Analisis Penerapan Steganografi Pada Sistem Keamanan *Mobile Banking*

Amelia Natalie/13509004[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13509004@*stei.itb.ac.id*

***Abstract*— Salah satu penggunaan teknologi komunikasi dalam bisnis adalah *mobile banking*. *Mobile banking* merupakan layanan yang diberikan kepada nasabah suatu perusahaan bank untuk dapat melakukan transaksi yang lebih fleksibel, di mana saja dan kapan saja. Selain kenyamanan dan fleksibilitas, nasabah juga menginginkan rasa keamanan yang dapat menjamin kerahasian informasi nasabah. Oleh karena itu, diperlukan sistem keamanan yang dapat menjamin hal tersebut. Sistem keamanan *mobile banking* pada umumnya memanfaatkan kriptografi. Penerapan kriptografi sendiri masih rentan penyadapan untuk mendapatkan *public/private key* dari jaringan. Dengan didapatkan kedua informasi tersebut, penyerang dapat dengan mudah mengetahui informasi rahasia seperti PIN / *password* nasabah. Steganografi merupakan teknik penyembunyian pesan yang dapat digunakana untuk peningkatan sistem keamanan, terutama dalam proses otentikasi maupun proses pertukaran informasi secara umum pada sistem keamanan *mobile banking.* Metode steganografi yang dimanfaatkan yaitu metode *least significant bit* (LSB) dengan gambar sebagai media penyisipan. Pembahasan pada makalah ini antara lain membahas tentang steganografi, sistem *mobile banking*, prinsip keamanan, masalah-masalah keamanan pada sistem *mobile banking*, analisis bagaimana metode steganografi dapat digunakan untuk mengatasinya, dan analisis perbandingan metode steganografi dengan metode lainnya.**

***Index Terms*— *mobile banking*, steganografi, LSB, prinsip keamanan, otentikasi, pertukaran informasi.**

I. Latar Belakang

Manusia berusaha untuk memenuhi berbagai kebutuhan hidupnya dengan menggunakan metode-metode tertentu. Pada zaman dahulu, manusia menggunakan metode barter sebagai cara bertransaksi dengan manusia lainnya. Cara barter kemudian digantikan dengan kepingan batu berharga sebagai alat transaksi. Setelah itu, cara uang menggantikan metode transaksi sebelumnya dan tetap digunakan sampai saat ini. Manusia terus berusaha untuk mencari cara untuk melakukan transaksi dengan mudah dan cepat. Hal inilah yang melatarbelakangi maraknya layanan kartu kredit, kartu debit, atau *cash card* oleh perusahaan-perusahaan perbankan untuk nasabahnya. Dengan layanan-layanan tersebut, seorang nasabah bank tidak perlu repot membawa banyak uang tunai dan tetap dapat melakukan banyak transaksi dengan mudah.

Tidak hanya layanan-layanan yang telah disebutkan sebelumnya, bank telah mengeluarkan layanan baru yang lebih fleksibel untuk nasabahnya yaitu *mobile banking*. *Mobile banking* adalah layanan yang ditawarkan untuk memudahkan nasabah dalam melakukan transaksi, seperti pembayaran, pengajuan kredit, pemeriksan rekening, dan transaksi-transaksi perbankan lainnya. Layanan ini memampukan nasabah untuk melakukan transaksi dimanapun nasabah tersebut berada dengan hanya bermodalkan sebuah media komunikasi *mobile* seperti telepon genggam atau *smartphone*. Menggunakan layanan ini, seorang nasabah dapat menyelesaikan transaksi pentingnya hanya dengan mengirimkan pesan teks singkat atau dengan menggunakan kode yang di-validasi melalui *web browser* pada *smartphone* miliknya. *Mobile banking* berkembang karena memenuhi kebutuhan masyarakat saat ini dan didukung oleh perkembangan teknologi komunikasi.

Seiring dengan maraknya layanan perbankan tersebut, semakin banyak pula modus kriminalitas dengan nasabah *mobile banking* sebagai sasarannya. Oleh karena itu, diperlukan usaha-usaha khusus untuk mengamankan aktivitas transaksi yang dilakukan melalui *mobile banking*. Usaha-usaha ini bertujuan untuk menjamin keamanan informasi nasabah, menjamin validitas data nasabah, dan menghindari kerugian nasabah akibat penyalahgunaan informasi rahasia nasabah oleh pihak-pihak tidak bertanggung jawab.

Saat ini kebanyakan sistem keamanan *mobile banking* menerapkan teknik kriptografi. Penerapan teknik steganografi sendiri masih belum dikembangkan pada *mobile banking*. Meskipun teknik ini merupakan metode yang sederhana, namun dapat bermanfaat untuk meningkatkan sistem keamanan.

Secara garis besar, makalah ini akan membahas mengenai gambaran arsitektur *mobile banking*, sistem keamanan *mobile banking* saat ini, masalah-masalah keamanan dalam sistem *mobile banking*, sifat-sifat steganografi dan bagaimana steganografi dapat berperan untuk meningkatkan sistem keamanan *mobile banking*.

II. Dasar Teori

A. *Steganografi*

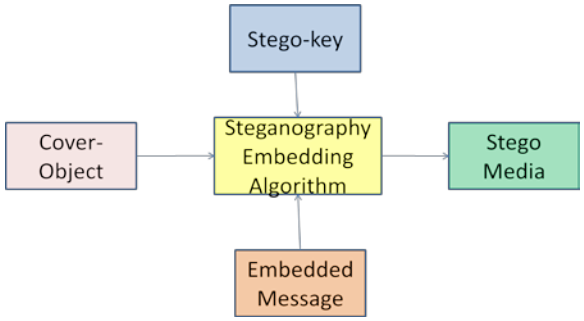
Steganografi (berasal dari kata *steganos* dalam bahasa Yunani yang berarti tertutup dan *graphie* yang berarti

tulisan[1]) adalah seni dan ilmu dalam menuliskan pesan tersembunyi sehingga tidak ada pihak selain dari pengirim dan penerima pesan yang dapat mengetahui keberadaan pesan tersebut. Saat ini, pesan biasanya disembunyikan dengan sebuah media, seperti gambar, suara, atau video. Steganografi telah digunakan semenjak dahulu. Pada saat itu, steganografi dilakukan dengan media kepala budak. Kepala budak dibotaki untuk ditulisi pesan dan dibiarkan tumbuh sebelum budak tersebut dikirim kepada si penerima. Selain itu, penggunaan tinta tak-tampak juga dilakukan sebagai alat steganografi pada zaman dulu[2].

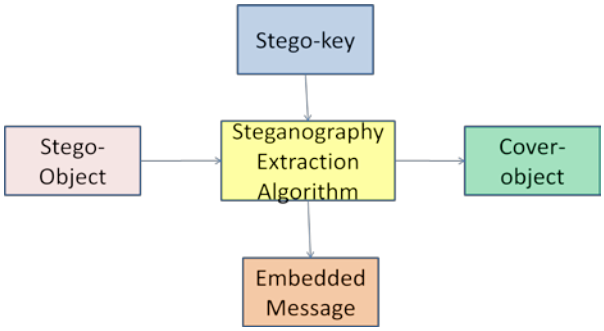
Dalam menyembunyikan data, steganografi memanfaatkan redudansi data dalam media untuk menyisipkan informasi tambahan sehingga tidak ada perubahan yang berarti pada media tersebut. Oleh karena itu, pihak lain seringkali tidak menyadari keberadaan pesan rahasia hasil dari teknik steganografi. Properti dalam teknik steganografi yaitu:

a. *Embedded message* yaitu pesan yang disembunyikan
b. *Cover-object* yaitu pesan yang digunakan untuk menyembunyikan *embedded message*
c. *Stego-object* yaitu pesan yang sudah berisi pesan *embedded message*
d. *Stego-key* yaitu kunci yang digunakan dalam proses penyisipan pesan dan pengekstraksian pesan dari *stego-object*.

Proses penyisipan dan ekstrasi pesan dalam steganografi ditunjukkan pada Gambar 1 dan Gambar 2.



Gambar 1 Penyisipan Informasi dengan Steganografi



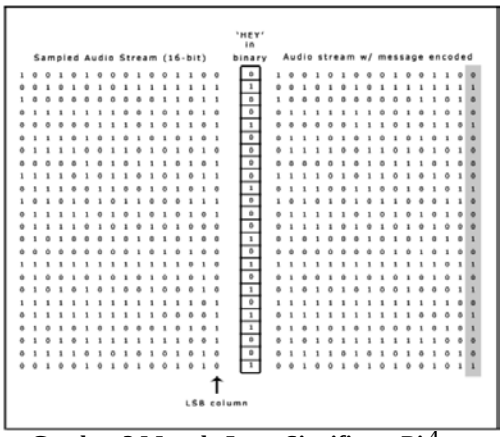
Gambar 2 Proses Ekstraksi dengan Steganografi

Terdapat banyak algoritma yang digunakan untuk steganografi pada gambar digital. Algoritma-algoritma tersebut dapat dikelompokan sebagai berikut[3]:

a. Spasial atau transformasi, bergantung pada redudansi penggunaan domain untuk proses *embedding*.
b. *Model based* atau *ad-hoc*, bergantung pada keadaan apakah algoritma memodelkan sifat statistik sebelum *embedding* dan menyimpan mereka, atau sebaliknya.
c. Pengawasan aktif atau pasif , berdasarkan pada keadaan apakah desain pendeteksi *embedder* memperhitungkan kehadiran penyerang aktif.

Untuk mengetahui lebih lengkap terkait berbagai jenis algoritma yang digunakan dalam steganografi dapat dibaca pada [3].

Metode steganografi pada citra digital yang paling sering digunakan adalah *Least Significant Bit Insertion (LSB)*. LSB dari setiap *byte* dalam sebuah citra digunakan untuk menyimpan data rahasia. Oleh karena penyisipan dilakukan pada LSB, maka perubahan yang dihasilkan terlalu kecil, sehingga sulit dikenali mata manusia. Kekurangan dari teknik ini adalah harus menggunakan format kompresi yang menjaga keutuhan data seperti *bmp* atau *gif* karena teknik ini menggunakan setiap pixel dalam sebuah citra. Apabila format kompresi tidak menjaga keutuhan data, maka beberapa informasi tersembunyi dapat hilang. Nasabahan metode LSB ditunjukkan pada Gambar 3 .



Gambar 3 Metode *Least Significant Bit*[4]

Keuntungan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesan tidak akan menarik perhatian bagi pihak selain pengirim dan penerima pesan. Sebuah pesan kode yang tidak tersembunyi, tidak peduli serumit apapun pesan diacak, akan menimbulkan kecurigaan dan keterbatasan karena di beberapa negara kriptografi dicap illegal. Seringkali, steganografi dan kriptografi digunakan secara bersama-sama untuk memastikan keamanan dari sebuah pesan.

[1] http://searchsecurity.techtarget.com/definition/steganography diakses tanggal 14 Maret 2013

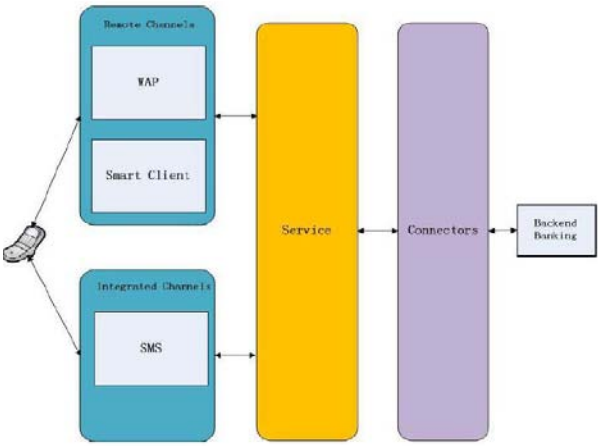
[2] Rinaldi Munir. 2012. *Algoritma Kriptografi Klasik,* (*http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/kripto10-11.htm#SlideKuliah*, diakses tanggal 14 Maret 2013)

[3] Kharrazi, Mehdi; Sencar, Husrev. 2004. Image Steganography: Concepts and Practice. Department of Electrical and Computer Engineering. Polytechnic University, Brooklyn, USA

[4] D. N. Meghanathan, "Jackson State University," 5 June 2011. [Online]. Available:http://www.jsums.edu/cms/tues/docs/Steganography/Basics-Steganography-Security.pdf. [Accessed 12 April 2013].

B. *Infrastruktur Mobile Banking*

Sebuah sistem *mobile banking* terdiri atas sebuah *mobile banking* unit dan sebuah pusat pemrosesan data yang merupakan komputer utama dari bank yang melakukan proses transaksi sebagai penyimpan data. Secara umum, sistem *mobile banking* menggunakan arsitektur seperti pada Gambar 4.



Gambar 4 Sistem *Mobile Banking*[5]

Berdasarkan gambar di atas, *connector layer* merupakan antarmuka antara sistem *mobile banking* dengan sistem bank yang melakukan transaksi sesungguhnya. Lapisan kedua, yaitu *service layer* berfungsi sebagai *layer* penghubung sekaligus menyembunyikan mekanisme akses antara *channel layer* dan *connector layer*. Lapisan pertama, yaitu *channel layer* berfungsi sebagai *layer* penghubung antara nasabah dengan sistem *mobile banking*.

Pada *channel layer* terdapat empat macam pendekatan utama[5]. Pendekatan pertama dan yang paling sederhana adalah *Interactive Voice Response* (IVR). IVR bekerja seperti layanan *customer service* dan ditunjukkan pada Diagram 1. Meskipun IVR sangat mudah untuk digunakan, layanan yang ditawarkan sangat terbatas sehingga *mobile banking* kemudian berkembang dengan memanfaatkan teknologi lain yaitu SMS.

Mobile banking dengan teknologi SMS (*Short Message Service*) dikenal dengan SMS *banking*. Nasabah cukup mengirimkan SMS berisi kode perintah tertentu ke nomor layanan SMS *banking* milik bank bersangkutan jika ingin melakukan transaksi. Setelah diterima oleh bank, maka bank akan merespon melalui *line* yang sama. Layanan ini banyak digunakan oleh nasabah karena semua jenis telepon genggam umumnya mendukung pemakaian layanan SMS dan hampir semua nasabah telepon genggam *familiar* dengan teknologi SMS. Selain itu, biaya layanan SMS jauh lebih murah dibandingkan biaya layanan melalui telepon.

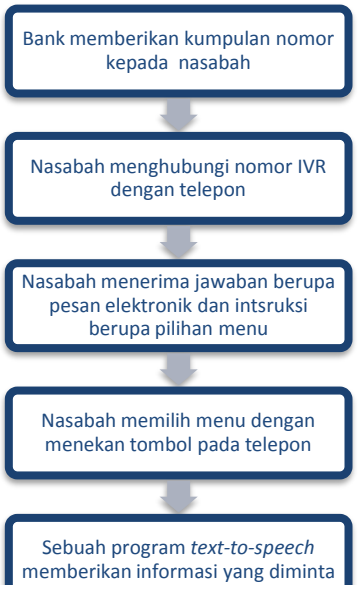


Diagram 1 Langkah kerja IVR[5].

Seperti yang telah dikatakan sebelumnya bahwa teknologi *mobile banking* berkembang seiring dengan berkembangnya teknologi komunikasi, maka *mobile banking* mulai merambah ke *mobile web* saat dimulainya era *smartphone*. Penggunaan *smartphone* yang mendukung *Wireless Application Protocol* (WAP) memudahkan nasabah untuk dapat mengakses web dari mana saja dan kapan saja sehingga nasabah dapat melakukan transaksi dengan antarmuka yang lebih interaktif dan mudah dimengerti (*user friendly*) dibandingkan melalui SMS. Teknologi ini juga lebih cepat, murah, dan mudah.

Selain dengan menggunakan *web browser* pada *smartphone*, saat ini penggunaan *mobile banking* makin dipermudah dengan adanya aplikasi khusus (*smart client*). Aplikasi ini dikembangkan oleh bank yang bersangkutan sehingga dapat tersedia untuk diunduh oleh nasabah.

C. *Prinsip Sistem Keamanan.*

Ketika perusahaan-perusahaaan di bidang perbankan menawarkan layanan *mobile banking*, keamanan dan kerahasiaan informasi nasabah merupakan hal utama yang harus diperhatikan. Klasifikasi keamanan berdasarkan elemen sistem dibagi menjadi tiga kelompok[6], yaitu:

a. Keamanan Jaringan: fokus kepada saluran (media) pembawa informasi.
b. Keamanan Aplikasi: fokus pada aplikasi yang digunakan, termasuk didalamnya adalah *database*
c. Kemanan Komputer: fokus kepada keamanan dari komputer termasuk *operating system (OS)*.

Terdapat lima prinsip keamanan pada suatu sistem yaitu[6]:

a. Privacy / Confidentiality. Proteksi ini dilakukan untuk menjaga data pribadi yang bersifat sensitif seperti data

[5] N. Jin and H. Xianling, "Mobile Banking Information Security and Protection Methods," IEEE, 2008

[6] Rahardjo, Budi. 2012. Prinsip Keamanan –*Security Principles*-, *(http://blendedlearning.itb.ac.id/app/course/info.php?id=125*, diakses tanggal 14 Maret 2013)

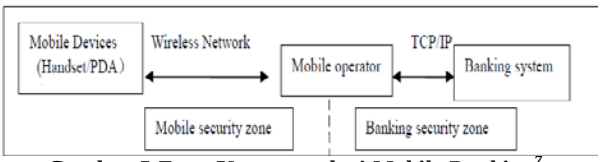
transaksi nasabah, biodata nasabah, jumlah saldo nasabah, dan lain-lain.

b. *Integrity.* Prinsip ini menitikberatkan pada informasi yang utuh atau berubah tanpa ijin.
c. *Availability.* Prinsip ini menyatakan bahwa informasi harus tersedia ketika dibutuhkan. Beberapa kasus dimana prinsip ini tidak dapat dijalankan yaitu ketika *server* dibuat *hang, down, crash,* ataupun lambat.
d. *Authentication.* Prinsip ini meyakinkan keaslian pihak yang mengakses data adalah pihak yang berhak. Pertanyaan penting dari prinsip ini adalah bagaimana mengenali nasabah bank pada *servis mobile banking.*
e. *Access control.* Prinsip ini merupakan mekanisme untuk mengatur siapa boleh melakukan apa.

III. ANALISIS PENERAPAN STEGANOGRAFI PADA SISTEM *MOBILE BANKING*

A. Masalah-masalah Keamanan Sistem *Mobile Banking*

Mobile banking memiliki dua zona yang perlu diamankan yaitu zona dari nasabah ke mobile operator dan zona dari mobile operator ke sistem bank seperti yang ditunjukkan pada Gambar 5. Gangguan dari penyerang biasanya dilakukan pada zona pertama yaitu zona melalui jaringan data tanpa kabel *(wireless network).* Dalam menggunakan jaringan data ini diperlukan teknologi yang dapat menjamin keaslian data yang dipertukarkan dalam jaringan. Jaringan radio dari satu sistem *mobile banking* tidak boleh terganggu oleh jaringan radio sistem lain yang dapat merusak keaslian data. Namun, keadaan teknologi *wireless* saat ini memungkinkan terjadinya kebocoran, kehilangan, atau perubahan terhadap informasi rahasia dalam transaksi-transaksi dengan *mobile banking*.



Gambar 5 Zona Kemanan dari *Mobile Banking*[7]

Beberapa teknik penyadapan data yang menyangkut keamanan informasi dalam sistem *mobile banking* adalah sebagai berikut[8].

a. Cross Frame Scripting

Penyerang mengirim sebuah *link* menuju halaman *web* yang berbahaya (misalnya mengandung virus) sekaligus mengambil data-data nasabah melalui halaman *web* tersebut.

b. Cross Site Request Forgery

Teknik ini bukanlah menyalahgunakan kepercayaan nasabah pada *website* bank yang dituju, melainkan menyalahgunakan kepercayaan *website* bank tersebut kepada penyimpanan data pada *cookie* atau *session* di sisi nasabah. Jadi pada teknik penyerangan ini, sebuah perintah seolah dikirimkan dari seorang nasabah yang sudah divalidasi kepada *website* yang sudah 'percaya' terhadap data-data di sisi klien (misalnya memiliki data *session* yang valid).

c. Reflection Injection

Ketika sebuah *website* melakukan otentikasi user tanpa menghapus validasi *session* yang lama, penyerang dapat menggunakan identitas *session* lama tersebut untuk masuk ke *website* yang bersangkutan. Dengan menggunakan identitas *session* lama, seperti *username* dan *password* yang sudah divalidasi, penyerang dapat mengambil informasi dari akun nasabah atau melakukan perubahan pada data milik nasabah.

B. Steganografi pada Sistem Keamanan *Mobile Banking*

Pengiriman informasi seperti saldo milik nasabah, data-data transaksi terakhir biasanya dilakukan melalui *website* atau (dengan permintaan nasabah) melalui saluran yang tidak aman. Dengan metode yang demikian, informasi mudah disadap oleh pihak ketiga sehingga mengakibatkan kebocoran informasi. Shirali-Shahreza (2007) memberikan gagasan untuk menyembunyikan semua informasi penting tersebut seperti *password* dengan metode steganografi dalam sebuah media gambar[9].

Ketika seorang nasabah melakukan permintaan atau ketika sistem harus mengirimkan informasi-informasi mengenai akun nasabah secara berkala, semua informasi tersebut disimpan dalam sebuah gambar. Gambar tersebut dibuat dalam format PNG dan disimpan di *website* bank yang bersangkutan. Setelah itu, sistem merespon permintaan nasabah dengan mengirimkan url gambar (*stego-image*) tersebut.

Algoritma untuk penyisipan informasi menggunakan metode LSB. Setiap byte *embedded message* dibagi menjadi 8 bit dan *cover-image* dibagi menjadi n blok dengan tiap blok terdiri dari m piksel. *Password* digunakan sebagai *stego-key* untuk memilih dua piksel dari *embedded message* untuk disisipi dan juga memilih blok mana yang akan disisipi. Kemudian akan dilakukan penyisipan piksel *embedded message* pada RGB *cover-image.* Hal ini dilakukan sampai semua *embedded message* telah disisipi.

Di pihak nasabah, gambar tersebut diterjemahkan oleh sebuah aplikasi *mobile* yang disediakan oleh bank dan dapat diunduh oleh nasabah sebelum proses komunikasi ini berlangsung. Setelah itu, aplikasi tersebut akan mengunduh gambar dari url dan melakukan ekstraksi informasi dari gambar tersebut

C. Analisis Sistem Keamanan *Mobile Banking* Memanfaatkan Steganografi.

Berdasarkan gagasan yang disampaikan pada bab III bagian B, dapat ditarik informasi bahwa dalam penerapan steganografi pada sistem keamanan terdapat dua pihak yang saling berkomunikasi yaitu:

[7] N. Jin and H. Xianling, "Mobile Banking Information Security and Protection Methods," IEEE, 2008.

[8] http://money.howstuffworks.com/personal-finance/online-banking/mobile-banking2.htm

[9] M. Shirali-Shahreza, "Improving Mobile Banking Security Using Steganography," IEEE, 2007.

a. *Server*. Bagian *server* berfungsi untuk menyimpan informasi (sebagai pusat informasi), merespon permintaan nasabah dengan mengirimkan informasi yang diinginkan, menyisipkan informasi pada *cover-object*, dan mengirimkan url *stego-image* pada *mobile phone* nasabah.
b. Nasabah. Bagian nasabah berfungsi untuk mengirimkan permintaan, menerima url *stego-image*, mengunduh *stego-image*, dan mengekstrasi pesan/informasi yang disisipkan.

Selain itu, berdasarkan studi literatur yang telah dilakukan, didapatkan informasi bahwa terdapat dua hal penting yang diperhatikan dalam proses tukar-menukar informasi antara *server* dan nasabah yaitu:

a. Tingkat keamanan pesan (informasi rahasia). Tingkat keamanan ini bergantung pada apakah pesan dapat dengan mudah diekstrasi/dipecahkan oleh pihak lain. Cara yang dapat dilakukan oleh pihak lain antara lain dengan berusaha memecahkan kunci atau mencuri kunci untuk mengekstrasi pesan tersebut. Hal ini terkait dengan prinsip keamanan yang pertama yaitu *privacy/ confidentiality.*
b. Kecepatan pemrosesan enkripsi untuk membuat pesan tidak dapat diketahui pihak selain nasabah yang berhak. Besar kapasitas yang diperlukan *server* untuk pemrosesan juga perlu diperhatikan karena jika pemrosesan "terlalu berat" bagi *server* maka dapat membuat *server* tidak dapat/lambat dalam melayani semua permintaan yang datang dari nasabah. Hal ini terkait dengan prinsip keamanan yang kedua yaitu *availability*. Selain itu, layanan yang lambat dapat berpengaruh negatif pada kepuasan nasabah dalam menggunakan layanan tersebut.

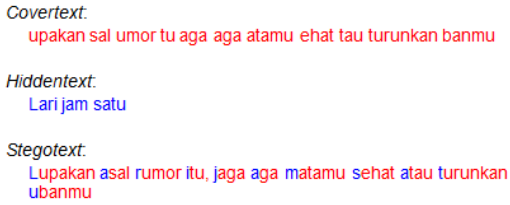
Kedua hal penting yang disebutkan di atas akan menjadi bahan analisis penulis dalam menganalisis penerapan steganografi sistem keamanan *mobile banking.*

Analisis pertama terkait dengan pemilihan *cover-media. Cover-media* yang dipilih adalah gambar bukan audio maupun video. Menurut penulis, pemilihan *cover-media* berupa gambar untuk penerapan steganografi pada sistem keamanan sudah tepat. Alasan untuk pernyataan tersebut sebagai berikut:

a. Indra pendengaran manusia jauh lebih sensitif dibandingkan dengan indra penglihatan manusia. Seseorang cendrung dapat peka terhadap sedikit perubahan pada suara dibandingkan dengan sedikit perubahan pada visual. Demi mencapai tujuan steganografi yaitu membuat keberadaan pesan tidak diketahui oleh pihak luar, maka penyisipan pesan pada media gambar lebih tepat dibandingkan pada media audio.
b. Penyisipan pada media video memakan waktu lebih banyak dibandingkan pada media gambar karena video terdiri dari banyak gambar. Kecepatan proses penyisipan pada *server* juga patut dipertimbangkan karena sangat mungkin terjadi permintaan transaksi dari banyak nasabah dalam waktu yang bersamaan. Oleh karena itu, diperlukan proses yang sederhana dan cepat sehingga *server* dapat melayani semua permintaan yang datang dan juga menghindari keadaan kelebihan beban *(overload)* pada *server.*

Namun, steganografi menggunakan media gambar memiliki kelemahan. Media yang melalui proses pengompresan dapat menyebabkan hilangnya beberapa bagian sehingga hasil pengekstrasian pesan tidak utuh. Oleh karena itu, pemilihan media gambar yang tidak terkompresi harus diperhatikan.

Analisis kedua terkait dengan *mobile phone* yang digunakan oleh nasabah sehingga dapat mendukung gagasan penerapan steganografi pada sistem ini. Pada bagian C, telah dijelaskan bahwa aplikasi di pihak nasabah berfungsi untuk menerima url/alamat dari *stego-object* dan mengekstraknya berdasarkan *password* yang dimasukkan oleh nasabah. Oleh karena itu, diperlukan *mobile phone* yang memiliki fasilitas untuk mendukung aplikasi yang dapat mengunduh dan mengekstrak gambar dari pesan. Kelemahan dari gagasan ini adalah tidak memperhitungkan kemungkinan nasabah yang tidak memiliki *mobile phone* dengan fasilitas yang disebutkan di atas. Namun, hal ini dapat disiasati dengan pengiriman url melalui SMS. Url tersebut dimasukkan pada aplikasi bank di PC (*Personal Computer*) milik nasabah. Melalui url tersebut, aplikasi akan mengunduh *stego-object* dan mengekstrasinya. Oleh karena itu, dapat disimpulkan bahwa aplikasi harus tersedia untuk berbagai *platform* seperti Android, Mac, Windows 7 dan PC. Alternatif kedua adalah melakukan steganografi pesan dengan media teks. Namun, hal ini sangat tidak disarankan untuk diterapkan karena pola-pola yang dihasilkan dapat terbaca oleh penyerang sehingga mudah untuk dipecahkan. Tanpa *password* yang benar dari pengguna, pesan yang disembunyikan dapat diketahui. Contoh steganografi pada teks ditunjukkan Gambar 6.



Gambar 6 Contoh Metode Steganografi dengan Media Teks[2]

Analisis ketiga membahas hubungan antara masalah-masalah keamanan yang terjadi dengan solusi penerapan steganografi yang ditawarkan. Masalah keamanan yang terjadi secara garis besar tentang pertukaran informasi penting dan rahasia seperti *password* pada saluran yang tidak aman. Masalah muncul jika pihak lain dapat menyadap informasi, memanfaatkan informasi tersebut dan mengakibatkan kerugian bagi nasabah. Solusi pertukaran informasi rahasia yang aman merupakan kunci dari masalah tersebut.

Upaya untuk mengamankan informasi rahasia dari pihak yang tidak berkepentingan dapat dilakukan dengan memanfaatkan kriptografi klasik. Namun, kebanyakan kriptografi klasik saat ini telah dipecahkan oleh kriptanalis. Kriptografi klasik mudah dipecahkan dengan berbagai metode antara lain metode terkaan, analisis frekuensi kemunculan huruf, metode kasiski, dan membandingkan beberapa pasangan plainteks dan chiperteks sehingga didapatkan kuncinya. Dengan

berbagai kelemahan tersebut, kemungkinan informasi rahasia nasabah bocor cukup besar jika memanfaatkan kriptografi klasik.

Kriptografi modern muncul karena kelemahan-kelemahan kriptografi klasik seperti yang dijelaskan di atas. Kriptografi modern sendiri dapat dikelompokan dalam dua bagian yaitu kriptografi kunci simetrik dan kriptografi kunci asimetris. Kriptografi kunci simetrik sendiri memiliki proses enkripsi yang kompleks. Sebagai contoh proses enkripsi pada kriptografi DEA (*Data Encryption Algorithm*) dapat dilihat pada [2]. Proses enkripsi yang kompleks pada kriptografi modern membuat tingkat kesulitan memecahkan pesan semakin meningkat. Namun, kelemahan dari kriptografi kunci simetri adalah pendistribusian kunci rahasia kepada penerima (dalam hal ini nasabah). Pengiriman kunci rahasia melalui saluran publik yang tidak aman sama seperti mengirimkan informasi rahasia tersebut dalam bentuk polos (*plain*) karena apabila kunci rahasia diketahui pihak lain maka pesan yang telah dienkripsi dapat dengan mudah dipecahkan. Selain itu, kunci yang harus disediakan oleh pihak bank untuk tiap nasabahnya haruslah berbeda-beda sehingga jumlah kunci yang dibuat cukup banyak yaitu sebanyak jumlah nasabah yang ada. Hal ini membuat kriptografi modern simetris kurang efektif untuk diterapkan dalam sistem keamanan *mobile banking*.

Kriptografi kunci asimetris berbeda dengan kriptografi simetris. Hanya terdapat dua kunci yang digunakan yaitu *public key* dan *private key*. *Public key* digunakan dalam proses enkripsi dan *private key* digunakan dalam proses dekripsi. Dalam kriptografi ini tidak terjadi pengiriman kunci rahasia sehingga tidak ada kemungkinan kunci bocor. Untuk lebih lengkapnya mengenai kriptografi asimetrik dapat dilihat pada [2]. Namun, kelemahan dari kriptografi ini adalah proses enkripsi dan dekripsi pesan yang lebih lambat dibandingkan kriptografi kunci simetris. Hal ini dikarenakan enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar. Selain itu, kriptografi asimetrik kurang sesuai dengan kebutuhan sistem keamanan *mobile phone*. Pada sistem pengiriman informasi *mobile phone*, pihak *server* (satu) mengirimkan informasi rahasia kepada pihak nasabah (banyak) dan pihak yang melakukan dekripsi adalah pihak nasabah. Sedangkan, pada kriptografi asimetrik pihak yang melakukan enkripsi menggunakan *public key* (banyak) mengirimkan pesan kepada pihak yang melakukan deksripsi menggunakan *private key* (satu). Berdasarkan penjelasan tersebut, pemanfaatan kriptografi kunci asimeterik juga tidak dapat menekan jumlah kunci yang harus dibuat oleh bank untuk nasabahnya.

Penerapan steganografi seperti yang digagaskan dalam bagian C menunjukan bahwa pertukaran informasi rahasia (*password*) dapat dihindari. Pihak nasabah dan *server* tidak harus mempertukarkan *password* melalui saluran internet (tidak aman). Pihak nasabah hanya perlu mengirimkan permintaan informasi yang diinginkannya pada *server*, kemudian *server* akan menyisipkan informasi tersebut pada media gambar kemudian mengirimkan url *stego-object* tersebut pada nasabah. Pihak nasabah akan mengunduh *stego-object* dan mengekstrasinya pada aplikasi yang dimilikinya dengan memasukkan *password* yang dimilikinya. Jika *password* yang dimilikinya benar maka pesan hasil ekstraksi yang dimilikinya akan bernilai benar dan sebaliknya akan salah jika *password* yang dimasukkannya salah. Analisis kedua terkait proses pemrosesan yang dilakukan pada *server*. Kecepatan respon/transaksi antara nasabah dan *server* juga meningkat karena jumlah informasi yang dipertukarkan berkurang. Hal ini disebabkan nasabah dan *server* hanya mempertukarkan url dari gambar dan bukan gambar itu sendiri. Meskipun proses penyisipan pesan pada media gambar di *server* memerlukan "tambahan kapasitas kerja" di pihak *server*, hal ini tidak terlalu "membebani" pihak *server* karena proses steganografi dilakukan pada media gambar dan memanfaatkan metode LSB. Penggunaan steganografi juga bermanfaat untuk menghindari kecurigaan dari penyerang. Hal ini dikarenakan hasil gambar (*stego-image*) tidak banyak berubah sehingga penyerang tidak menyadari keberadaan pesan.

Analisis berikutnya mengenai tingkat kesulitan pengekstrasian pesan (informasi rahasia) menggunakan metode ini. Dalam metode steganografi, sulit untuk mengekstrasi *embedded message* dari *covered-object* tanpa mengetahui *password*-nya (*stego-key*). Hal ini dikarenakan peran kunci yang sangat penting dalam proses penyisipan dan pengekstrasian pesan. Kunci digunakan sebagai alat untuk mengetahui letak bit-bit pesan disisipkan.

D. Kelebihan dan Kekurangan Sistem Keamanan *Mobile Banking* Menggunakan Steganografi

Berdasarkan pemaparan-pemaparan yang telah disebutkan, didapatkan informasi terkait kelebihan jika menggunakan steganografi antara lain:

a. Jika menggunakan steganografi, infromasi tidak pernah ditukarkan atau disebarkan di internet dalam bentuk *plain* sehingga kemungkinan informasi didapatkan oleh pihak penyerang rendah.
b. Pertukaran *password* tidak diperlukan lagi antara *server* dengan nasabah
c. Kecepatan respon/ transaksi antara nasabah dan sistem bank meningkat. Hal ini memenuhi prinsip keamanan *privacy/ confidentiality*.
d. Sulit untuk mengekstrasi *embedded message* dari *covered-object* tanpa mengetahui *password*-nya (*stego-key*). Hal ini memenuhi prinsip keamanan *availability*.
e. Penggunaan steganografi juga bermanfaat untuk menghindari kecurigaan dari penyerang.

Selain kelebihan-kelebihan yang dimiliki jika memanfaatkan metode steganografi dalam sistem keamanan *mobile banking*, terdapat juga kelemahan pada metode ini yaitu:

a. Metode ini hanya berlaku untuk *mobile banking* melalui *smartphone* maupun *mobile device* yang memiliki fasilitas internet dan ekstrasi gambar.
b. Media gambar yang digunakan terbatas pada media yang tidak mengalami pengompresan seperti PNG, GIF, atau BMP.

E. Penerapan Metode Steganografi pada Sistem Keamanan *Mobile Banking*

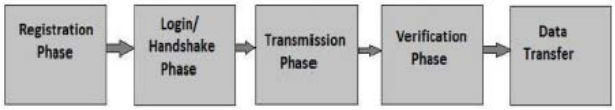
Berdasarkan kelebihan dan kekurangan dari metode steganografi ini, penerapannya dalam sistem keamanan dapat dilakukan pada proses pengiriman data nasabah dan otentikasi. Ide terkait penerapan pada tiap proses dijelaskan sebagai berikut:

a. Proses Pengiriman Data Nasabah.

Metode proses pengiriman data ini sama seperti yang dijelaskan pada bagian C. Data akan disembunyikan pada media gambar dan alamat hasil proses steganografi (*stego-object*) akan dikirimkan pada nasabah. Aplikasi di pihak nasabah akan mengunduh dan mengekstrak isi pesan (informasi data saldo, data-data transaksi, dan sebagainya). Ekstrasi dapat dilakukan jika nasabah memasukkan *password* yang benar pada aplikasi tersebut.

b. Otentikasi

Otentikasi merupakan proses untuk menyakinkan bahwa nasabah yang sedang mengakses adalah nasabah yang asli/ nasabah yang berhak. Masalah yang paling sulit dikendalikan dalam proses otentikasi adalah keamanan pada saluran komunikasi. Seperti yang telah dibahas pada bagian B, sistem *mobile banking* saat ini kebanyakan memanfaatkan jaringan *wireless* untuk melakukan transfer data. Kemungkinan terjadinya penyadapan data atau pengubahan data sampai ke pihak tujuan masih sangat besar karena jaringan *wireless* yang belum tentu aman. Proses otentikasi sistem *mobile banking* terdiri dari lima fase seperti yang ditunjukkan pada Gambar 7[10]. Teknik steganografi dapat diterapkan pada tahap ketiga, yaitu fase transmisi. Pada fase transmisi data yang diterima dari fase registrasi dan login akan ditransmisikan dari pengguna ke server bank melalui internet. Pada tahap inilah informasi paling rentan untuk diserang. Pada proses otentikasi dengan steganografi, nasabah akan mengirimkan sebuah identitas dan *password* bersama dengan gambar yang digunakan untuk menyembunyikan informasi. Gambar yang digunakan adalah gambar-gambar yang berhubungan dengan kehidupan biasa atau gambar lain yang dengan mudah diabaikan oleh pihak penyerang. Proses penyisipan pesan pada media gambar sama seperti yang dijelaskan pada bagian C. Pada fase verifikasi, pihak bank akan menerima informasi tersebut dan mengekstraknya. Jika ID dan *password* terdefinisi dalam *database* bank maka proses selanjutnya dapat dilanjutkan, tetapi jika tidak maka proses akan diulangi atau dihentikan sampai ID dan *password* yang diberikan oleh nasabah benar (terdefinisi).



Gambar 7 Fase yang terjadi dalam proses otentikasi[10]

[10] S. Anup, K. Suraj, P. Rahul and D. Harshad, "Survey on 2-Step Security for Authentication in M-Banking," IISTE, 2011.

VI. KESIMPULAN

Berdasarkan studi literatur yang telah dilakukan, dapat dilihat bahwa sistem keamanan merupakan elemen yang sangat penting dalam teknologi *mobile banking*. Dengan semakin maraknya pengguna *mobile banking*, ancaman dari luar untuk mengambil informasi-informasi rahasia juga semakin banyak. Salah satu metode yang dapat digunakan adalah steganografi.

Meskipun metode ini tergolong sangat umum dan cukup sederhana, tapi metode steganografi sangat menjanjikan untuk mencegah terjadinya kebocoran informasi dengan cukup efektif. Steganografi dapat diterapkan dalam proses otentikasi dan juga dapat meningkatkan keamanan informasi jika digunakan dalam proses pertukaran informasi secara keseluruhan. Dengan demikian, penyadapan informasi menjadi sulit dilakukan dan komunikasi antara bank dan nasabah juga lebih aman.

Di masa depan, sistem keamanan *mobile banking* dapat lebih banyak menerapkan metode steganografi yang dikombinasikan dengan metode keamanan lain, seperti kriptografi. Dengan demikian, data tersebut semakin sulit untuk diambil oleh pihak yang tidak berkepentingan.

V. REFERENCES

Munir, Rinaldi. 2012. *Algoritma Kriptografi Klasik*, (*http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2010-2011/kripto10-11.htm#SlideKuliah*, diakses tanggal 14 Maret 2013)

Rahardjo, Budi. 2012. Prinsip Keamanan *–Security Principles-, (http://blendedlearning.itb.ac.id/app/course/info.php?id=125*, diakses tanggal 14 Maret 2013)

N. Jin and H. Xianling, "Mobile Banking Information Security and Protection Methods," IEEE, 2008.

B. Cao and Q.-M. Fan, "The Infrastructure and Security management of Mobile Banking System," IEEE, 2010.

D. N. Meghanathan, "Jackson State University," 5 June 2011. [Online]. Available:http://www.jsums.edu/cms/tues/docs/Steganography/Basics-Steganography-Security.pdf. [Accessed 15 Maret 2013].

S. Anup, K. Suraj, P. Rahul and D. Harshad, "Survey on 2-Step Security for Authentication in M-Banking," IISTE, 2011.

M. Shirali-Shahreza, "Improving Mobile Banking Security Using Steganography," IEEE, 2007.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 28 Maret 2013

ttd

Amelia Natalie / 13509004