SISTEM STEGANOGRAPHY DENGAN METODE LEAST SIGNIFCANT BIT (LSB) & METODE CAESAR CIPHER BERBASIS ANDROID

Abrar Hiswara[1], Aida Fitriyani[2], Reza Adi Nugraha[3]

[123]Fakultas Teknik, Teknik Informatika Universitas Bhayangkara Jakarta Raya
Jl. Raya Perjuangan, Bekasi Utara - Indonesia
Telp. (021) 88955882 Fax. (021) 88955871
e-mail : abrar@dsn.ubharajaya.ac.id

ABSTRACT

*This research aims at information security in the form of document files, documents are casual but have a vital role, due to many cyber crimes that try or commit data theft, illegal access or misuse of documents that are used as a particular crime tool. the software development method uses the Rapid Application Development (RAD) model, while the research method applies the Least Significant Bit (LSB) method of hiding information into a digital media (image) as a steganographic technique and Caesar Cipher as a cryptographic technique that encrypts * document filename into a form Caesar randomly characters. The results of the study resulted in an android-based steganography system that uses the Java programming language, as data security for document systems using the least significant bit and caesar cipher method as a top priority and making the system more friendly and interactive to be used easily by users. Steganography system is considered to provide an alternative for users as a system that is able to maintain the confidentiality of documents and provide information to users of the importance of a data security measure.*

Keywords *: Android, Java, Steganography, Cryptography, Rapid Application Development, Least Significant Bit, Caesar Cipher.*

ABSTRAK

Penelitian ini bertujuan untuk keamanan informasi berupa file dokumen, dokumen merupakan hal kasual tetapi memiliki peran vital, dikarenakan banyak kejahatan cyber yang mencoba atau melakukan tindak pencurian data, ilegal akses ataupun penyalahgunaan dokumen yang dijadikan alat kejahatan tertentu. metode pengembangan perangkat lunak digunakan model Rapid Application Development (RAD), sedangkan metode penelitian menerapkan metode Least Significant Bit (LSB) teknik menyembunyikan informasi kedalam sebuah media digital (image) sebagai teknik steganografi dan Caesar Cipher sebagai teknik kriptografi yang mengenkripsi *filename dokumen kedalam bentuk Caesar secara random karakter. Hasil penelitian menghasilkan sebuah sistem steganography berbasis android yang menggunakan bahasa pemrograman Java, sebagai keamanan data terhadap dokumen sistem menerapkan metode least significant bit dan caesar cipher sebagai prioritas utama dan menjadikan sistem yang lebih ramah dan interaktif untuk dapat digunakan dengan mudah oleh pengguna. Sistem steganography dirasa memberikan alternatif untuk pengguna sebagai sistem yang mampu menjaga kerahasiaan dokume serta memberi informasi kepada pengguna pentingnya sebuah langkah keamanan data.

Kata Kunci : Android, Java, Steganografi, Kriptografi, Rapid Application Development, Least Significant Bit, Caesar Cipher.

I. PENDAHULUAN

Perkembangan teknologi Internet memunculkan kejahatan yang disebut dengan cybercrime atau kejahatan melalui jaringan Internet. Munculnya beberapa kasus cybercrime di Indonesia, merupakan fenomena, seperti pencurian kartu kredit, hacking terhadap berbagai situs, penyadapan transmisi data orang lain, (misalnya email), dan manipulasi data dengan cara menyiapkan perintah yang tidak dikehendaki ke dalam programer komputer.

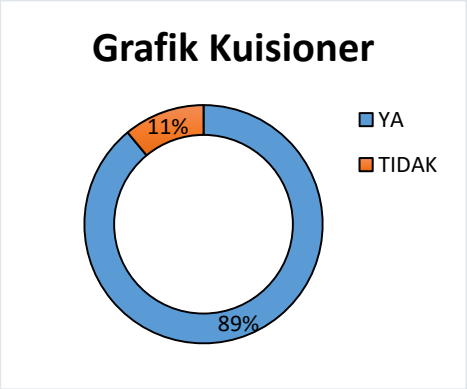
Bersangkutan dengan hal tersebut Cybercrime kerap disamakan dengan computer crime. menurut The U.S. Department of Justice adalah sebagai "…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution". Hal senada disampaikan oleh Organization of European Community Development, yang mendefinisikan computer crime sebagai: "Any illegal, unehtical or unauthorized behavior relating to the automatic processing and/or the transmission of data".

Salah satu tindak ilegal dalam keamanan data adalah Data forgery, teknik ini dilakukan dengan tujuan memalsukan data pada dokumen-dokumen penting yang ada di internet. Dokumen-dokumen ini biasanya dimiliki oleh institusi atau lembaga yang memiliki situs berbasis web database. Menurut hasil statistik dari Breach Level Index (BLI) membuktikan, sepanjang 2018 telah terjadi 3.353.172.708 kehilangan atau pencurian data di seluruh dunia, atau sama dengan 18.525.816 data per hari, dan 771,909 per jam. Dari keseluruhan pelanggaran data di 2018 hanya 3% pembobolan data dianggap tidak berhasil karena data yang dicuri sudah terlebih dulu dienkripsi oleh perusahaan.

Berdasarkan keterangan data BLI di atas, enkripsi menjadi salah satu solusi terbaik bagi perusahaan untuk memecahkan masalah pelanggaran keamanan data. Secara global kasus pencurian / pembobolan data terjadi karena sebagian besar data yang disimpan tidak disertai enkripsi, tindak kriminal sangat mudah untuk mengakses data tersebut, bahkan hingga di perjual-belikan melalui darkweb dengan tujuan tindak kriminal, Cangkupan yang dijangkau dalam penelitian ini bersifat umum atau open public , karena penelitian ini akan menghasilkan sebuah sistem yang memang dikhususnya dan diperuntukkan

untuk kebutuhan user dengan mengenkripsi sebuah data. Bersamaan dengan hal tersebut, penulis berinisiatif membuat kuisioner sebagai bahan perbandingan, pertimbangan apakah sistem yang dibuat penulis dapat menjadi sarana pencengahan terjadinya tindak ilegal akses terhadap file.

Pernyataan penulis ini terbukti dari hasil kuesioner yang dilakukan penulis dengan mendapatkan perolehan suara dari 50 responden yang merupakan mahasiswa dan pengguna regional yang menghasilkan 89% responden yang setuju bahwa keamanan data merupakan faktor penting dan dibutuhkannya sistem yang dibuat oleh penulis.



Gambar 1. Grafik Hasil Kuisioner

Berdasarkan data diatas, ada beberapa teknik keamanan untuk melindungi pesan yang disimpan maupun dikirim, tetapi yang digunakan dalam penelitian adalah teknik cryptography dan teknik steganography, teknik cryptography digunakan untuk melakukan encoding atau enkripsi terhadap pesan rahasia, pesan dilindungi sedemikian rupa sehingga tidak dapat terbaca oleh pihak yang tidak berwenang dan hanya dapat dibaca oleh pihak yang memiliki otoritas sedangkan teknik steganography yang memiliki fungsi untuk menyembunyikan atau menyamarkan pesan rahasia kedalam objek citra.

Penelitian dilaksanakan untuk merancang aplikasi steganografi dengan mengkombinasikan Metode *Least Significant Bit* (LSB) & Metode *Caesar Cipher* sebagai teknik *steganography* dan *cryptography* yang hadir untuk mewujudkan keamanan data. Diharapkan pada hasil penelitian ini, proses pengamanan data akan lebih cepat dan lebih aman**,** penulis perancangan, pengembangan sistem yang lebih baik dengan metode penelitian yang berbeda, penelitian ini bertujuan untuk mencegah atau menyelesaikan permasalahan yang ada pada penelitian sebelumnya, sistem yang dibangun diharapkan dapat menjadi solusi yang lebih baik, tanpa mengurangi atau merendahkan penelitian sebelumnya, penelitian ini juga memfokuskan pemecahan masalah yang hampir serupa tapi dengan gaya penyelesaian yang berbeda dengan menggabungkan 2 metode yang bertugas untuk menyembunyikan dokumen kedalam media objek citra

digital (image 24-bit) tanpa efek kerusakan pada *file*, dan mengenkripsi *file* kedalam bentuk *Caesar cipher*, dan diberikan *single-key algorithm* agar *file* tidak mudah diakses oleh sembarang *user* serta terdapat contoh kasus dan teori keamanan data. Dalam pembuatan sistem ini Penulis menggunakan program *Android Studio* untuk *design* dan pengkodean proses dan metode pengembangan *software* Penulis menggunakan metode *Rapid Application Development* (RAD) karena dengan menggunakan metode ini jalannya penelitian lebih fleksibelAda beberapa penelitian sebelumnya yang membahas tentang hal ini, dibawah ini merupakan beberapa penelitian terdahulu yang digunakan sebagai bahan perbandingan untuk penelitian yang akan peneliti lakukan, sebagai berikut.

Ajar Rohmanu (2017) dalam penelitian **"Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma *Des* dan Metode *End Of File*"** menyatakan metode EOF menawarkan teknik yang menggunakan cara dengan menyisipkan data pada akhir *file*. Teknik ini dapat digunakan untuk menyisipkan data yang ukurannya sesuai dengan kebutuhan. Ukuran *file* yang telah disisipkan data sama dengan ukuran *file* sebelum disisipkan data ditambah dengan ukuran data yang disisipkan ke dalam *file* tersebut. Kemudian untuk menambah tingkat keamanan data yang disisipkan, digunakan algoritma DES. algoritma DES termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok. DES beroperasi pada ukuran blok 64 *bit*. DES mengenkripsikan 64 bit *plainteks* menjadi 64 *bit cipherteks* dengan menggunakan 56 *bit* kunci internal (*internal key*) atau sub kunci (*subkey*).

Satriya Tri Cahya Kurniawan (2017) dalam penelitian "**Implementasi Kriptografi Algoritma *Rivest Shamir Adleman* dengan *Playfair Cipher* pada Pesan Teks"** menyatakan algoritma *rivest shamir adleman* (RSA) yang dipadukan dengan *playfair cipher* menawarkan dua kunci keamanan, yaitu kunci publik dan kunci pribadi. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Kemudian agar lebih terjaga keamanannya kriptografi ini dikombinasikan dengan *playfair cipher* yaitu menggunakan tabel 5x5.

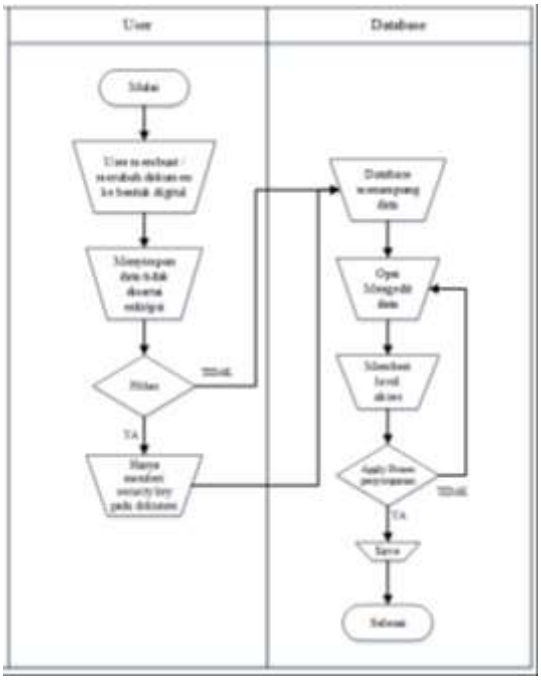
Putra (2014) dalam penelitian **"Aplikasi Steganografi untuk Keamanan Basis Data dengan Metode *Pixel Value Differencing* dan Algoritma *Rijndael*"** menyatakan metode PVD

menawarkan kapasitas penyimpanan yang lebih besar dengan kualitas citra yang lebih baik dari metode lain. Kemudian untuk menambahkan tingkat keamanan data yang disisipkan, digunakan algoritma enkripsi berupa algoritma *Rijndael* 128 *bit*. Algoritma *Rijndael* merupakan algoritma yang digunakan untuk standar kriptografi *Advanced Encryption Standard* (AES).

II. METODE PENELITIAN

a. Analisis

Dibawah berupa Analisis sistem berjalan.



Gambar 2. Analisis sistem berjalan

Berdasarkan gambar diatas, sistem berjalan menjelaskan setiap bagian yang ada pada sistem usulan.. Dalam sistem yang berjalan user hanya membuat interaksi dengan database, dimana user membuat ataupun mengubah dokumen kedalam bentuk digital agar dapat disimpan ke database, pengguna tidak menggunakan langkah enkripsi untuk menjaga keamanan dokumen. Tindakan yang dilakukan hanya memberikan security key terhadap dokumen sebelum di simpan ke database.

Database sebagai media penyimpan hanya mampu menampung dokumen dan memberikan level akses untuk membatasi user yang ingin mengakses dokumen. e. Data tersimpan dalam database tanpa perlindungan teknik enkripsi yang membuat dokumen tersebut rentan akan ancaman pencurian data, ataupun tindak illegal akses lainnya.

b. Metode Pengembangan Sistem

Menurut Whitten & Bentley (2007), Rapid Application Development (RAD) adalah sebuah strategi pengembangan sistem yang menekankan kecepatan dalam pengembangan melalui keterlibatan pengguna dalam pembangunan secara cepat, interaktif, dan incremental dari suatu serangkaian prototype dari suatu sistem yang dapat berkembang menjadi suatu sistem akhir atau versi tertentu.

c. Least Significant Bit (LSB)

Menurut Kuanchin Chen (2009:402-409) Least Significant Bit merupakan teknik penyembunyian data yang bekerja pada domain spatial atau waktu. arti dari

LSB merupakan salah satu metode steganografi yang paling sederhana, cepat dan mempunyai kapasitas penyisipan yang cukup besar. LSB menggunakan cara menyisipkannya pada bit rendah atau bit paling kanan (LSB) pada data pixel yang menyusun file tersebut

d. Caesar Cipher

Menurut Joshua Holden (2017) Caesar Cipher merupakan salah satu algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi. Caesar cipher merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada cipherteks.

Perbedaan penelitian yang dilakukan ini dengan penelitian sebelumnya adalah Caesar cipher dimodifikasi pada randomisasi urutan yang digunakan untuk proses pergeseran karakter. Nilai yang digunakan sebagai pergeseran adalah nilai semi acak (pseudorandom), nilai awal (seed) yang digunakan adalah hasil modulasi XOR dari masukan password / kunci. Caesar cipher yang dimodifikasi ini digunakan untuk menyandikan citra digital (image). Pada penelitian ini digunakan algoritma semi acak (pseudorandom) untuk membangkitkan nilai pergeseran.

e. Implementasi

Berikut merupakan tampilan laman *login* dan *register*, peneliti menyediakan fungsi *login* dimaksudkan agar sistem hanya bisa diakses oleh *user* yang telah melakukan *register* terlebih dulu.

- *Login Page*

Gambar 3**.** Login Page

Keterangan Gambar : Ini adalah tampilan dari laman *login*, *user* diharusnya untuk *login* terlebih dulu agar dapat mengakses setiap fungsi yang terdapat dalam sistem.

- *Register Page*

Gambar 4**.** Register Page

Keterangan Gambar : ini adalah laman *register*, *user* harus terlebih dulu membuat *account* agar dapat mengakses semua fungsi sistem, dan *login* sebelum masuk ke menu utama.

- *Main Menu*

Berikut merupakan tampilan dari "Main Menu" pada sistem, sistem menampilkan *interface* yang cukup ramah agar user dapat dengan mudah memahami maksud dari setiap opsi yang ditampilakan.

Gambar 5. Main Menu

Keterangan Gambar : Diatas merupakan laman "Main Menu", terlihat ada 3 opsi untuk *user* memilih, setiap opsi mempunyai fungsi yang berbeda, perlu diketahui fungsi *encrypt* dan *decrypt* memiliki keterkaitan fungsi.

- *Menu Story*

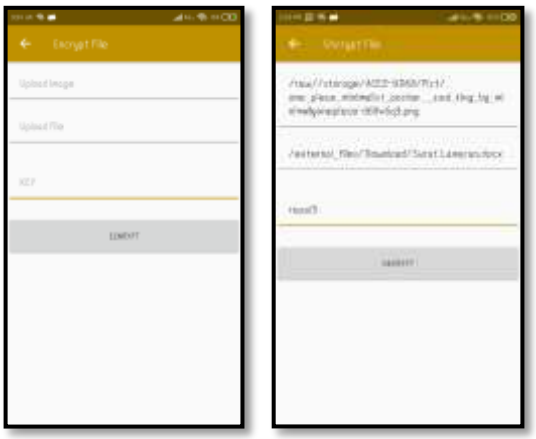
Berikut merupakan tampilan laman dari "Menu *Story*" pada sistem, dimaksudkan sebagai penyedia informasi tentang keamanan data.

Gambar 6. Menu Story

Keterangan Gambar :Tampilan ini menunjukan dimana *user* mengakses menu *story*, menu *story* ini merupakan menu yang menyediakan informasi yang menyangkut keamanan data, metode enkripsi data, informasi yang terdapat dalam menu ini disediakan penulis dikarenakan kebutuhan informasi agar membantu *user* untuk memahami aspek keamanan data.

- *Menu Encrypt*

Dibawah ini merupakan tampilan dari menu "*Encrypt*" pada sistem, sebagai contoh penulis melakukan proses enkripsi

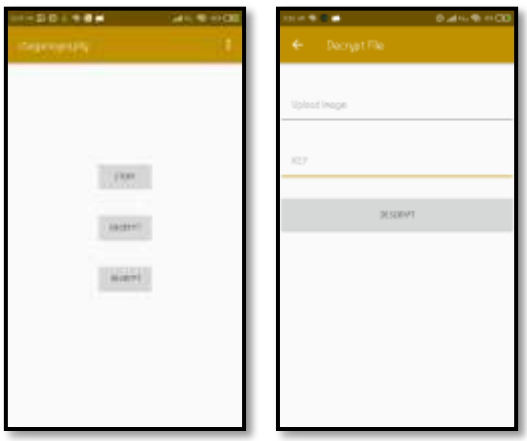


Gambar 7. Menu Encrypt

Keterangan Gambar : Tampilan dimana *user* mengakses menu enkripsi, menu ini berfungsi untuk mengubah bentuk *file* dokumen kedalam bentuk *Caesar cipher* dan akan disisipkan dengan steganografi LSB, disertakan dengan *key* sebagai kunci pengamanan *file*.

- *Menu Decypt*

Dibawah merupakan tampilan dari laman "*Decrypt*" pada sistem, *user* akan menggunakan fungsi ini, setelah terjadi proses enkripsi.

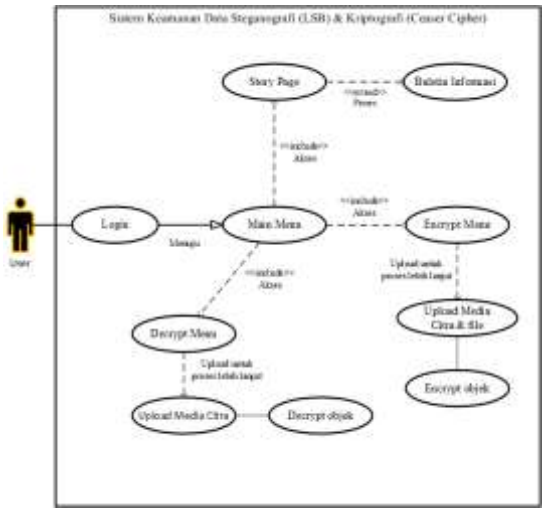


Gambar 8. Menu Decrypt

Keterangan Gambar : Tampilan dimana user mengakses menu *decrypt*, menu ini berfungsi untuk *user* mengembalikan sebuah *file* yang telah ter-enkripsi, *file* yang telah terenkripsi sebelumnya akan diuraikan oleh *decrypt*, *input image* yang ter-enkripsi sebelumnya dan masukan *key* dari file tersebut.

III. HASIL DAN PEMBAHASAN

- *Usecase Diagram Sistem*



Gambar 9. Usecase Diagram Sistem

Diatas merupakan rancangan *usecase* dari sistem yang akan dibuat oleh penulis, setiap *point* memiliki perannya masing-masing didalam sistem, menjadi satu kesatuan yang membentuk sistem yang dinamis.

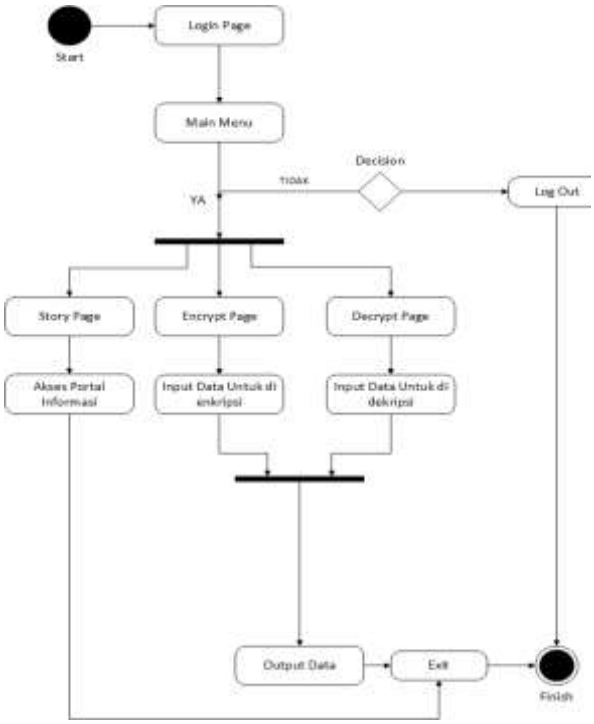
Tabel 1. Deskripsi Aktor

No	Aktor	Deskripsi
1.	*User*	Aktor yang memproses semua fungsi yang terdapat dalam sistem.

Tabel 2**.** Deskripsi *Usecase*

No	Nama *Usecase*	Deskripsi
1.	*Story*	*Usecase* yang menggambarkan kegiatan menampilkan informasi keamanan data.
2.	*Encrypt*	*Usecase* yang menggambarkan kegiatan proses *encrypt* terhadap *file.*
3.	*Decrypt*	*Usecase* yang menggambarkan kegiatan proses *decrypt* terhadapa *file*.

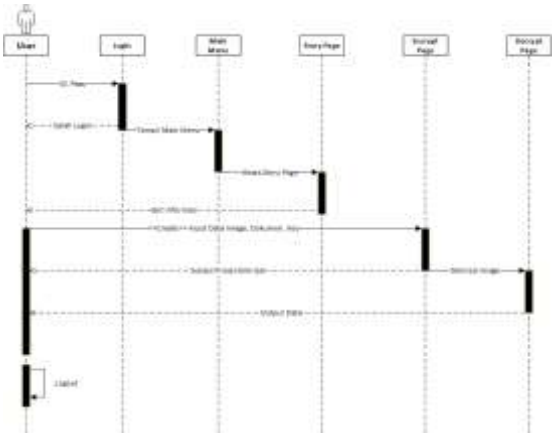
- Activity Sistem



Gambar 10. Activity Sistem

Keterangan Gambar: Diatas merupakan activity diagram yang dirancang penulis sebagai acuan dalam merancang system pada penelitian ini, activity diatas merupakan rancangan activity sistem tanpa *swimlane.*

- Sequence Sistem



Gambar 11**.** Sequence Sistem

Keterangan Gambar: Digunakan dalam penelitian untuk membentuk aplikasi yang telah direncanakan, rancangan diatas menjelaskan hasil yang mengacu terhadap *usecase* diagram dan *activity* diagram.

IV. SIMPULAN

a. Dengan adanya aplikasi "*steganography*" sebagai media keamanan data, user dapat menggunakan aplikasi ini untuk menyembunyikan informasi yang dirasa sangat rahasia untuk di enkripsi dan disisipkan kedalam media citra (*image*).
b. Dengan adaya aplikasi "*steganography*" sebagai media keamanan data, *use*r dapat menjaga keaslian informasi dengan menkonversikan informasi tersebut kebentuk gambar sebagai media penampung.
c. Sistem ini bukan sebagai solusi mengurangi kejahatan pencurian data, tetapi sebagai pencegahan awal untuk mengamankan data dari sebuah informasi.
d. Dengan adanya aplikasi "*steganography*" yang sangat mudah digunakan, *user* dapat mengakses portal sistem informasi yang terdapat dalam aplikasi dimanapun dan kapan

pun yang menampilkan informasi tentang keamanan data.

PENELITIAN LANJUTAN

a. *Interface* / tampilan aplikasi yang dirasa belum terlalu memuaskan sebagai sistem, karena interface memiliki kesan tersendiri dimata *user*, agar *user* lebih nyaman dalam menggunakan aplikasi.
b. Sistem ini akan lebih bermanfaat jika ada versi di sistem operasi lainnya tidak hanya di android saja.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada.

1. Keluarga besar atas do'a, bimbingan, serta cinta yang selalu tercurah.
2. Bapak Abrar Hiswara, S.T., M.M.,M.Kom., & Ibu Aida Fitriyani, S.Kom.,MMSI, selaku pembimbing I & II atas bimbingan, saran dan motivasi yang diberikan kepada Penulis.
3. Pristin's Family yang selalu memberikan motivasi serta dorongan bagi penulis dan selalu mendukung penulis untuk menyelesaikan skripsi ini.
4. Keluarga besar Universitas Bhayangkara Jakarta Raya, khususnya teman-teman seperjuangan Teknik Informatika atas dukungan, semangat, serta kerjasama nya.

DAFTAR PUSTAKA

[1] Chun-Shien Lu. 2005. *Multimedia Security:Steganography And Digital Watermarking Techniques For Protection Of Intellectual Property*. The University Of Michigan, USA : Idea Group Publishing.

[2] Dony Ariyus. 2008. Pengantar Ilmu Kriptografi. Yogyakarta : C.V ANDI OFFSET

[3] Imamah, S.Kom., M.Kom. 2016. Pemrograman Berbasis Mobile Menggunakan Android Studio.

[4] Jerry FitzGerald, Andra F. FitzGerald, Warren D. Stalling. Jr. 1981. *Fundamental of System Analysis*. New York : John Willey & Sons.

[5] Jeffrey L. Whitten, Lonnie D. Bentley. 2007. *Systems Analysis & Design Methods.* The University Of California, USA : *Mcgraw-Hill/Irwin*.

[6] John W. Satzinger, Robert B. Jackson, Stephen D. Burd. 2011. *Systems Analysis And Design In A Changing World 6th Edition.*

[7] Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett,. 2004 *Steganography And Digital Watermarking*. School of Computer

Science : The University of Birmingham.

[8] Joshua Holden. 2017. *The Mathematics Of Secrets : Cryptography From Caesar Ciphers To Digital Encryption Book.*

[9] Kuanchin Chen. 2009. Encyclopedia Of Multimedia Technology And Networking, Second Edition. *Pages 402-409*, USA : Western Michigan University.

[10] Fitria, Y. A. (2019). *Visualization Of Data On Earthquake Prone Areasfrom The Analysis Of Earthquake Data Vibrations*. Test Engineering & Management, 5301-5308.

[11] Marliana B. Winanti,S.Si.,M.Si. 2014. *Sistem Informasi Manajemen*. Bandung

[12] Pulung Nurtantio Andono, T. Sutojo, Muljono. 2018. Pengolahan Citra Digital. Andi Publisher.

[13] Prabowo Pudjo Widodo, Herlawati. 2011. Menggunakan UML, Unified Modeling Language. Bandung : Informatika.

[14] Sadikin, Rifki. 2012. Kriptografi untuk Keamanan Jaringan. Penerbit Andi, Yogyakarta.

[15] S, Rosa A dan M. Shalahuddin. 2014. Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek. Bandung : Informatika.

[16] Yakub. 2012. Sistem Informasi Edisi Pertama. Graha Ilmu : Yogyakarta.

[17] Setiawan, M. (2017, October). Metode K-Means Untuk Sistem Informasi Pengelompokan Mahasiswa Baru Pada Perguruan Tinggi. In *Prosiding Seminar Nasional Darmajaya* (Vol. 1, No. 1, pp. 130-145).