PROTEKSI KEAMANAN DOKUMEN TRANSAKSI BERUPA FILE IMAGE, JPG ATAU TIF TRANSFER ANTAR BANK MENGGUNAKAN STEGANOGRAFI DAN KRIPTOGRAFI

Sucipto Basuki[1], Mustar Aman[2], Reksa Anugrah[3]
Sekolah Tinggi Manajemen Informatika dan Komputer Insan Pembangunan
Jl. Raya Serang Km. 10 Bitung – Tangerang. Tlp.(021) 59492836, Fax. (021) 59492837
Email : ciptainsan@yahoo.com, mustar_ip@yahoo.com, reksa_anugrah@yahoo.com,

ABSTRACT

Information security process can be done by hiding the information on other media or by certain methods, so that other people do not realize there is some information in the media. Technique known as Steganography and Cryptography. Steganography is a technique to hide or disguise the existence of secret messages in the media reservoirs. While Cryptography disguise the meaning of a message, but do not hide that there is a message. In a bank cannot be separated in the presence of inter-bank transactions which transfer if the transfer interbank transactions done in branch offices and nominal transaction exceeds the transaction limit branch offices will require official approval in the upper branch. How do I prove the authenticity of the document transfer transaction? Therefore, a company in the banking sector needs to be a medium to prove the validity of the document sent by the branch transaction. In this case the author has designed an application with a blend of steganography and cryptography techniques that can be used in testing the validity of the transaction document. By using steganographic techniques undercover in a media that has brought and cryptographic key assignment as random, then the document that is sent in the branch office can be proved.

Keywords: Steganography, Cryptography, certificates, validity, proof

ABSTRAK

Proses pengamanan informasi dapat dilakukan dengan menyembunyikan informasi tersebut pada media lain atau dengan metode tertentu, sehingga orang lain tidak menyadari ada suatu informasi didalam media tersebut. Dikenal dengan teknik Steganografi dan Kriptografi. Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam media penampungnya. Sedangkan Kriptografi menyamarkan arti dari suatu pesan, tetapi tidak menyembunyikan bahwa ada suatu pesan. Di dalam sebuah perbankan tidak lepas dengan adanya transaksi transfer antar bank dimana apabila transaksi transfer antar bank dilakukan di kantor cabang pembantu dan nominal transaksi melebihi limit transaksi kantor cabang tersebut maka diperlukan approval pejabat di atas kantor cabang tersebut. Bagaimana cara membuktikan keaslian document transaksi transfer tersebut? Oleh karena itu sebuah perusahaan dibidang perbankan perlu adanya media untuk membuktikan keabsahan document transaksi yang dikirimkan oleh cabang. Dalam hal ini penulis telah merancang sebuah aplikasi dengan perpaduan teknik steganografi dan kriptografi yang dapat digunakan dalam pengujian keabsahan dari document transaksi tersebut. Dengan menggunakan teknik steganografi yang melakukan penyamaran pada media yang dibawa dan kriptografi yang mempunyai tugas sebagai kunci acak, maka dokument yg di dikirimkan kantor cabang dapat di buktikan.

Kata Kunci : Steganografi, Kriptografi, keabsahan, pembuktian

1. PENDAHULUAN

Pertukaran informasi melalui media internet merupakan salah satu keuntungan yang diperoleh dari berkembangnya teknologi saat ini. Bagaimana menjaga kemanan data yang dikirim serta Menjamin keabsahan data yang diterima merupakan salah satu yang menjadi tujuan utama. Dalam dunia komputer, ada 2 istilah teknik keamanan data yang sangat dikenal yaitu steganografi dan kriptografi. Steganografi adalah teknik menyembunyikan atau menyamarkan keberadaan pesan rahasia dalam media penampungnya. Sedangkan Kriptografi menyamarkan arti dari suatu pesan, tetapi tidak menyembunyikan bahwa ada suatu pesan. Secara teori, semua file yang ada didalam komputer dapat digunakan sebagai media penampung pesan, seperti file citra berformat JPG, TIF, BMP, file audio berformat MP3, WAV, bahkan didalam

sebuah video dengan format AVI, atau dalam format lainya seperti TXT, HTML, PDF.

Di dalam sebuah perbankan tidak lepas adanya transaksi transfer antar bank. Jika transaksi transfer antar bank dilakukan dicabang pembantu yang nominal transaksinya tidak melebihi limit transaksi kantor cabang tersebut tidak akan menjadi kendala karena tidak memerlukan approval pejabat diatas kantor cabang tersebut. Lain cerita jika transaksi dikantor cabang tersebut nominalnya melebihi limit transaksi kantor cabang tersebut, Artinya transaksi transfer antar bank tersebut memerlukan approval pejabat diatas kantor cabang tersebut. Pejabat diatas kantor cabang tersebut mengunduh document transaksi transfer antar bank tersebut melalui email kantor. Apa yang akan menjadi bukti keaslian document transaksi tersebut yang dikirim dari kantor cabang? Oleh karena itu sebuah perbankan perlu adanya media untuk membuktikan tentang keabsahan dokumen yang di dikirimkan oleh kantor cabang pembantunya.Dengan adanya teknik steganografi yang melakukan penyamaran pada media yang di bawah dan kriptografi yang mempunyai tugas sebagai kunci acak maka dokumen yg di kirim oleh kantor cabang dapat di buktikan.

1.1 TUJUAN

Tujuan dari penelitian ini adalah merancang suatu sistem atau aplikasi dengan menggunakan teknik steganografi dan kriptografi yang digunakan untuk enkripsi dan menguji keabsahan data digital terutama document transaksi perbankan dalam bentuk file JPEG,BMP dan TIF. Pejabat yang akan mengapprove transaksi akan merasa aman.

1.2 BATASAN MASALAH

Permasalahan yang ditemukan selama penelitian ini dibatasi oleh hal-hal yang berkut ini : Implementasi teknik steganografi untuk mengamankan data digital document transaksi dalam bentuk file JPEG,BMP dan TIF dan teknik kriptografi untuk mengetahui isi pesan dari data digital dokument dengan metode decrypt.

2. TEORI DASAR

Dalam dunia komputer, ada 2 istilah teknik keamanan data yang sangat dikenal yaitu steganografi dan kriptografi.

a. Steganografi

Menurut Jati Sasongko dari Fakultas Teknologi Informasi, Universitas Stikubank Semarang. Tahun 2004 berjudul "*Pengamanan Data Informasi menggunakan Kriptografi Klasik*", Steganografi (steganography) adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata "steganografi" berasal dari bahasa Yunani ***"steganos"***, yang artinya "tersembunyi atau terselubung", dan ***"graphein"***, "menulis".

Sebuah pesan steganografi (*plaintext*), dienkripsikan dengan beberapa arti tradisional, yang menghasilkan *ciphertext*. Kemudian, *covertext* dimodifikasi dalam beberapa cara sehingga berisi *ciphertext*, yang menghasilkan *stegotext*. Contohnya, ukuran huruf, ukuran spasi, jenis huruf, atau karakteristik *covertext* lainnya dapat dimanipulasi untuk membawa pesan tersembunyi. Hanya penerima (yang harus mengetahui teknik yang digunakan) dapat membuka pesan dan mendekripsikannya. Format yang biasa digunakan dengan menggunakan teknik steganografi di antaranya:

- Format *image* : bitmap (bmp), tif, pcx, jpeg, dll.
- Format audio : wav, voc, mp3, dll.
- Format lain : teks file, html, pdf, dll.

b. Kriptografi

Kriptografi (cryptography) merupakan ilmu dan seni untuk menjaga pesan agar aman. (Cryptography is the art and science of keeping messages secure) "*Crypto*" berarti "secret" (rahasia) dan "*graphy*" berarti "writing" (tulisan). Para pelaku atau praktisi kriptografi disebut cryptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat. Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh

orang yang tidak berhak. Data yang dienkripsi dapat disandikan dengan menggunakan sebuah kunci (key). Untuk membuka (decrypt) data tersebut digunakan juga sebuah kunci yang sama dengan kunci untuk mengenkripsi (untuk kasus private key cryptography) atau dengan kunci yang berbeda (untuk kasus public key cryptography).

PERBEDAAN STEGANOGRAFI DAN KRIPTOGRAFI

Steganografi dan kriptografi mempunyai prinsip kerja yang berbeda, meskipun keduanya mempunyai hubungan yang dekat dalam dunia keamanan data.

Hasil dari **kriptografi** biasanya berupa data yang berbeda dari bentuk aslinya dan biasanya data seolah-olah berantakan sehingga tidak dapat diketahui informasi apa yang terkandung didalamnya (namun sesungguhnya dapat dikembalikan ke bentuk semula lewat proses dekripsi), sedangkan hasil keluaran dari **steganografi** memiliki bentuk persepsi yang sama dengan bentuk aslinya. Kesamaan persepsi tersebut adalah oleh indera manusia (khususnya visual), namun bila digunakan komputer atau perangkat pengolah digital lainnya dapat dengan jelas dibedakan antara sebelum proses dan setelah proses.

2.1 METODOLOGI PENELITIAN

a. Fase Analisis

- ❖ Studi Literatur, Studi ini dilakukan dengan cara mencari sekaligus mempelajari beberapa literatur dan artikel mengenai steganografi dan kriptografi sebagai acuan dalam perencanaan dan pembuatan sistem atau aplikasi.
- ❖ Pendefinisian dan analisis masalah untuk mencari solusi yang tepat
- ❖ Studi Pustaka

b. Fase Pembuatan Program

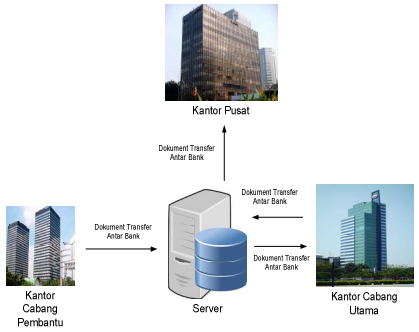
Perancangan dan implementasi sistem yang dilakukan secara ekperimental, yaitu bereksperimen membuat program berdasarkan materi dan algoritma yang telah dipelajari.

c. Pengujian Program

Pengujian dilakuakan terhadap program yang telah dibuat.

2.2. POLA PIKIR

Dengan banyak aplikasi atau *tool software* desain grafis dan foto *editing* yang beredar di pasaran maka sangat rentan sekali document di palsukan. Dan bagaimana bentuk pertanggung jawaban sebuah perbankan untuk menjamin transaksi nasabah aman. Jika kasusnya adalah transaksi antar bank dilakukan di cabang nominalnya tidak melebihi limit kantor cabang tersebut maka tidak ada masalah karena tidak memerlukan approval pejabat kantor cabang diatas cabang tersebut. Bagaimana jika kasusnya adalah transaksi antar bank nominalnya melebihi limit kantor cabang tersebut, sehingga memerlukan approval pejabat diatas kantor cabang tersebut ? Bagaimana document transaksi antar bank tersebut dapat dicek keaslianya ? Berdasarkan kasus tersebut perlu rancangan sistem yang dapat melakukan fungsi tersebut, sehingga sebuah keaslian document transaksi transfer antar bank dapat di pertanggung jawabkan. Berikut ini disampaikan ilustrasi permasalahan yang dialami pada transaksi transfer antar bank yang nominalnya melebihi limit kantor cabang dan memerlukan approval pejabat diatas kantor cabang tersebut.



Gambar 1. Ilustrasi Transaksi Transfer Antar Bank yang memerlukan Approval Pejabat diatas Kantor Cabangnya

Untuk menjawab permasalah tersebut kita perlu mempelajari permasalah yang sudah ada dari penelitian sebelumnya agar hasil akhirnya dapat memecahkan permasalahan yang ada. Studi ini dilakukan dengan cara mencari sekaligus mempelajari beberapa literatur dan artikel mengenai steganografi dan kriptografi sebagai acuan dalam perencanaan dan pembuatan sistem atau aplikasi. Dalam upaya pengembangan penelitian ini perlu dilakukan

studi pustaka sebagai salah satu dari penerapan metode penelitian yang akan dilakukan. Diantaranya adalah mengidentifikasikan persamaan dari steganografi dan kriptografi, mengidentifikasikan metode yang pernah dilakukan, meneruskan penelitian sebelumnya, serta mengetahui orang lain yang spesialisasi dan area penelitiannya sama dibidang ini. Beberapa *Literature review* tersebut adalah sebagai berikut :

a. Penelitian ini dilakukan oleh Jati Sasongko dari Fakultas Teknologi Informasi, Universitas Stikubank Semarang. Tahun 2004 berjudul "*Pengamanan Data Informasi menggunakan Kriptografi Klasik*". Penelitian ini membahas mengenai Algoritma yang digunakan untuk menentukan kekuatan dari enkripsi. Keamanan sebuah algoritma yang digunakan dalam enkripsi atau dekripsi bergantung kepada beberapa aspek. Salah satu aspek yang cukup penting adalah sifat algoritma yang digunakan. Apabila kekuatan dari sebuah algoritma sangat tergantung kepada pengetahuan (tahu atau tidaknya) orang terhadap algoritma yang digunakan, maka algoritma tersebut disebut "restricted algorithm". Apabila algoritma tersebut bocor atau ketahuan oleh orang banyak, maka pesan-pesan dapat terbaca. Tentunya hal ini masih bergantung kepada adanya kriptografer yang baik. Jika tidak ada yang tahu, maka sistem tersebut dapat dianggap aman (meskipun semu) [1].
b. Penelitian ini dilakukan oleh Yogie Aditya, Andhika Pratama dan Alfian Nurlifa dari Fakultas Teknologi Industri, Universitas Islam Indonesia tahun 2010 berjudul *"Studi Pustaka Untuk Steganografi Dengan Beberapa Metode*". Penelitian ini dilakukan dengan menggunakan metode *LSB(Least Significant Bit)* dan *EOF(End Of File)*. Pada penelitian ini, dijelaskan bahwa metode LSB bekerja dengan cara menambahkan bit data yang akan disembunyikan (pesan) di bit terakhir yang paling cocok atau kurang berarti. Sehingga Jika dilihat berdasarkan ukuran *stego image* LSB lebih baik karena tidak mengubah ukuran file yang disisipi, namun untuk kualitas *image*, LSB banyak mengurangi kualitas *image* yang semula. Sedangkan cara kerja metode EOF adalah dengan menambahkan data atau file yang akan disembunyikan lebih dari ukuran file image. Data yang disembunyikan tersebut akan disisipkan pada akhir file sehingga file image akan terlihat sedikit berbeda dengan aslinya. Ada penanda khusus yang terlihat dari file image di paling bawah seperti garis-garis. Sehingga Untuk kualitas *image,* EOF lebih baik karena kualitas *image* tetap terjaga, namun ukuran file lebih besar dari sebelum disisipi oleh pesan [2].

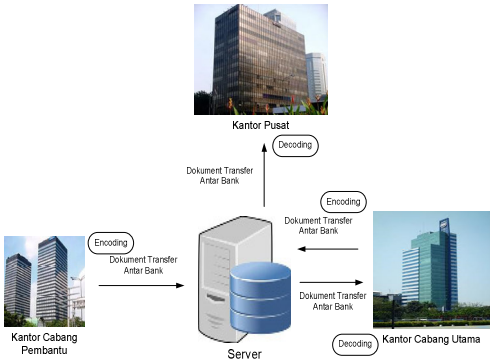
No	Metode	Size Image	Size Pesan	Stego Image
1	LSB	150x200	422 karakter	150x200
2	EOF	150x200	422 karakter	153x200

Tabel 1. Tabel Hasil Perbandingan Ukuran *Stego Image*

c. Penelitian ini dilakukan oleh David, A. Murtado dan Utin Kasma dari program Studi Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak tahun 2012 berjudul *"Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online*". Penelitian ini membahas aplikasi steganografi dengan metode LSB yang melukan penyisipan berbagai jenis data dengan ekstensi yang berbeda. Ukuran dari file bitmap setelah disisip (*Stego Bitmap*) tidak mengalami perubahan dari ukuran file bitmap sebelumnya (*Cover Bitmap*). Metode LSB juga dapat melakukan manipulasi BPC (*Bit Per Channel*) untuk meningkatkan daya tamping cover bitmap semaksimal mungkin. Dengan metode LSB, efisiensi waktu enkripsi dan dekripsi yang relatife cepat dan integritas data sebelum dan sesudah proses ekstrak tidak mengalami perubahan sama sekali.[3]

d. Penelitian ini di lakukan oleh Andreas Westfeld.Technische Universit¨at Dresden Institute for System Architecture, Germany pada tahun 2006 berjudul "*Steganalysis in the Presence of Weak Cryptography and Encoding*" Penelitian ini membahas masalah pada kelemahan pada kriptografi pada ecoding. [4].

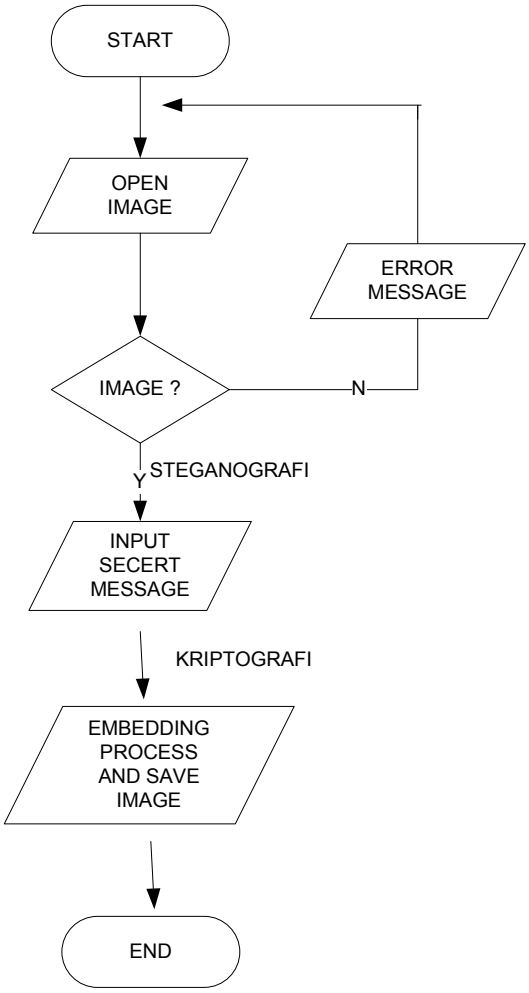
Dari *Literature review* yang di utarakan di atas kami dapat menarik sebuah titik terang untuk memecahkan permasalahan yang sedang kami hadapi dengan tehnik steganografi dan kriptografi. Kedua teknik ini dapat di terapkan pada sebuah document transaksi transfer antar bank yang dikirimkan cabang-cabang Dari jenis kebutuhan tersebut dan di gabungkan dengan Steganografi dan kriptografi makan konsep yang terjadi adalah untuk dokumen yang penting maka cukup dengan melakukan steganografi sebagai bukti keaslian sebuah dokumen yang di cabang-cabang. Sedangkan jika dokument tersebut sangat rahasia maka untuk steganografi dan kriptografi berkolaborasi. Untuk lebih jelasnya tentang permasalahan di atas makan penjelasanya dapat di gambarkan sebagai berikut:



Gambar 2. Ilustrasi Transaksi Transfer Antar Bank yang memerlukan Approval Pejabat diatas Kantor Cabangnya

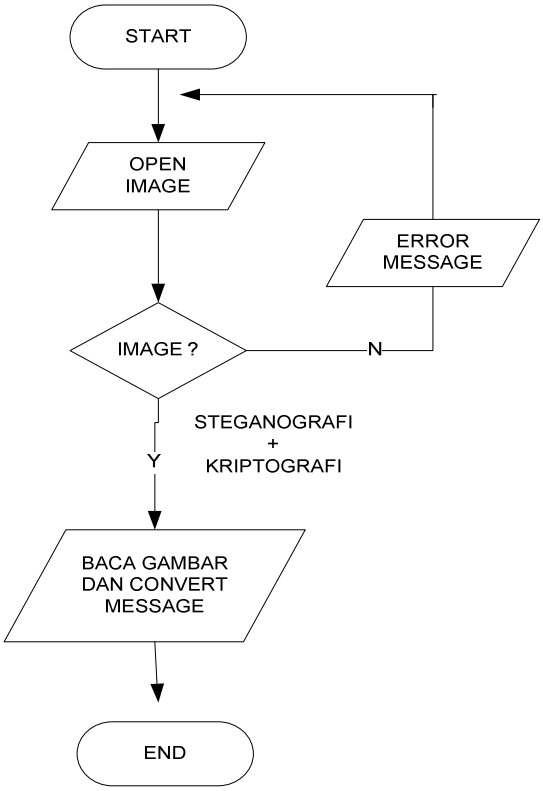
3. ALGORITMA

Setelah tahapan pola pikir dan alur dari konsep sudah didapat maka di sini akan di perlihatkan algoritma dari aplikasi yang sesuai dengan rancangan di atas. Berikut adalah gambar flowchat saat proses penyisipan pesan.



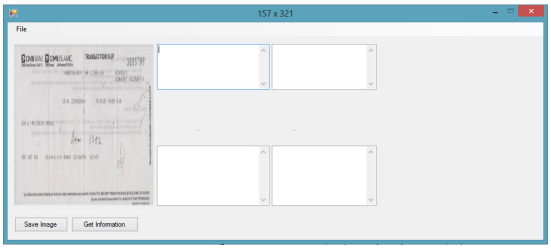
Gambar 3. Flowchart Embedding

Berikut adalah gambar flowchart untuk mengembalikan pesan teks yang disisipkan, sehingga menghasilkan pesan teks dari gambar.



Gambar 4. Flowchart Ekstraksi

3.1 HASIL PERCOBAAN



Gambar 5. Tampilan Program

3.2 ANALISA

Dari flowchart Gambar 3, dapat dijelaskan alur program yaitu program akan melakukan proses validasi terhadap image yang diupload. Syaratnya adalah file harus berupa gambar atau JPEG,TIF atau BMP. Jika pengguna ingin membuat file stegano menyisipkan pesan, maka cukup mengisikan pesan yang akan disisipkan pada text box yang disediakan dan system akan melakukan encrypt data. Tombol Save Image akan menyimpan hasil dari file yang sudah kita sisipkan pesan.

Dari flowchart Gambar 4, dapat dijelaskan alur program untuk membuka pesan atau teks yang disisipkan pada gambar yang sudah kita lakukan proses stegano. Prosesnya hampir sama dengan proses embedding, yaitu open Image gambar yang akan dibuka isi pesannya. Lalu klik tombol get information untuk convert message dan decrypt data.

4. KESIMPULAN

Dari hasil percobaan sistem yang telah dibuat maka dapat disimpulkan bahwa file yang mengalami proses embedding atau proses penyisipan pesan, file tidak mengalami banyak perubahan dengan kata lain gambar yang dihasilkan masih sama dengan file aslinya, hanya berbeda pada size atau ukurannya.
Dengan menggunakan teknik steganografi dan kriptografi memungkinkan untuk validasi keabsahan suatu dokumen transaksi yang dikirimkan cabang

DAFTAR ACUAN

Aditya Yogie, Pratama Andhika dan Nurlifa Alfian. *"Studi Pustaka Untuk Steganografi Dengan Beberapa Metode"*. Fakultas Teknologi Industri. Universitas Islam Indonesia. 2010.

David, Murtado A. dan Kasma Utin. *"Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online"*. Program Studi Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer Pontianak. 2012

Sasongko, Jati. "*Pengamanan Data Informasi menggunakan Kriptografi Klasik*". Fakultas Teknologi Informasi. Universitas Stikubank Semarang. 2005.

Utami Ema. *"Pendekatan Metode Least BIT Modification Untuk Merancang Aplikasi Steganography Pada File Audio Digital Tidak Terkompresi"*. STMIK AMIKOM Yogyakarta. 2009

Westfeld Andreas. "*Steganalysis in the Presence of Weak Cryptography and Encoding*". Technische Universit¨at Dresden Institute for System Architecture, Germany. 2006.