Pada teknik tipe ini, umumnya dilakukan enkripsi data pada *password* yang ada untuk memberikan keamanan yang lebih. Akan tetapi pada teknik seperti ini juga memiliki beberapa kelemahan karena pengguna lebih cenderung memilih *password* dari kata-kata yang berarti atau bermakna bersumber dari kamus atau beberapa hal yang berhubungan dengan identitas si pengguna, sehingga membuat *password* tekstual mudah ditebak dan rentan terhadap serangan *brute force*. Guna mencegah kejadian tersebut, teknik otentikasi baru diusulkan dalam tesis ini dalam upaya pengembangan sistem untuk menyediakan alternatif bagi sistem otentikasi yaitu dengan menggunakan kombinasi teknik kriptografi dan steganografi. Semua data dan informasi penting seperti *password* tekstual akan dienkripsi terlebih dahulu dengan *Data Encryption Standard (DES)* kemudian hasil enkripsi tersebut akan disimpan dalam suatu gambar yang disebut gambar *cover* dengan menggunakan teknik steganografi. Teknik steganografi yang digunakan dalam tesis ini adalah teknik *Least Significant Bit (LSB)*. Dengan teknik ini, data rahasia dapat disembunyikan di bit paling kurang signifikan dari gambar *cover* sehingga mata manusia tidak akan mampu melihat pesan tersembunyi dalam gambar *cover*. Gambar hasil teknik steganografi inilah yang akan digunakan sebagai *password* sistem otentikasi yang baru pada aplikasi *Android* sehingga gambar tersebut akan bertindak sebagai media pembawa dari *password* tekstual asli yang ada.

Kata Kunci : Otentikasi; *Least Significant Bit (LSB)*; Kriptografi; *Data Encryption Standard (DES)*; Steganografi; *Android*.

ABSTRACT

Providing a security to confidential information on the mobile platforms has been becoming a topical issue for the application developers. Above mentioned can be achieve with a good authentication system. One of the authentication techniques is a textual password based. On this type techniques commonly follows an encryption algorithm to provide more security. Also this techniques has some weakness because users tend to choose meaningful words from dictionaries or several things that can be related with user identity, which make textual passwords easy to break and vulnerable to dictionary or brute force attacks. To overcome those matter, a new authentication technique is proposed in this paper in order to improvement for authentication system using cryptography and steganography techniques. The steganography technique in this thesis used Least Significant Bit (LSB) embedding technique. With this technique, data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. All data and critical information like the textual password are encrypted with Data Encryption Standard (DES) then will be hidden in an image using steganography technique to hide secret information onside some carrier. This stegano-image becomes as a carrier of original textual password on authentication system that run under Android.

Keywords: Authentication; Least Significant Bit (LSB); Cryptography; Data Encryption Standard (DES); Steganography; Android.

KATA PENGANTAR

Puji dan Syukur yang sedalam-dalamnya kepada Allah SWT, karena hanya dengan rahmat dan karunia-Nya-lah naskah tesis yang berjudul “Pengembangan Sistem Otentikasi Di Aplikasi Berbasis *Android* Dengan Penerapan Gambar Digital Sebagai *Password*” dapat diselesaikan.

Dalam penyusunan proposal tesis ini, penulis menyampaikan terima kasih yang tulus kepada:

1. Tuhan Yang Maha Esa, dengan semua Kehendak Rahmat-Nya Laporan Penelitian ini dapat terselesaikan.
2. Yang tercinta Orangtuaku dan seluruh keluarga yang selalu memberikan dukungan dan do’a yang tidak pernah berhenti agar bisa terselesainya laporan penelitian ini.
3. Bapak Prof. Ir. Suryo Hapsoro Tri Utomo, Ph.D., selaku Rektor Universitas Budi Luhur.
4. Bapak Prof. Dr. Sugiharto, M.Sc, M.Fin., selaku Direktur Program Pascasarjana Universitas Budi Luhur.
5. Bapak Dr. M. Syafrullah, M.Kom., M.Sc., selaku Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
6. Bapak Dr. Ir. Nazori AZ, M.T., selaku pembimbing tesis yang banyak memberikan bimbingan dan arahan.
7. Seluruh Dosen Program Studi Magister Ilmu Komputer Universitas Budi Luhur yang banyak memberikan ilmu selama perkuliahan.
8. Istriku tercinta Yudi Eka Mahareni yang selalu memberikan do’a dan dukungan dengan penuh kesabaran dan pengertian setiap waktu terutama dalam proses pembuatan laporan ini.
9. Anakku tersayang Malka Athara Permadi yang selalu membuatku termotivasi dan semangat dalam setiap waktu.

10. Rekan-rekan mahasiswa MKOM Universitas Budi Luhur terimakasih atas kebersamaannya, kerjakeras dan dukungan semangatnya
11. Serta semua pihak yang tidak dapat dituliskan.

Penulis menyadari bahwa penulisan tesis ini jauh dari sempurna. Untuk itu penulis berharap mendapatkan kritik dan saran yang dapat berguna untuk membangun demi kesempurnaan tulisan tesis ini.

Jakarta, Januari 2017

Penulis



DAFTAR ISI

ABSTRAK	i
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	x
BAB I : PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Masalah Penelitian	3
1.2.1. Identifikasi Masalah	3
1.2.2. Batasan Masalah	3
1.2.3. Rumusan Masalah	4
1.3. Tujuan dan Manfaat Penelitian	4
1.4. Tata Urut Penulisan	5
1.5. Daftar Pengertian	6
BAB II : LANDASAN PEMIKIRAN	9
2.1. Tinjauan Pustaka	9
2.1.1. Otentikasi	9
2.1.2. Kriptografi	10
2.1.3. <i>Data Encryption Standard (DES)</i>	14
2.1.4. Steganografi	22
2.1.5. <i>Least Significant Bit (LSB)</i>	24
2.1.6. <i>Android</i>	25
2.1.7. Citra Digital	33
2.1.8. Metode Pengembangan Sistem	35
2.1.9. <i>Unified Modelling Language</i>	40
2.2. Tinjauan Studi	42
2.3. Tinjauan Objek Penelitian	44
2.4. Kerangka Konsep	45
2.5. Hipotesis	46

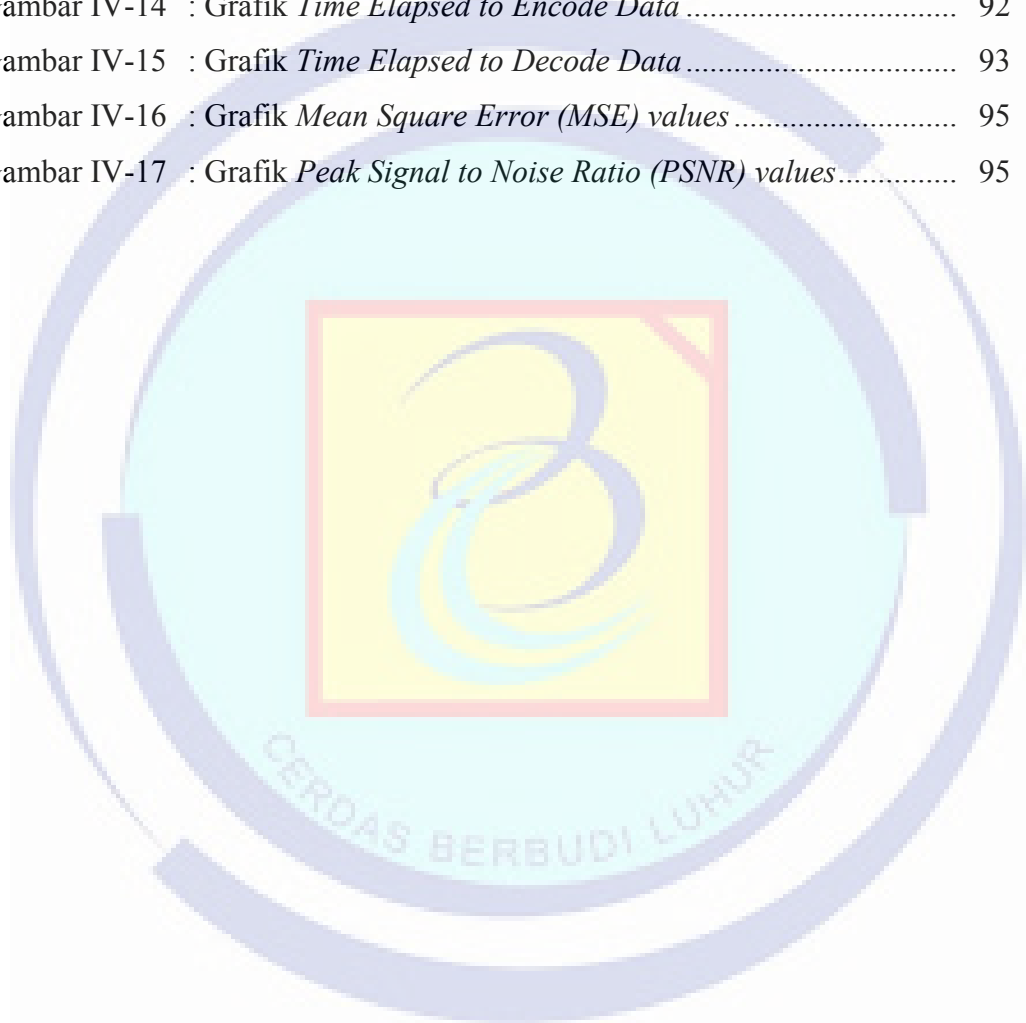
BAB III : LANDASAN PEMIKIRAN	47
3.1. Metode Penelitian	47
3.2. Metode Pemilihan Sampel	47
3.3. Metode Pengumpulan Data	48
3.4. Instrumentasi	49
3.5. Teknik Analisis dan Pengujian Data	49
3.5.1. <i>Mean Square Error (MSE)</i>	49
3.5.2. <i>Peak Signal to Noise Ratio (PSNR)</i>	49
3.5.3. <i>Time Elapsed to Encode and Decode Data</i>	50
3.6. Rancangan Sistem	50
3.6.1. Enkripsi Pesan Menggunakan Algoritma <i>DES</i>	50
3.6.2. Dekripsi Pesan Menggunakan Algoritma <i>DES</i>	59
3.6.3. Penyisipan Pesan Rahasia Menggunakan Algoritma <i>LSB</i>	63
3.7. Langkah-Langkah Penelitian	67
3.8. Jadwal Penelitian	70
BAB IV : PEMBAHASAN HASIL PENELITIAN	72
4.1. Analisis Sistem	72
4.1.1. Analisis Proses Bisnis Sistem Berjalan	72
4.1.2. Analisis Kebutuhan Fungsional, Nonfungsional, dan Pengguna	72
4.1.3. Analisis Perilaku Sistem	75
4.2. Perancangan Sistem	81
4.2.1. Perancangan Spesifikasi Program	81
4.2.2. Perancangan <i>Database</i>	83
4.2.3. Perancangan Infrastruktur <i>Architecture</i>	83
4.3. Konstruksi Model	84
4.3.1. Lingkungan Konstruksi	84
4.3.2. Konstruksi <i>Database</i>	85
4.3.3. Konstruksi <i>User Interface</i>	85
4.4. Pengujian Sistem	88

4.4.1. Lingkungan Pengujian.....	88
4.4.2. <i>Blackbox Testing</i>	89
4.4.3. Hasil Pengukuran <i>Time Elapsed to Encode</i> dan <i>Decode Data</i>	92
4.4.4. Hasil Pengukuran <i>Mean Square Error (MSE)</i> dan <i>Peak Signal to Noise Ratio (PSNR)</i>	94
4.5. Implikasi Penelitian	96
4.5.1. Aspek Sistem	96
4.5.2. Aspek Manajerial	97
4.5.3. Aspek Penelitian Lanjutan	98
4.6. Rencana Implementasi Sistem	98
BAB V : PENUTUP	100
DAFTAR PUSTAKA	101
LAMPIRAN-LAMPIRAN	103

DAFTAR GAMBAR

Gambar II-1	: Alur Proses Kriptografi	11
Gambar II-2	: Alur Kriptografi Simetris	12
Gambar II-3	: Alur Kriptografi Asimetris	13
Gambar II-4	: Skema global <i>Data Encryption Standard</i>	15
Gambar II-5	: Algoritma enkripsi dengan <i>DES</i>	16
Gambar II-6	: Proses pembangkitan kunci-kunci <i>internal DES</i>	18
Gambar II-7	: Rincian komputasi fungsi <i>f</i>	19
Gambar II-8	: Skema perolehan R_i	20
Gambar II-9	: Proses penyembunyian pesan rahasia ke dalam media digital dengan teknik steganografi	24
Gambar II-10	: (a) Skema <i>embedding</i> ; (b) Skema <i>extraction</i>	24
Gambar II-11	: Gambar Contoh Steganografi	25
Gambar II-12	: Arsitektur <i>Android</i>	28
Gambar II-13	: (a) Citra <i>biner</i> ; (b) Representasi citra <i>biner</i>	34
Gambar II-14	: (a) Citra <i>grayscale</i> ; (b) Citra warna	35
Gambar II-15	: <i>System Development Live Cycle</i>	35
Gambar II-16	: Model <i>Waterfall</i>	36
Gambar II-17	: Kerangka Konsep Penelitian	45
Gambar III-1	: Langkah-Langkah Penelitian	68
Gambar IV-1	: <i>Usecase Diagram</i>	75
Gambar IV-2	: <i>Register Activity Diagram</i>	76
Gambar IV-3	: <i>Login Activity Diagram</i>	77
Gambar IV-4	: <i>Register Sequence Diagram</i>	79
Gambar IV-5	: <i>Login Sequence Diagram</i>	80
Gambar IV-6	: <i>Class Diagram</i>	81
Gambar IV-7	: <i>Deployment Diagram</i>	82
Gambar IV-8	: Infrastruktur Sistem	83

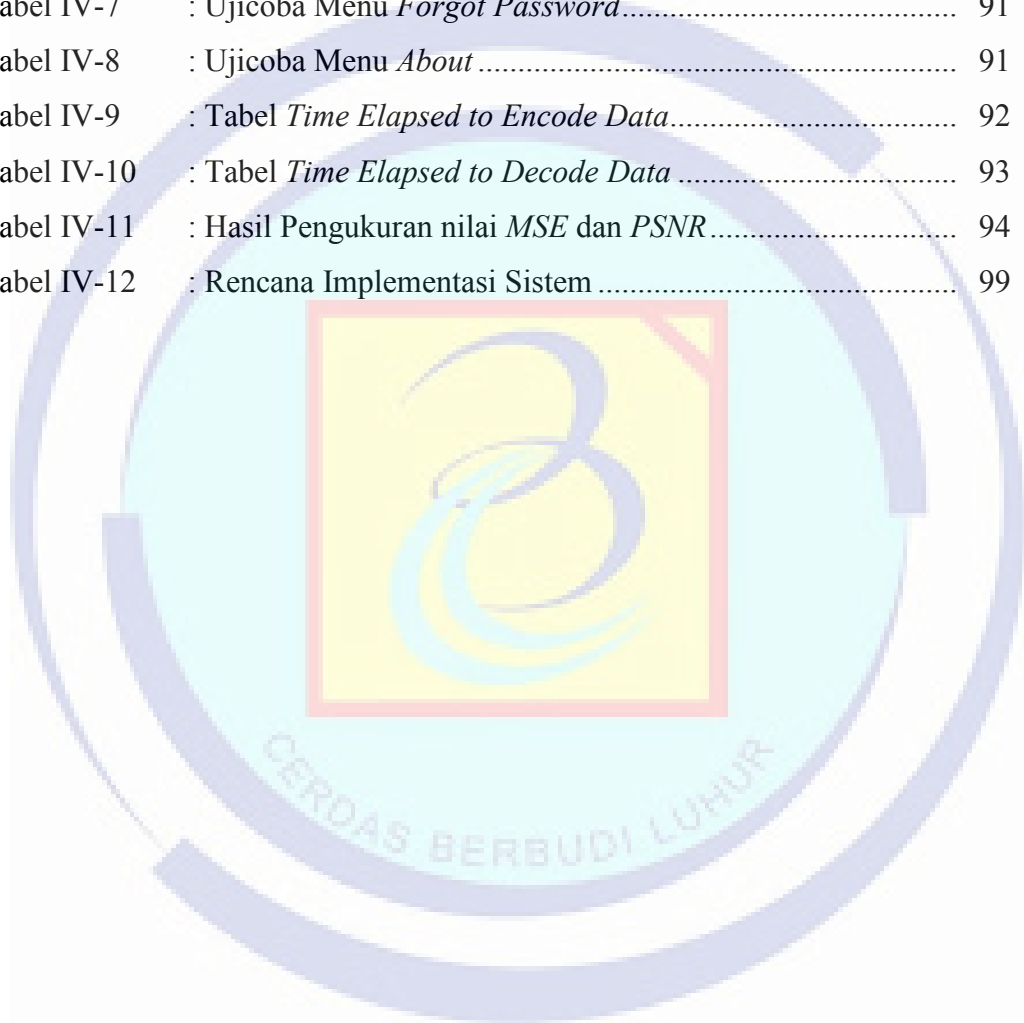
Gambar IV-9	: Tampilan <i>MainActivity</i> Aplikasi	86
Gambar IV-10	: Tampilan <i>Menu Register</i>	86
Gambar IV-11	: Tampilan <i>Register Success</i>	87
Gambar IV-12	: Tampilan <i>Menu Login</i>	87
Gambar IV-13	: Tampilan <i>Login Success</i>	88
Gambar IV-14	: Grafik <i>Time Elapsed to Encode Data</i>	92
Gambar IV-15	: Grafik <i>Time Elapsed to Decode Data</i>	93
Gambar IV-16	: Grafik <i>Mean Square Error (MSE) values</i>	95
Gambar IV-17	: Grafik <i>Peak Signal to Noise Ratio (PSNR) values</i>	95



DAFTAR TABEL

Tabel I-1	: Daftar Pengertian Istilah	6
Tabel II-1	: <i>Cipher</i> Julius Caesar	11
Tabel II-2	: Permutasi Awal (<i>Initial Permutation</i>).....	16
Tabel II-3	: Matriks Permutasi Kompresi <i>PC-1</i>	17
Tabel II-4	: Matriks Permutasi Kompresi <i>PC-2</i>	18
Tabel II-5	: Fungsi Ekspansi	19
Tabel II-6	: Matriks Permutasi <i>P</i>	20
Tabel II-7	: Matriks Permutasi Akhir	21
Tabel II-8	: Daftar Macam Versi <i>Android</i>	27
Tabel II-9	: Penelitian Terkait	42
Tabel III-1	: Variasi Banyaknya Teks Karakter dari Password Asli	48
Tabel III-2	: Pembuatan C_n dan D_n	52
Tabel III-3	: <i>S box 1</i>	55
Tabel III-4	: <i>S box 2</i>	56
Tabel III-5	: <i>S box 3</i>	56
Tabel III-6	: <i>S box 4</i>	56
Tabel III-7	: <i>S box 5</i>	56
Tabel III-8	: <i>S box 6</i>	57
Tabel III-9	: <i>S box 7</i>	57
Tabel III-10	: <i>S box 8</i>	57
Tabel III-11	: 16 kunci dekripsi	59
Tabel III-12	: Nilai Piksel Citra Penampung RGB 5x5 Piksel	64
Tabel III-13	: Nilai Biner Citra Penampung RGB 5x5 Piksel	64
Tabel III-14	: Nilai Biner Pesan yang akan Disisipkan	65
Tabel III-15	: Nilai Biner Citra Penampung Setelah Disisipi Pesan	66
Tabel III-16	: Jadwal Penelitian.....	70
Tabel IV-1	: Tabel <i>User</i>	83

Tabel IV-2	: Ujicoba <i>MainActivity</i>	89
Tabel IV-3	: Ujicoba <i>MainActivity</i>	89
Tabel IV-4	: Ujicoba Menu <i>Login</i>	90
Tabel IV-5	: Ujicoba Menu <i>Change Password</i>	90
Tabel IV-6	: Ujicoba Menu <i>Delete Account</i>	91
Tabel IV-7	: Ujicoba Menu <i>Forgot Password</i>	91
Tabel IV-8	: Ujicoba Menu <i>About</i>	91
Tabel IV-9	: Tabel <i>Time Elapsed to Encode Data</i>	92
Tabel IV-10	: Tabel <i>Time Elapsed to Decode Data</i>	93
Tabel IV-11	: Hasil Pengukuran nilai <i>MSE</i> dan <i>PSNR</i>	94
Tabel IV-12	: Rencana Implementasi Sistem	99



DAFTAR LAMPIRAN

Lampiran 1	: <i>Change Password Activity Diagram</i>	103
Lampiran 2	: <i>Delete Account Activity Diagram</i>	104
Lampiran 3	: <i>Recovery Password Activity Diagram</i>	105
Lampiran 4	: <i>Change Password Sequence Diagram</i>	106
Lampiran 5	: <i>Delete Account Sequence Diagram</i>	107
Lampiran 6	: <i>Recovery Password Sequence Diagram</i>	108
Lampiran 7	: Tampilan Menu Utama/ <i>Welcome</i>	109
Lampiran 8	: Tampilan Menu <i>Change Password</i>	109
Lampiran 9	: Tampilan <i>Change Password Success</i>	110
Lampiran 10	: Tampilan Menu <i>Delete Account</i>	110
Lampiran 11	: Tampilan Menu <i>Forgot Password</i>	111
Lampiran 12	: Tampilan Menu <i>About</i>	111
Lampiran 13	: <i>Source Code Aplikasi</i>	112

DAFTAR PUSTAKA

Agarwal, Ankita. 2012, *Security Enhancement Scheme for Image Steganography using S-DES Technique*, *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 2, Issue 4, 164-169.

Alatas, Putri. 2014, *Implementasi Teknik Steganografi Dengan Metode LSB Pada Citra Digital*, Tugas Akhir Jurusan Sistem Informasi, Fakultas Ilmu Komputer & Teknologi Informasi, Universitas Gunadarma.

Ariyus, D. 2006. *Kriptografi, Keamanan Data dan Komunikasi*, Graha Ilmu, Yogyakarta.

Burnette. 2009, *Hello Android 2nd Edition*, Pragmatic Bookshelf, USA.

Bucerzan, Dominic, Crina Rațiu dan Misu-Jan Manolescu. 2013, *SmartSteg: A New Android Based Steganography Application*, *International Journal Computer Communication* 8(5), 681-688.

Dennis, Alan. 2009, *Systems Analysis and Design with UML – 3rd Edition*. John Wiley & Sons, Inc.

Dooley, J. 2013, *A Brief History of Cryptology and Cryptographic Algorithms*, Springer, New York.

Fairuzabadi, M. 2010, *Implementasi Kriptografi Klasik Menggunakan Borland Delphi*. Jurnal Dinamika Informatika. 4 (2).

Ghare, Rajashri, Pruthvi Bansode, Sagar Bombale dan Bilkis Chandargi. 2015, *LSB Steganography Using Android Phone*, *International Journal of Computer Science and Information Technologies*, Vol. 6 (2), 1027-1029.

Gargenta, M. 2011, *Learning Android*, O'Reilly Media, California.

Goodrich, Michael T. dan Roberto, T. 2011, *Introduction to Computer Security*, Pearson Education Limited, Boston.

Hadapad, Dattereya dan Raj, Steven 2013, *Android Application For Secure File Transferring using Data Encryption Standard*, *International Journal of Engineering Research & Technology (IJERT)*, Vol. 2 Issue 7, 1890-1895.

Hastuti, K., dan Hidayat, E.Y. 2013, *Analisis Steganografi Metode Least Significant Bit (LSB) dengan Penyisipan Sekuensial dan Acak Secara Kuantitatif dan Visual*, *Techno.COM* 12(3): 157-167.