JURNAL TEKNIK

TEKNIK INFORMATIKA - TEKNIK MESIN - TEKNIK SIPIL - TEKNIK ELEKTRO - TEKNIK INDUSTRI

Diterbitkan Oleh:
Fakultas Teknik Universitas Muhammadiyah Tangerang
Jl. Perintis Kemerdekaan I No. 33, Cikokol Tangerang - Tlp. 021 - 51374916

Jurnal Teknik	Vol.	No.	Hlm.	FT. UMT	ISSN
	5	2	1-114	Desember 2016	2302-8734

JURNAL TEKNIK

Teknik Informatika ~ Teknik Mesin ~ Teknik Sipil
Teknik Elektro ~ Teknik Industri

FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH TANGERANG

JURNAL TEKNIK
Diterbitkan Oleh:
Fakultas Teknik Universitas Muhammadiyah Tangerang

Alamat Redaksi:
Jl. Perintis Kemerdekaan I No. 33, Cikokol Tangerang
Tlp. (021) 51374916

	Vol.	No.	Hlm.	UMT	ISSN
Jurnal Teknik	5	2	1-114	Desember 2016	2302-8734

DAFTAR ISI

Sambutan Dekan
Fakultas Teknik
Universitas Muhammadiyah Tangerang

Puji Syukur kehadirat Allah Swt. karena berkat karunia dan ijin-Nyalah Tim penyusun Jurnal Teknik Fakultas Teknik Universitas Muhammadiyah Tangerang dapat menyelesaikan tugasnya tepat sesuai dengan waktu ditetapkan.

Saya menyambut baik diterbitkannya Jurnal Teknik Vol. 5 No. 2, Desember 2016, terbitnya jurnal ini, merupakan respon atas terbitnya Peraturan Menteri Pendidikan Nasional No. 17 Tahun 2010 tentang Pencegahan dan Penanggulangan Plagiat di Perguruan Tinggi; Surat Dirjen Dikti Nomor 2050/E/T/2011 tentang kebijakan unggah karya ilmiah dan jurnal; Surat Edaran Dirjen Dikti Nomor 152/E/T/2012 tertanggal 27 Januari 2012 perihal publikasi karya ilmiah yang antara lain menyebutkan untuk lulusan program sarjana terhitung mulai kelulusan setelah 2012 harus menghasilkan makalah yang terbit pada jurnal ilmiah.

Terbitnya Jurnal ini juga diharapkan dapat mendukung komitmen dalam menunjang peningkatan kemampuan para dosen dan mahasiswa dalam menyusun karya ilmiah yang dilandasi oleh kejujuran dan etika akademik. Perhatian sangat tinggi yang telah diberikan rektor Universitas Muhammadiyah Tangerang khususnya mengenai *plagiarism* dan cara menghindarinya, diharapkan mampu memacu semangat dan motivasi para pengelola jurnal, para dosen dan mahasiswa dalam menyusun karya ilmiah yang semakin berkualitas.

Saya mengucapkan banyak terimakasih kepada para penulis, para pembahas yang memungkinkan jurnal ini dapat diterbitkan, dengan harapan dapat dimanfaatkan seoptimal mungkin dalam peningkatan kualitas karya ilmiah.

Dekan Fakultas Teknik
Universitas Muhammadiyah Tangerang,

Ir. Saiful Haq, M.Si.

Pengantar Redaksi
Jurnal Teknik
Universitas Muhammadiyah Tangerang

Puji dan Syukur Alhamdulillah kami panjatkan kehadapan Allah Swt. atas karunia dan lindungan-Nya sehingga Jurnal Teknik Vol. 5 No. 2 BulanDesember 2016 dapat diterbitkan.

Menghasilkan karya ilmiah merupakan sebuah tuntutan perguruan tinggi di seluruh dunia. Tri Dharma Perguruan Tinggi yaitu darma pendidikan, darma penelitian, dan darma pengabdian kepada masyarakat mendorong lahirnya dinamika intelektual diantaranya menghasilkan karya-karya ilmiah. Penerbitan Jurnal Teknik ini dimaksudkan sebagai media dokumentasi dan informasi ilmiah yang sekiranya dapat membantu para dosen, staf dan mahasiswa dalam menginformasikan atau mempublikasikan hasil penelitian, opini, tulisan dan kajian ilmiah lainnya kepada berbagai komunitas ilmiah.

Buku Jurnal yang sedang Anda pegang ini menerbitkan 13 artikel yang mencakup bidang teknik sebagaimana yang tertulis dalam daftar isi dan terdokumentasi nama dan judul-judul artikel dalam kulit cover Jurnal Teknik Vol. 5 No. 2 Bulan Desember 2016 dengan jumlah halaman 1-114 halaman.

Jurnal Teknik ini tentu masih banyak kekurangan dan masih jauh dari harapan, namun demikian tim redaksi berusaha untuk ke depannya menjadi lebih baik dengan dukungan kontribusi dari semua pihak. Harapan Jurnal Teknik akan berkembang menjadi media komunikasi intelektual yang berkualitas, aktual dan faktual sesuai dengan dinamika di lingkungan Universitas Muhammadiyah Tangerang.

Tak lupa pada kesempatan ini kami mengundang pembaca untuk mengirimkan naskah ringkasan penelitiannya ke redaksi kami. Kami sangat berterimakasih kepada semua pihak yang telah membantu penerbitan Jurnal Teknik ini semoga buku yang sedang Anda baca ini dapat bermanfaat.

Pimpinan Redaksi Jurnal Teknik
Universitas Muhammadiyah Tangerang,

Drs. Ir. Sumardi Sadi, MT.

PENGEMBANGAN PURWARUPA SISTEM PROTEKSI *HYBRID* KEASLIAN FAKTUR ELEKTRONIK (*E-INVOICE*) PADA E-BISNIS MENGGUNAKAN *QR CODE*, STEGANOGRAFI DAN KRIPTOGRAFI

Dedy Alamsyah
Program Studi Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Tangerang
Jl. Perintis Kemerdekaan I/33, Cikokol, Kota Tangerang
e-mail: *wafasa@gmail.com*

ABSTRAK

Faktur elektronik merupakan transformasi bentuk faktur konvensional berbasis kertas *(hardcopy)* menjadi faktur berbentuk digital (*e-invoice*) yang diterbitkan ketika terjadi transaksi bisnis. Faktur elektronik (*e-invoice*) berisi informasi-informasi yang berkaitan dengan transaksi bisnis antara penjual dan pelanggan. Faktur elektronik didistribusikan melalui *email* dan harus dapat dipastikan diterima pelanggan dan mampu diverifikasi keasliannya apabila terindikasi terjadi perubahan data dan informasi oleh pihak yang tidak berkepentingan. Pada penelitian ini sistem proteksi yang digunakan untuk melakukan proteksi terhadap faktur elektronik berbasis *Portable Document Forma*t (PDF) adalah metode *hybrid* yaitu penggabungan *QR-Code*, Steganografi dan Kriptografi sehingga faktur elektronik berbasis *Portable Document Format* yang dikirim ke pelanggan menjadi lebih aman. Sistem aplikasi yang dibuat berbasis web dan online lewat internet memungkinkan pelanggan melakukan verifikasi sehingga memberikan kepercayaan antara kedua belah pihak.

***Kata Kunci**: PDF protection, Hybrid Protection, Protection E-invoices, Steganography EOF, AES Encryption, Secure QR Code.*

I. PENDAHULUAN

Invoice atau faktur dalam transaksi bisnis sangat berperan penting dimana fungsinya adalah untuk komunikasi antara pihak pembeli dengan penjual dan digunakan sebagai pernyataan tagihan yang harus dibayar oleh pembeli [1] yang di dalamnya tercantum data-data penjualan seperti nomor faktur, nama perusahaan, alamat, nomor kontak, nama barang, jumlah barang, harga barang, pajak dan informasi lainnya [2] yang berkaitan dengan transaksi bisnis yang dilakukan. Faktur penjualan yang umumnya berbentuk kertas *(hardcopy)* dan didistri-busikan secara manual melalui pos atau kurir perlahan-lahan mulai berganti dengan faktur berbentuk elektronik (*e-invoice*). Perubahan dari faktur yang berbasis *hardcopy* ke bentuk digital (elektronik) ini bukan tanpa alasan karena banyak keuntungan yang dapat diambil dari faktur berbasis elektronik ini seperti: lebih cepat, lebih murah, lebih dapat diandalkan, dan memangkas pemborosan penggunaan kertas dalam prosesnya. [3]

Dalam buku *Information Security Mana-gement Handbook* dipaparkan bahwa terdapat 3 (tiga) aspek yang harus dipenuhi dalam keamanan informasi yaitu aspek kerahasiaan *(confidentiality)*, keutuhan data *(integrity)*, dan ketersediaan *(availability)* atau yang dikenal dengan CIA *Triad*. Selain ketiga aspek tersebut, terdapat aspek tambahan yang harus dipenuhi yaitu otentikasi penyedia/ penerima informasi *(authentication)* serta nir penyangkalan *(non repudiation)*.[4]

Sejalan dengan konsep pemodelan ke-amanan sistem informasi di atas, faktur elektronik *(e-invoice)* haruslah memenuhi kriteria-kriteria yang disebutkan di atas terutama dalam hal *data integrity*, artinya faktur elektronik harus terjaga integritas datanya dari upaya perubahan yang dilakukan oleh pihak yang tidak berwenang, *authentication* artinya faktur elektronik harus dapat diverifikasi dan dipastikan keasliannya dan *non repudiation* dalam artian faktur elektronik harus dapat tersebut diper-tanggungjawabkan dan diakui keasliannya tanpa ada penyangkalan.

1.1. Identifikasi Masalah

1. Berdasarkan latar belakang masalah maka dapat diidentifikasi masalah sebagai

berikut: File format PDF (*Portable Document Format*) yang mudah untuk dimodifikasi.
2. Belum adanya sistem proteksi yang memadai terhadap *faktur* penjualan elektronik berbasis file PDF (*Portable Document Format*) yang digunakan di PT Alamkaca Prabawa Indonesia saat ini.

1.2. Rumusan Masalah

Berdasarkan identifikasi masalah dan batasan masalah diatas, maka permasalahan dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana melakukan pengamanan (proteksi) serta dapat mengetahui apabila ada perubahan data atau informasi (verifikasi) di faktur elektronik berbasis PDF (*Portable Document Format*)?
2. Bagaimana membangun purwarupa aplikasi sistem proteksi file format PDF (*Portable Document Format*) dengan *QR-Code*, Steganografi dan Kriptografi?

II. LANDASAN TEORI DAN KERANGKA PEMIKIRAN

2.1. Konsep Keamanan Informasi (Information Security)

Keamanan informasi berarti melindungi informasi dan sistem informasi dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi atau perusakan.[5]

Tujuan dari keamanan informasi adalah untuk melindungi aset dan juga untuk menjamin kelangsungan bisnis, meminimalkan kerusakan bisnis, dan memaksimalkan keuntungan atas investasi.[6]

Seperti yang didefinisikan oleh ISO 17799, keamanan informasi dicirikan sebagai pemeliharaan terhadap:

- Kerahasiaan: Memastikan informasi yang dapat diakses hanya untuk mereka yang berwenang untuk mendapatkan akses.
- Integritas: Menjaga keakuratan dan kelengkapan informasi dan pengolahan metode.
- Ketersediaan: Memastikan bahwa pengguna yang berwenang memiliki akses ke informasi dan aset yang terkait bila diperlukan.[6]

Gambar 1 Komponen keamanan informasi atau kualitas (*CIA Triad*).[5]

Pada tahun 2002, Donn Parker mengusulkan model alternatif untuk *CIA triad* klasik yang ia sebut enam unsur informasi. Unsur-unsur tersebut adalah kerahasiaan, kepemilikan, integritas, keaslian, ketersediaan, dan utilitas.[5]

Selanjutnya konsep CIA triad yang awalnya hanya tiga unsur berkembang menjadi 6 bagian unsur sebagai berikut:

1. *Confidentiality;*
2. *Integrity;*
3. *Availability;*
4. *Authenticity;*
5. *Non-Repudiation;*
6. *Risk Management.*

2.2. Faktur Elektronik (E-Invoice)

Faktur Penjualan (*Invoice*) adalah dokumen yang menunjukan jumlah yang berhak ditagih kepada pelanggan yang menunjukan informasi kuantitas, harga dan jumlah tagihan. [7]

Faktur elektronik dapat didefinisikan sebagai transfer secara elektronik informasi yang berkaitan dengan faktur, termasuk penagihan dan informasi pembayaran antara mitra bisnis. [8]

Faktur elektronik harus bisa dipastikan kredibilitas asal usulnya, integritas datanya dan juga mudah dibaca. Keaslian asal dokumen pajak dalam bentuk elektronik dan integritas isinya dapat dibuktikan oleh tanda tangan elektronik yang diakui atau pertukaran informasi elektronik. [9]

Sistem E-faktur biasanya tercakup tanda tangan digital yang mumpuni yang meningkatkan validasi dari faktur elektronik tersebut.[10] Faktur elektronik harus memenuhi persyaratan keamanan yang ketat untuk menjadi bagian dari praktek-praktek keuangan perusahaan. [11]

2.3. E-Bussiness (Electronic Bussiness)

E-business menggambarkan penggunaan alat-alat dan platforms elektronik untuk menjalankan bisnis perusahaan.[12] Menurut Judy Straus dan rekan *e-business* merupakan optimisasi aktivitas bisnis perusahaan terus menerus melalui teknologi digital. [13]

Sedang menurut Budi Sutedja, *e-business* merupakan suatu istilah yang digunakan untuk memberi nama kegiatan-kegiatan bisnis yang dilakukan melalui internet. [14]

Maka dapat disimpulkan bahwa *e-Bussiness* meliputi segala macam fungsi dan kegiatan bisnis menggunakan data elektronik, sehingga *e-Business* berkaitan secara menyeluruh dengan proses bisnis termasuk *value chain*; pembelian secara elektronik (*electronic purchasing*), manajemen rantai suplai (*supply chain management*), pemrosesan order elektronik, penanganan dan pelayanan kepada pelanggan, dan kerja sama dengan mitra bisnis.

Kegiatan *e-business* dapat dikelompokkan menjadi beberapa jenis berdasarkan perilaku bisnis yang saling berhubungan yaitu

1. *Business to Business* (B2B): merupakan hubungan bisnis antar perusahaan.
2. *Business to Customer* (B2C): merupakan hubungan bisnis antara perusahaan dengan konsumen.
3. *Customer to Customer* (C2C): merupakan hubungan bisnis antar perorangan konsumen.
4. *Customer to Business* (C2B): merupakan hubungan bisnis antara perorangan dengan perusahaan.
5. *Business to Government* (B2G): merupakan hubungan bisnis antara perusahaan dengan Pemerintah. [14]

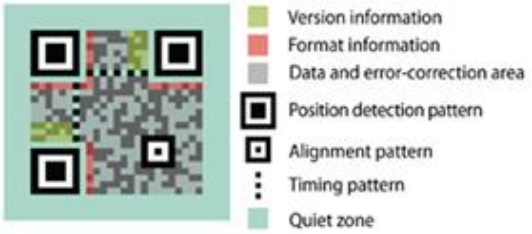
2.4. QR Code (Quick Response Code)

QR Code adalah simbol dua dimensi yang dikembangkan oleh *Denso Wave* 1994 dengan tujuan utama sebagai simbol yang dapat dengan mudah diinterpretasikan oleh alat *scanner*. [15]

QR Code adalah merek dagang terdaftar dari perusahaan Jepang *Denso Wave*, anak perusahaan dari Toyota, yang menemukan teknologi tersebut pada tahun 1994 untuk melacak bagian dalam perakitan kendaraan.

Gambar 2. *QR Code* dan *Barcode* [15]

Struktur QR Code yang terdiri dari *finder patterns*, alignment patterns, timing patterns, dan quiet zone ditunjukkan pada gambar di bawah



Gambar 3. Struktur *QR Code* [15]

a) Finder Pattern

Merupakan pola untuk mendeteksi posisi *QR Code*. Dengan mengatur pola ini pada tiga sudut simbol, posisi, ukuran, dan sudut dari simbol dapat dideteksi.

Finder pattern ini terdiri dari sebuah struktur yang dapat dideteksi dari semua arah (360 derajat).

b) Alignment Pattern

Merupakan pola untuk mengoreksi distorsi dari *QR Code*. Ini sangat efektif untuk mengkoreksi distorsi non linear. Koordinat pusat dari *alignment pattern* akan diidentifikasi untuk mengoreksi distorsi simbol. Untuk tujuan ini, sebuah sel hitam terisolasi ditempatkan di *alignment pattern* untuk membuatnya lebih mudah untuk mendeteksi koordinat pusat dari *alignment pattern*.

c) Timing Pattern

Merupakan pola untuk mengidentifikasi koordinat pusat untuk setiap sel di *QR Code* dengan pola hitam dan putih yang disusun berselang-seling. Ini digunakan untuk mengoreksi koordinat pusat dari sel data jika simbol terdistorsi atau jika ada *error* untuk setiap area sel. Pola ini disusun dengan arah vertikal dan horizontal.

d) Quiet Zone

Ruang margin diperlukan untuk *membaca QR Code*. *Quiet zone* membuat simbol lebih mudah untuk dideteksi diantara gambar-gambar yang dibaca oleh sensor CCD. Empat atau lebih sel dibutuhkan untuk *quiet zone*.

e) Data Area

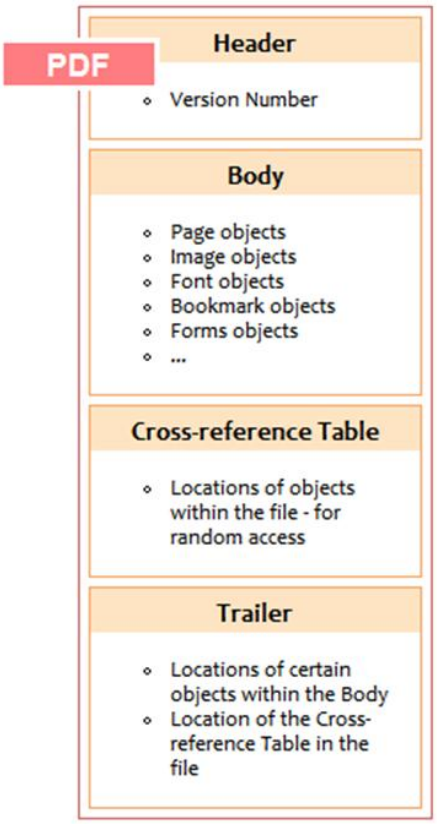
Data *QR Code* akan disimpan (dikodekan) ke area data. Bagian abu-abu pada gambar 2 mewakili area data. Data akan dikodekan ke bilangan biner 0 dan 1 berdasarkan aturan pengkodean. Bilangan biner 0 dan 1 akan dikonversikan ke sel hitam dan putih dan akan disusun. Area data akan memiliki kode *Reed-Solomon* yang digunakan untuk data yang tersimpan dan fungsionalitas pengkoreksian *error*.

2.5. Portable Document Format (PDF)

Format (PDF) adalah sebuah protokol dekripsi halaman *extensible* yang mengimplementasikan format file asli dari produk perangkat lunak komersial *Adobe Acrobat Suite*. Tujuan dari format tersebut adalah untuk memungkinkan pertukaran (*hardware independen)* dokumen resolusi tinggi, dokumen yang berisi teks, grafis, elemen multimedia, dan atau tipe data kustomisasi, plus (opsional) *link* ke file lain atau URL, atau item yang dikandungnya. Format ini mendukung pencarian berbasis teks, akses data *random*, *bookmark*, *link*, penjelasan, elemen halaman interaktif (kotak centang, bidang edit-teks, dan lain-lain), enkripsi, kompresi, aksi terhadap *javascript*, dan banyak lagi lainnya. [16]

Spesifikasi File PDF

Berikut adalah struktur file PDF dalam gambar:



Gambar 4: Spesifikasi file PDF perbagian[17]

Dari skema file PDF di atas dapat dipetakan menjadi beberapa bagian besar yang secara garis besar spesifikasi tersebut dari:

a. ***Header* (Bagian Kepala) PDF:** baris pertama dari PDF menentukan format file PDF. *Header* ini adalah bagian paling atas dari sebuah dokumen. Ini menunjukkan informasi dasar file PDF, misalnya, "PDF-1.4", itu berarti bahwa format PDF adalah versi keempat. Kesimpulannya, untuk membaca PDF, anda harus mendownload *Adobe Reader* atau *software* pembaca file PDF lainnya yang kompatibel untuk melihat file PDF tersebut.

b. **Bagian *Body* (Bagian Tubuh) PDF:** Tubuh file PDF terdiri dari benda-benda yang membentuk isi dokumen. Obyeknya bisa meliputi data gambar, *font*, penjelasan, *stream text* (teks) dan sebagainya. Pengguna juga dapat mengintegrasikan obyek yang tak terlihat atau elemen-elemen lainnnya. Obyek-obyek ini dapat ditanamkan fitur-fitur interaktif dalam dokumen seperti animasi atau grafis. Seorang pengguna juga dapat mengimplementasikan struktur logis dalam do-

kumen. Anda juga dapat membuat isi dari dokumen PDF lebih aman dengan menerapkan fitur keamanan, seperti melindungi isi dokumen dari pencetakan yang tidak sah, melihat atau mengedit atau memodifikasi. Bagian tubuh (*body)* file PDF juga mendukung dua jenis angka yaitu bilangan bulat dan bilangan *real*.

c. **Bagian Tabel *Cross-Referensi:*** biasa disebut *xref table*, yaitu tabel referensi silang terdiri dari link ke semua obyek atau lemen dalam file PDF tersebut. Kita dapat menyebarkan fitur ini untuk menavigasi ke halaman lain atau konten dalam dokumen. Ketika pengguna meng-*update* file PDF mereka, mereka akan otomatis mendapatkan update pada tabel referensi silang tersebut. Juga bisa melacak perubahan yang diperbarui pada table referensi silang tersebut.

d. **Bagian *Trailer:*** Trailer berisi *link* ke tabel referensi silang dan selalu berakhir dengan "EOF" untuk mengidentifikasi akhir dari file PDF. Bagian " EOF" sangat diperlukan pada file PDf, jika baris ini hilang, PDF tidak lengkap dan tidak dapat diproses dengan benar. Ini tidak sama dengan *PostScript.* Jika beberapa baris terakhir dari file *PostScript* hilang kita masih bisa mencetaknya. Jika pada file PDF hal ini tidak bisa.[18]

2.6. Steganografi

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian rupa sehingga keberadaan (eksistensi) pesan tidak terdeteksi oleh indera manusia. Kata "*steganografi*" berasal dari bahasa Yunani "*steganos*", yang artinya "tersembunyi atau terselubung", dan "*graphein*", "menulis".[19]

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 diantaranya:

1. Format *image: bitmap* (bmp), gif, pcx, jpeg, dll.
2. Format audio: wav, voc, mp3, dll.
3. Format lain: teks file, html, pdf, dll.[20]

Ada beberapa hal yang diperlukan untuk menyembunyikan pesan yaitu:

1. Algoritma Penyisipan (*Embeding Algorithm*).

Algoritma ini digunakan untuk menyisipkan suatu pesan yang disembunyikan ke dalam suatu data yang akan dikirim. Proses penyisipan ini diproteksi oleh sebuah *keyword* sehingga hanya orang-orang yang mengetahui *keyword* ini yang dapat membaca pesan yang disembunyikan tersebut.

2. Fungsi Detektor (*Detector Function*).

Fungsi Detektor ini adalah untuk mengembalikan pesan-pesan yang disembunyikan tersebut.

3. *Carrier Document*.

Merupakan dokumen yang berfungsi sebagai media yang digunakan untuk menyisipkan informasi. Dokumen ini dapat berupa file-file seperti file audio,video atau citra (gambar).

4. Key

Merupakan kata kunci yang ikut disisipkan kedalam dokumen berguna dan dipakai sebagai proses verifikasi sewaktu informasi akan ditampilkan atau diuraikan.

5. Secret Message/ Plaintext

Merupakan pesan rahasia yang akan disisipkan kedalam *carrier* document. Pesan inilah yang tidak ingin terlihat dan terbaca oleh orang yang tidak berkepentingan.[21]

2.7. Kriptografi

Kriptografi merupakan sebuah seni perlindungan keamanan pesan rahasia dengan mengacaukan dan menyandikan pesan rahasia menjadi kode-kode rahasia atau *chiphertext.* [22]

Dengan menggunakan kriptografi orang lain dapat menyadari keberadaan pesan rahasia tersebut, tetapi hanya orang yang memiliki kunci yang dapat membacanya.[23] Kriptografi digunakan untuk menjaga kerahasiaan pesan yang dikirim dengan menggunakan media tertentu sehingga pesan tidak dapat dibaca oleh orang yang tidak berhak.

Tujuan utama penggunaan teknik kriptografi dalam pengiriman pesan rahasia teragi menjadi beberapa poin-poin penting, yaitu. [24]

1) *Confidentialy* (Kerahasiaan).
2) *Authentication* (Keaslian).
3) *Data integrity* (Integritas data).
4) *Non-Repudiation* (Anti Penyangkalan).
5) *Acces Control* (Kendali Akses).

Berdasarkan kunci yang digunakan algoritma kriptografi terbagi menjadi 2 golongan yaitu Algoritma Simetris dan Algoritma Asimetris. [25]

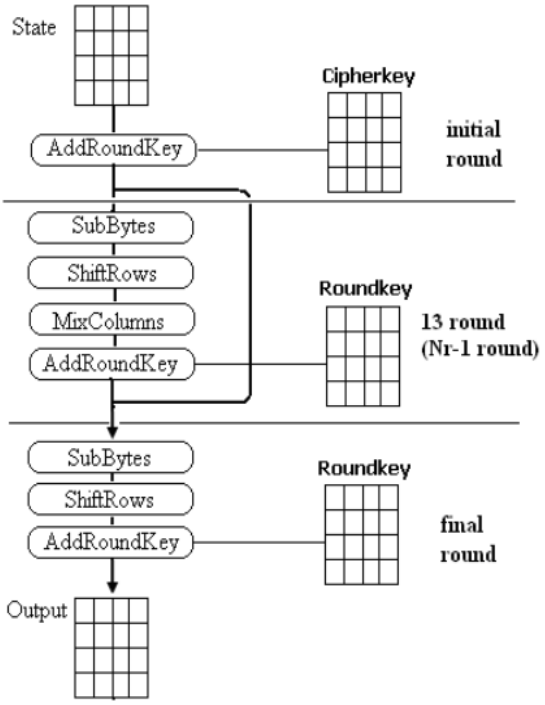
2.8. Advance Encryption Standard (AES)

Pada tahun 2001, Algoritma *Rijndael*, karya peneliti dari universitas di Belgia yaitu Joan Daemen dan Vincent Rijmen ditetapkan menjadi *Advanced Encryption Standard* (AES). Rijndael merupakan algoritma yang dapat menerima masukan data 128 bit dan menghasilkan data 128 bit pula. [26]

Tabel 1 Perbandingan Jumlah *Round* dan *Key* [27]

JENIS	Jumlah *Key* (Nk)	Ukuran *Block* (Nb)	Jumlah Putaran (Nr)
AES 128	4	4	10
AES 192	6	4	12
AES 256	8	4	14

Berikut ilustrasi proses enkripsi AES dapat digambarkan seperti ini:



Gambar 5. Diagram Proses Enkripsi AES [28]

2.9. ISO 9126

ISO 9126 adalah standar internasional yang diterbitkan oleh ISO (*International Standart for Organization*) untuk mengevaluasi kualitas perangkat lunak dan merupakan pengembangan dari ISO 9001. Standar ini dibagi menjadi empat bagian yang masing-masing menjelaskan model kualitas, metrik *eksternal*, metrik *internal*, dan metrik kualitas yang digunakan. Ada enam ukuran kualitas yang ditetapkan oleh ISO 9126 yaitu fungsionalitas, kehandalan (*realibility*), kebergunaan (*usability*), efisiensi, portabilitas, serta keterpeliharaan (*maintainability*).[29]

Setiap standar internasional yang diterbitkan oleh ISO, memiliki karakteristik yang berbeda-beda. Di dalam ISO 9126-1 *Software quality model* juga memiliki karakteristik tersendiri. Terdapat 6 karakteristik utama untuk ISO 9126-1, yaitu:

1. Functionality

Kemampuan untuk memenuhi fungsi produk perangkat lunak yang menyediakan kepuasan kebutuhan user.

2. Reliability

Kemampuan perangkat lunak untuk perawatan dengan level performansi.

3. Usability

Kemampuan yang berhubungan dengan penggunaan perangkat lunak.

4. Efficiency

Kemampuan yang berhubungan dengan sumber daya fisik yang digunakan ketika perangkat lunak dijalankan.

5. *Maintainability*

Kemampuan yang dibutuhkan untuk membuat perubahan perangkat lunak.

6. *Portability*

Kemampuan yang berhubungan dengan kemampuan perangkat lunak yang dikirim ke lingkungan berbeda.[29]

Tabel 2. Karakteristik Kualitas Perangkat Lunak ISO 9126

Karakteristik	Sub Karakteristik
Functionality	suitability, accuracy, interoperability, security
Reliability	maturity, fault tolerance, recoverability
Usability	understandability, learnability, operability, attractiveness
Efficiency	time behavior, resource utilization
Maintainability	analyzability, changeability, stability
Portability	daptability, installability, co-existence, replacability

2.10. Sistem, Sistem Proteksi dan Sistem Proteksi Hybrid

Sebuah sistem adalah seperangkat elemen atau komponen yang berinteraksi untuk mencapai tujuan. Masing-masing elemen dan hubungan di antara mereka menentukan bagaimana sistem bekerja. Sistem memiliki input, mekanisme pengolahan, *output*, dan umpan balik. [30]

Sistem adalah berbagai komponen yang bekerja sama untuk mencapai tujuan bersama, atau beberapa tujuan, dengan menerima masukan, pengolahan, dan menghasilkan output secara terorganisir. Sebagai contoh sebuah *sound system* terdiri dari banyak komponen elektronik dan mekanik, seperti kepala laser optik, *amplifier*, *equalizer*, dan sebagainya. Sistem ini menggunakan input berupa tenaga listrik dan suara direkam pada media seperti CD atau DVD, dan memproses masukan untuk mereproduksi musik dan suara lainnya. Kesemua komponen tersebut bekerja sama untuk mencapai tujuan ini. [31]

Sedangkan proteksi *(protection)* adalah Tindakan melindungi seseorang atau sesuatu, atau keadaan dilindungi. [32]

Dari definisi-definisi di atas dapat disimpulkan bahwa Sistem Proteksi adalah separangkat elemen atau komponen yang saling berinteraksi dimana tujuannya adalah untuk melindungi sesuatu yang dalam hal ini obyek inputnya yaitu faktur elektronik *(e-invoice)* dan outputnya adalah faktur elektronik *(e-invoice)* yang sudah dilindungi keasliannya dengan metode atau teknik tertentu.

Kesimpulan dari sistem proteksi *hybrid* adalah sebuah metode proteksi dengan menggunakan gabungan dari beberapa teknik yaitu *QR Code*, Steganografi dengan Kriptografi untuk melakukan pengamanan akan keaslian dokumen faktur penjualan berbasis file *Portable Document Format* (PDF) sehingga file faktur tersebut dapat diverifikasi keasliannya.

2.11. Tinjauan Studi

Tinjauan studi yang dijadikan acuan dalam melakukan penelitian tesis ini mengacu pada beberapa penelitian yang terkait dilakukan sebelumnya yaitu sebagai berikut:

1. Teknik Steganografi Pada File PDF

a. *Diantara kata atau diantara karakter yang diembed.*

Penelitiaan dari I-Shi Lee dan W-H. Tsai yang mengetengahkan dua algoritma dalam memanfaatkan *non-breaking space* yang merupakan Standar Amerika untuk Kode pertukaran informasi (*Information Interchange*) (ASCII) yaitu kode A0.Teknik pertama yaitu meng*embed* data dengan mengubah ruang kosong (*white space*) menjadi A0 untuk mengkodekan 1, dan membiarkan *white space* biasa untuk mengkodekan 0. Teknik tidak meningkatkan ukuran file sama sekali, tetapi jumlah data yang dapat disisipkan sangat terbatas sekali dengan jumlah *white space* yang ada di dalam teks. Teknik kedua mengambil keuntungan dari karakter A0: dengan mengubah lebarnya menjadi nol tampak sama sekali tidak terlihat, sehingga Anda dapat memasukkan jumlah antara dua karakter tanpa mengubah tampilan teks. Data disisipkan dengan memasukkan sejumlah ruang (*space*) *zero-length* di setiap lokasi antara karakter; jumlah ruang mengkodekan karakter ASCII. Efeknya Teknik ini tidak meningkatkan ukuran file, namun jumlah data yang dapat disisipkan jauh lebih banyak. dengan meng*encode* pesan rahasia dengan ASCII *code* dan menyisipkannya antaran kata dan karatker di sebuah *text* pada PDF *file*, menjadi tidak terlihat dengan menggunakan pembaca PDF biasa. Membuat effek steganografi untuk transmisi rahasia pada PDF *file* [33]

b. *Update Inkremental*

Penelitian H. Liu et al. yang mengetengahkan tiga algoritma, yaitu memanfaatkan fitur *update* inkremental dari file PDF.Teknik pertama mengembed data dengan mengubah teks dengan cara yang terlihat (mengubah nilai beberapa variabel state teks), kemudian menulis *update* inkremental berisi data PDF asli, sehingga teks yang diubah tidak benar-benar ditampilkan. Teknik kedua yaitu dengan meng-*embed* data dengan menulis update inkremental untuk obyek yang tidak ada dalam data asli, sehingga *update* tidak berpengaruh. Data tertanam dalam nilai *object stream* yang digunakan pada *update*. Teknik ketiga yaitu meng-*embed* data dengan menulis update inkremental dengan panjang yang diberikan untuk beberapa obyek; maka selanjutnya data dapat diambil dengan membaca bagian *cross-reffence* (referensi silang) dari update, dan juga termasuk alamat awal setiap obyek yang diperbarui.[34]

c. *Justified-text dan TJ Operator*

S. Zhong et al. menyajikan teknik untuk membuat dan mengeksploitasi celah rahasia dengan membuat penggunaan *Justified-Text*. Mereka menyatakan bahwa *Justified-Text* (sehingga sejajar dengan margin kiri dan margin kanan) menggunakan alikasi pembuat PDF akan menghasilkan nilai acak untuk *operator* TJ yang digunakan untuk memposisikan huruf (*characters*). Sangat dimungkinkan untuk menyembunyikan data dalam bit paling signifikan (*least significant bit*) dari beberapa nilai *operator* TJ ini.Namun ini hanya bekerja jika nilai-nilai o*perator* TJ adalah acak dan tidak mengandung pola apapun. [35]

Dalam tulisan ini, S. Zhong et al. menyajikan-teknik steganografi baru untuk menyembunyikan data dalam bentuk teks PDF. Kami pertama kali menunjukkan saluran rahasia dalam semacam teks PDF berbahasa inggris, yang dihasilkan dari dokumen yang membuat perataan teks untuk menempati secara penuh lebar kolom dan posisi masing-masing karakter pada lebar halaman. Berturut-turut, di gambarkan sistem steganografi *PDFStego* di mana beberapa strategi diterapkan untuk meningkatkan ke-amanan, seperti memanfaatkan duplikasi un-tuk melengkapi keamanan; merupakan dua *chaotic-maps* untuk memenuhi prinsip *Kerckhoffs* dan mencegah serangan statistik, dan menerapkan algoritma *hash* yang aman untuk mengaktifkan layanan terintegrasi dan layanan yang melakukan ekstraksi secara membabi buta. Selain itu, kita mendefinisikan kapasitas *embed* dari sistem. PDFStego dapat digunakan untuk bertukar data yang sensitif secara aman atau untuk menambahkan informasi hak cipta ke file PDF.

d. *Metode Operator TJ*

Salah satu metode saat ini dan paling menjanjikan menggunakan nilai-nilai *operator* TJ, yang digunakan untuk menampilkan teks dalam file PDF untuk menyembunyikan data. Tujuan dari proyek penelitian adalah untuk meningkatkan kapasitas dan, jika mungkin, juga faktor keamanan dari metode ini.Dan karenanya secara hati-hati metode *operator* TJ dianalisis untuk mencari kelemahan. dalam proses untuk melakukan hal ini, pelaksanaan metode ini dikembangkan. Analisis statistik dari nilai-nilai *operator* TJ menunjukkan bahwa metode *operator* TJ sangat begitu kuat dan data yang disembunyikan dapat dengan mudah dideteksi. Berdasarkan hasil dari banyak percobaan yang telah dilakukan, dua algoritma yang berbeda disusun. Yang pertama memiliki kapasitas lebih rendah tapi lebih aman. Dan yang kedua kapasitas *embed* datanya jauh lebih banyak sementara masih menyimpan tingkat keamanan yang sama. Kedua algoritma diusulkan sebagai alternatif untuk metode *operator* TJ yang asli.[36]

2. Keamanan Informasi dan Dokumen

a. Penelitian yang dilakukan oleh Ary Budi Warsito, Lusi Fajarita, Nazori AZ yang berjudul Proteksi Keamanan Dokumen Sertifikat File JPEG Pada Perguruan Tinggi Dengan Menggunakan Steganografi Dan Kriptografi. Mereka melakukan proteksi dengan menggunakan teknik steganografi dan enkripsi (namun tidak dijelaskan teknik steganografi model seperti apa dan jenis algoritma apa yang digunakan) terhadap file terbitan akademik yang berbentuk JPEG agar keabsahan suatu sertifikat pada perguruan tinggi yang diterbitkan secara online tetap terjaga.[20]

b. Penelitian yang dilakukan Ana Wahyuni dengan judul Aplikasi Kriptografi Untuk Pengamanan E-Dokumen Dengan Metode Hybrid: Biometrik Tandatangan Dan

DSA (*Digital Signature Algorithm*). Dalam penelitian ini metode yang digunakan adalah Kriptografi metode *Hybrid* yaitu Tanda Tangan Digital dan *Bio Metric algorithm* DSA (*Digital Signature Algorithm*) yang bertujuan untuk melakukan proteksi terhadap *e-document* yang ditransmisikan via *email* dan dapat diverifikasi keabsahannya oleh sipenerima.[37]

c. Penelitian yang dilakukan oleh Eko Ari Wibowo yang berjudul Aplikasi Pengamanan Dokumen Office dengan Algoritma Kriptografi Kunci Simetris El-Gamal teknik proteksi yang digunakan adalah Kriptografi dengan Enkripsi Simetris algoritma ElGamal yang bertujuan melakukan proteksi terhadap dokumen dalam format *Microsoft Office*.[38]

d. Penelitian yang dilakukan oleh Ari Muzakir dengan judul Pemanfaatan dan Implementasi *Library* XMLSEC Untuk Keamanan Data Pada XML *Encryption* dimana proteksi yang digunakan adalah algoritma Kriptografi RSA dengan panjang kunci 1024 bit yang tujuannya adalah untuk melakukan proteksi file XML dalam komunikasi *Web Service*.[39]

e. Penelitian yang dilakukan oleh Supriyono dengan judul Pengujian Sistem Enkripsi-Dekripsi Dengan Metode RSA Untuk Pengamanan Dokumen. Teknik proteksi yang digunakan adalah Kritografi dengan metode RSA yang bertujuan adalah untuk melakukan proteksi dokumen dari akses oleh sembarang orang.[40]

Penelitian kali ini yang berjudul Pengembangan Purwarupa Sistem Proteksi *Hybrid* Keaslian Faktur Elektronik (*E-Invoice*) Pada E-Bisnis Menggunakan *QR Code*, Steganografi Dan Kriptografi. Pendekatan metode yang diusulkan penulis adalah metode penggabungan atau *hybrid* yaitu dengan menggabungkan proteksi dan sekaligus proteksi berbasis *QR Code* dan Steganografi dengan menyisipkan teks atau *plaintext* yang sudah ditentukan yang merupakan data rahasia yang sebelumnya sudah dienkripsi dengan teknik kriptografi menggunakan algoritma *Advanced Encryption Standard* (AES) *Rijndael* sehingga menjadi *chipertext* yang kemudian disisipkan ke *QR Code* yang berfungsi sebagai kombinasi dari *url* alamat sistem dan kode tertentu untuk verifikasi. Di isi lainnya yaitu teknik steganografi setelah tag %%EOF pada struktur *source* file PDF. *Chipertext* yang disisipkan ke dalam *QR Code* dan juga ke dalam struktur file PDF menjadi sebuah penanda untuk melakukan verifikasi ketika terjadi perubahan atau *editing* terhadap data atau informasi terhadap file PDF. Metode penyisipan di akhir tag %%OEF pada source file PDF terinspirasi dari penelitian Aniello Castiglionea, Alfredo De Santisa, Claudio Soriente tentang *Security and privacy issues in the Portable Document Format* memaparkan bahwa ketika file PDF dibuat, tabel *xref* (referensi silang) hanya memiliki satu bagian dan setiap kali file diperbarui ada bagian-bagian baru ditambahkan. Setiap bagian berisi satu entri per obyek, untuk sejumlah obyek yang bersebelahan atau berdampingan dan seterusnya. File PDF selalu dibaca dari akhir file dengan cara mencari offset relatif terhadap bagian terakhir dari tabel *cross-reference* (referensi silang), ini diperlukan untuk mengidentifikasi obyek yang merupakan versi terbaru dari file PDF. Setiap kali dokumen diperbarui maka akan otomatis menambahkan obyek baru (memodifikasi yang sudah ada), sebuah struktur *body* baru, table *cross-reference* (referensi silang) dan trailer ditambahkan ke file PDF konsep ini disebut *incremental update*. Kesimpulannya adalah setiap kali faktur penjualan elektronik berbasis PDF baru dibuat maka sejatinya hanya akan terdiri dari satu set xref, *body* dan satu tag %%EOF di akhir file, maka ketika file faktur PDF tersebut terjadi editing atau penambahan informasi otomatis akan menambahkan set table *xref*, struktur *body* baru dan tentu saja tag %%OEF dengan bantuan *chipertext* yang telah disisipkan maka secara otomatis perubahan akan terdeteksi.

2.12. Hipotesa

Berdasarkan kerangka konsep yang telah dikemukakan maka pernyataan penelitian ini dapat dirumuskan sebagai berikut:

1. Diduga pengamanan data dokumen faktur elektronik berbasis PDF (*Portable Document Format*) dengan *QR-Code*, Steganografi dengan teknik *End Of File* (EOF) dan Kriptografi dengan menggunakan enkripsi *Advanced Encryption Standard* (AES) *Rijndael* meningkatkan keamanan

Faktur Penjualan Elektronik Berbasi File PDF.

2. Diduga tingkat kualitas sistem purwarupa yang dihasilkan dengan mengadaptasi model ISO 9126 yaitu: *functionality*, *reability*, *usability*, dan *efficiency* adalah baik.

III. METODOLOGI DAN RANCANGAN PENELITIAN

3.1. MetodePenelitian

Penelitian ini menggunakan metode kualitatif dimana penelitian bertolak dari asumsi dasar terhadap kelemahan yang ada pada file PDF yang didukung oleh data yang ada serta teori-teori yang mendukung, kemudian dengan memanfaatkan teori dari penelitian yang ada maka diusulkan suatu pendekatan yang mampu melakukan proteksi dan juga verifikasi terhadap faktur elektronik berbasis PDF.

Adapun jenis penelitian termasuk penelitian terapan (*Applied Research*). Hasil penelitian dapat langsung diterapkan untuk memecahkan permasalahan yang dihadapi.[41] Hasil penelitian berupa purwarupa sistem yang berfungsi untuk melakukan proteksi dan verifikasi faktur elektronik berbasis PDF berbasis *web* di PT Alamkaca Prabawa Indonesia langsung dapat diterapkan untuk pemecahan permasalahan yang dihadapi.

3.2. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Observasi (Pengamatan)

Observasi adalah kegiatan pengamatan yang direncanakan, sistematis dan hasilnya dicatat serta diinterpretasikan dalam rangka memperoleh pemahaman tentang obyek yang diamati.[42] Pada penelitian ini observasi dilaksanakan dengan cara mencatat dan mengamati langsung secara *real-time* proses proteksi dan verifikasi pada faktur elektronik berbasis file *Portable Format Document* (PDF) dengan *QR Code* yang berisi kode tertentu, kemudian dengan teknik steganografi dengan cara menyisipkan kode rahasia berupa *text* yang diproteksi dengan teknik Kriptografi menggunakan enkripsi (*Advanced Encryptrd Standard*) AES Rijndael dan selanjutnya *text* yang sudah dienkripsi tersebut disisipkan dengan teknik Steganografi dengan metode *End Of File* (EOF) untuk mendapatkan faktur elektronik berbasis PDF (*stego-pdf*) untuk dilakukan analisis lebih lanjut.

2. Studi Pustaka

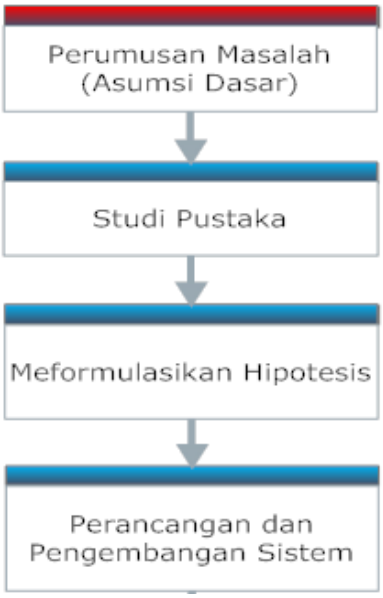
Merupakan metode pengumpulan data dengan cara mengumpulkan data-data dari berbagai sumber yang mendukung penelitian baik itu dari buku, jurnal ilmiah, paper nasional maupun internasional, makalah prosiding maupun artikel terkait lainnya yang bersumber dari internet. Hasil dari studi pustaka berupa asumsi, kesimpulan dari teori yang ada, teori dan perkembangan terkini mengenai teknik proteksi faktur elektronik (*e-invoice*) file berbasis *Portable Document Format* (PDF) dan teori yang terkait lainnya.

3. Wawancara

Wawancara dengan pihak-pihak yang berkaitan dengan penelitian. Teknik wawancara dilakukan dengan wawancara berstruktur.[42] Dalam hal ini adalah yang berkaitan dengan penelitian pengembangan sistem proteksi faktur elektronik berbasis *Portable Document Format* (PDF). Responden dalam wawancara ini adalah yang telah disebutkan pada pemilihan sampling sebelumnya. Pertanyaan-pertanyaan untuk mendapatkan data yang terkait dengan sistem faktur penjualan yang sedang berjalan saat ini, kebutuhan fungsional, non-fungsional, dan pengguna untuk sistem yang akan dikembangkan.

3.3. Langkah-langkah Penelitian

Berikut langkah-langkah penelitian yang dilakukan dalam penelitian ini sebagai berikut:



Gambar 6: Langkah-langkah Penelitian

1. *Perumusan Masalah*

Rumusan masalah yang diangkat dalam tesis ini adalah "Bagaimana menerapkan pengamanan (proteksi) untuk meningkatkan keamanan dan juga dapat mengetahui apabila ada perubahan data atau informasi (verifikasi keaslian) pada faktur elektronik berbasis PDF (*Portable Document Format*) dengan menggunakan teknik ganda *(hybrid)* menggunakan *QR Code*, teknik Steganografi metode *End of File* (EOF) dan teknik Kriptografi menggunakan enkripsi *Advanced Encryptrd Standard* (AES) *Rijndael*?".

2. *Studi Pustaka*

Studi pustaka dilakukan terhadap penelitian-penelitian yang sudah dilakukan yang terkait dengan masalah yang ingin diteliti khususnya yang berkaitan dengan spesifikasi jenis file *Portable Document Format* (PDF), teknik steganografi terhadap file PDF, kriptografi, algoritma *Advanced Encryption Standard* (AES), seluk beluk teknologi *QR Code* dan teori-teori pendukung lainnya.

3. *Meformulasikan Hipotesis*

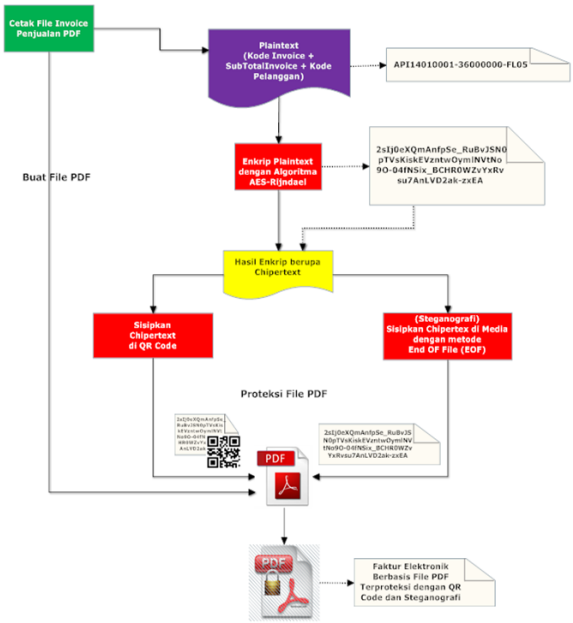
Hipotesis diformulasikan untuk penelitian tesis ini dari informasi-informasi yang terkait dengan masalah yang ingin dicari solusinya. Hipotesis merupakan prediksi dan kesimpulan sementara tentang hubungan keterkaitan antar variabel atau fenomena dalam penelitian.

4. *Perancangan dan Pengembangan Sistem*

Pendekatan desain dan analisis berorientasi obyek atau *Object Oriented Analysis and Design* (OOAD) pada tahap perancangan dalam aplikasi ini menggunakan notasi *Unified Modeling Language* (UML).

Perancangan sistem secara umum untuk pembangunan purwarupa aplikasi proteksi faktur elektronik terdiri dari beberapa tahap, antara lain meliputi perancangan:

a) Proteksi File PDF

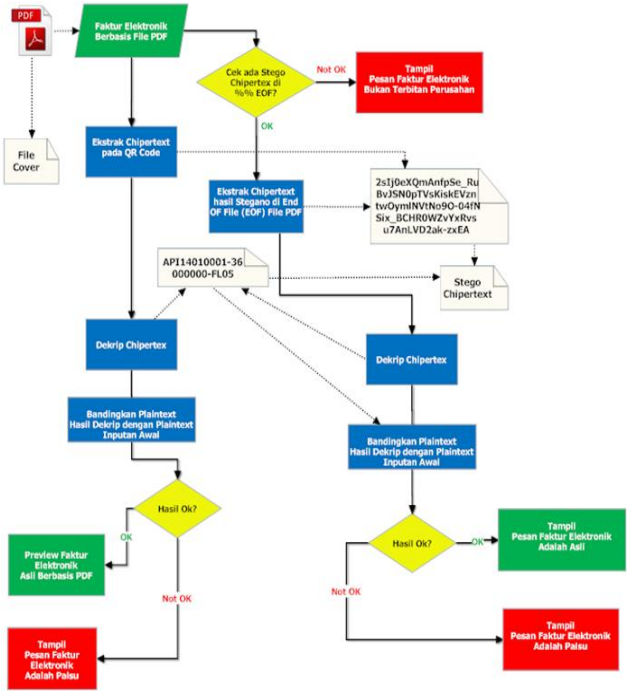


Gambar 7 Alur Sistem Proteksi Faktur Elektronik Berbasis PDF

Penjelasan gambar di atas adalah sebagai berikut:

1. Proses cetak Faktur Penjualan Elektronik berbasis PDF di dalamnya terdapat sub proses yaitu mencetak faktur ke file PDF dan melakukan proses proteksi menggunakan *QR Code* dan Steganografi.
2. Kode (*plaintext*) dienkrip dengan menggunakan algoritma *Advanced Encryption Standard (AES) Rijndael* menghasilkan kode yang sudah terenkripsi (*Chipertext*).
3. Selanjutnya *Chipertext* distegano dengan menggunakan metode *End Of File (EOF)* pada file PDF.
4. Dilain sisi yang lain *Chipertext* juga di sisipkan ke dalam *QR Code*.
5. Maka setelah proses di atas dilakukan maka terbentuklah sebuah proteksi *hybrid* terhadap file PDF (Faktur Penjualan Elektronik berbasis file PDF).

b) Verifikasi File PDF



Gambar 8 Alur Sistem Verifikasi Keaslian Faktur Elektronik Berbasis PDF.

Penjelasan gambar di atas adalah sebagai berikut:

a) Steganografi

1. Melakukan pengecekan apakah ada atau tidak kode (*chipertex*) pada tag %%EOF (End Of File) pada file Faktur berbentuk PDF. Kalau OK maka akan dilanjutkan ke proses selanjutnya namun kalau hasilnya NOT OK maka akan ditampilkan pesan bahwa File yang di cek adalah bukan file Faktur Elektronik Penjualan terbitan dari PT. Alamkaca Prabawa Indonesia.
2. Setelah itu lakukan ekstrak *chipertext* yang disteganografi
3. *Chipertext* yang sudah diekstrak kemudian didekrip untuk menghasilkan *plaintext*.
4. *Plaintext* hasil dekrip kemudian dibandingkan dengan *plaintext* (*stego text*) awal.
5. Kalau hasilnya OK maka akan ditampilkan pesan bahwa file Faktur Elektronik Penjualan berbasis PDF adalah ASLI oleh sistem. Namun apabila hasilnya TIDAK OK maka akan tampil pesan file Faktur Elektronik Penjualan berbasis PDF adalah Tidak Asli.

b) QR Code

1. Baca data (*chipertex*) dari QR Code yang ada pada file Faktur berbentuk PDF yang sudah diproteksi dari pelanggan.
2. Setelah itu lakukan ekstrak *chipertext* yang disteganografi
3. *Chipertext* yang sudah diekstrak kemudian didekrip untuk menghasilkan *plaintext*.
4. Setelah itu akan dilakukan pengecekan *plaintext* apakah cocok dengan *text* yang ada di sisi sistem. Kalau hasilnya OK maka akan ditampilkan (*preview*) file Faktur Elektronik Penjualan berbasis PDF pada sistem. Namun apabila hasilnya TIDAK OK maka akan tampil pesan kesalahan.

5. *Pembuatan Purwarupa (Prototype) Sistem*

Pada tahapan ini dilakukan pembuatan Purwarupa Sistem Proteksi *Hybrid* Keaslian Faktur Elektronik *(E-Invoice)* Pada E-Bisnis Menggunakan QR Code, Steganografi dengan metode *End OF File* (EOF) Dan Kriptografi dengan menggunakan bahasa pemrograman PHP versi 5.3 (*PHP Hypertext Processor*), HTML (*Hyper Text Markup Language*), JQuery, CSS (*Cascading Style Sheet*), *database* MySQL versi 5.x.

6. *Pengujian dan Analisa*

Teknik pengujian yang dilakukan terbagi dua bagian yaitu pengujian dari sisi konsep proteksi dan verifikasi faktur penjualan elektronik berbasis file PDF dan Purwarupa sistem yang telah dibuat sebagai berikut:

a) Sistem Proteksi dan Verifikasi Faktur Penjualan Elektronik Berbasis PDF

Pengujian dan analisis dilakukan untuk dapat mengetahui apakah konsep proteksi dan verifikasi terhadap faktur elektronik penjualan berbasis PDF yang telah dibuat sesuai dengan analisis kebutuhan pelanggan. Pengujian konsep atau metode proteksi dan juga verifikasi dilakukan dengan pengujian *Error Detection*, sedangkan untuk pengujian validasi fungsional dengan menggunakan *Black Box Testing*.

b) Kualitas Purwarupa Sistem

Dari enam karakteristik hanya empat karakteristik saja yang diadaptasi dalam pene-

litian ini, yaitu Functionality *(Suitability, Accuracy, Security), Reliability (Fault Tolerance), usability (Understandability, Learnability, Operability), dan Efficiency (Time Behavior, Resource Utilization).*

Khusus untuk sub karakteristik *Time Behavior* selain dilakukan testing secara *black-box* oleh reponden juga dilakukan tes dengan menggunakan *tools YSLow*, untuk sub kategori *security* juga akan dilakukan pengujian dengan menggunakan tools security (*Acunetix Web Vulnerablity Scanner* dan *OWASP ZAP Proxy*) untuk mengetahui tingkat kualitas keamanan berdasarkan jenis-jenis kelemahan dan kerentanan apkikasi berbasis *web* dari purwarupa sistem sebelum nantinya benar-benar diterapkan.

7. *Penarikan Kesimpulan*

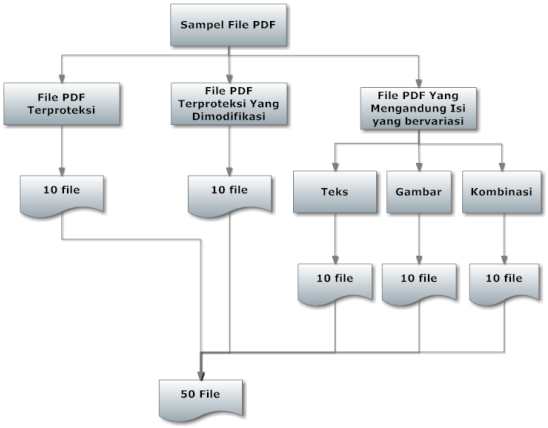
Setelah dilakukan pengujian baik dari sisi obyek file PDF yang belum dilakukan proteksi dibandingkan dengan file faktur penjualan PDF yang sudah diproteksi dengan menggunakan aplikasi *HexEditor* dan pengujian purwarupa sistem dengan mengadopsi beberapa karakteristik sesuai dengan ISO 9126 dengan menggunakan *Black Box Testing* yang hasil keluarannya berbentuk hasil questioner yang selanjutnya dihitung dengan skala *likert*.

IV. PEMBAHASAN HASIL PENELITIAN

4.1. Skenario Pengujian Error Detection

Skenario pengujian *Error Detection* Proteksi dan Verifikasi Faktur Penjualan Elektronik Berbasis File PDF adalah sebagai berikut:

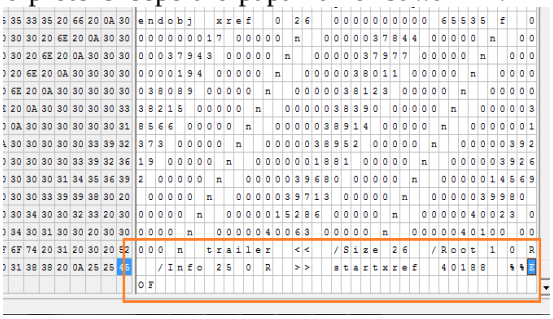
1. Obyek file PDF yang akan dilakukan pengujian *Error Detection* dibagi ke dalam 3 jenis yaitu
   a. File Faktur Penjualan Elektronik yang sudah diproteksi menggunakan *QR Code* dan Steganografi dan Enkripsi.
   b. File Faktur Penjualan Elektronik yang sudah diproteksi menggunakan *QR Code* dan Steganografi dan Enkripsi yang isinya sudah dirubah atau dimodifikasi.
   c. Variasi file format PDF lainnya yang di dalamnya terkandung gambar, teks, kombinasi gambar dan teks.
2. Masing-masing sampel file PDF yang akan dilakukan pengujian masing-masing berjumlah 10 buah file.



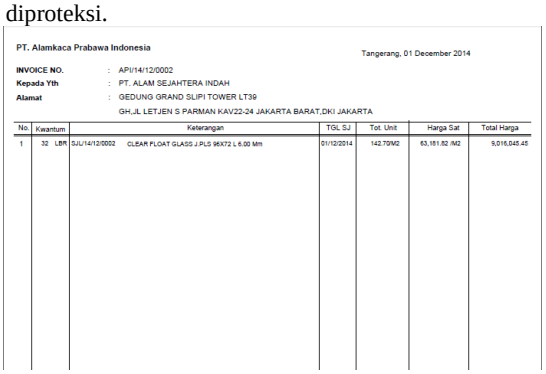
Gambar 9 Skema skenario sampel file PDF untuk pengujian

4.2. Gambaran Sampel File yang Belum Diproteksi dan Yang Sudah Diproteksi

Sebelum dilakukan pengujian proteksi dan verifikasi File Faktur Elektronik PDF maka akan dijelaskan terlebih dahulu perbedaan secara tampilan *source* file PDF antara yang belum diproteksi dan yang sudah diproteksi seperti dipaparkan di bawah ini.

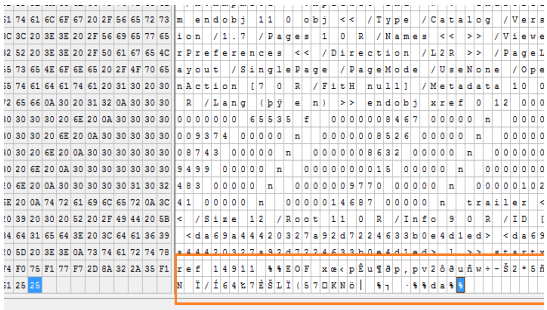


Gambar 10. Tampilan *source* file PDF yang belum diproteksi.

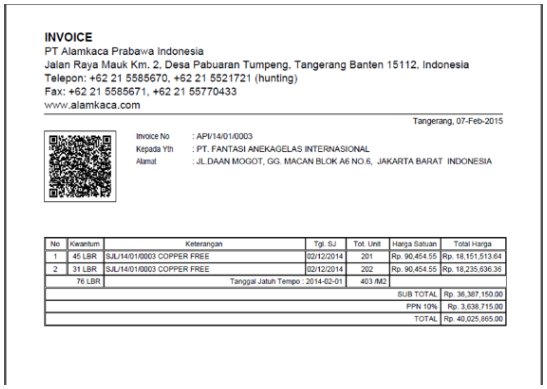


Gambar 11. Tampilan Faktur Penjualan PDF yang belum diproteksi.

Gambar di atas adalah tampilan *hexa* dan faktur penjualan berbasis PDF yang belum dilakukan proteksi di mana setelah tag %%EOF%% (*End Of File*) tidak ada data apapun.



Gambar 12. Tampilan *source* file PDF yang sudah diproteksi.



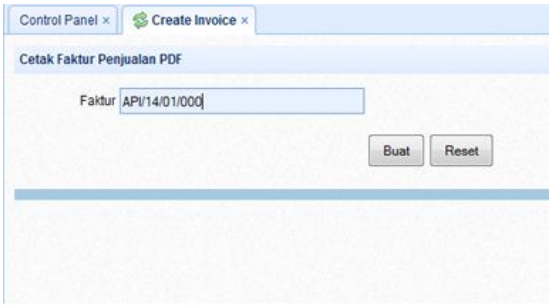
Gambar 13. Tampilan faktur penjualan PDF yang sudah diproteksi.

Gambar di atas adalah tampilan *hexa* dari file faktur penjualan PDF yang sudah dilakukan proteksi di mana setelah tag %%EOF%% (*End Of File*) terdapat karakter acak yang disembunyikan.

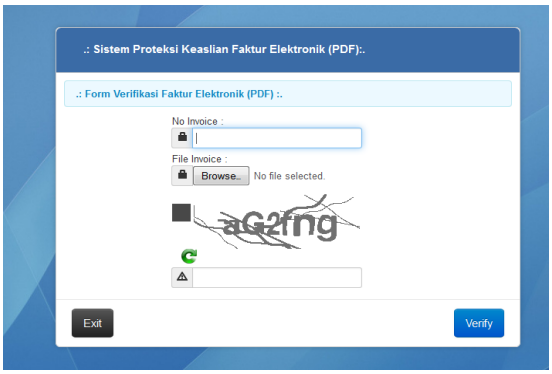
Dari dua gambar hasil membedah file PDF menggunakan *Hex Editor* terlihat perbedaan antara faktur PDF yang belum diproteksi dan yang sudah diproteksi menggunakan teknik steganografi metode EOF (*End Of File*) terenkripsi menggunakan enkripsi AES Rijndael.

Pada gambar IV-23 terlihat ada tambahan setelah tag %%EOF%% berupa karakter acak (terenkripsi) yang merupakan hasil proses steganografi teknik EOF yang terenkripsi.

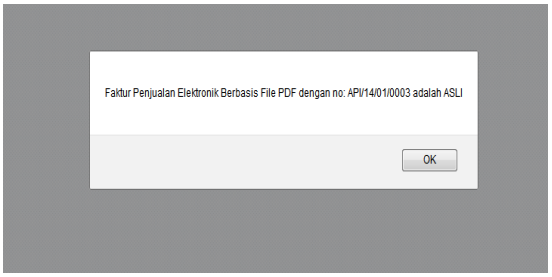
Berikut tampilan layar untuk pengujian proteksi dan verifikasi:



Gambar 14 Tampilan Layar Cetak dan Proteksi Faktur ke PDF.



Gambar 15 Tampilan Layar Verifikasi Faktur Elektronik PDF.



Gambar 16 Tampilan Pesan Verifikasi Faktur Penjualan PDF Asli.

Gambar 17 Tampilan Pesan Verifikasi Faktur Penjualan PDF Tidak Asli.

4.3. Hasil Pengujian Error Detection

Dari table data hasil pengujian di atas dapat dibuat matrik rekalitulasi hasil pengujian sebagai berikut:

Tabel 3 Matrik rekapitulasi hasil pengujian *error detection*,

No	Jenis File	Jumlah File	Hasil Sukses	Hasil Gagal

1	File Faktur Penjualan Elektronik Berbasis PDF yang sudah diproteksi	10	10	0
2	File Faktur Penjualan Elektronik Berbasis PDF yang sudah diproteksi dan dimodifikasi	10	10	0
3	File PDF yang mengandung teks	10	10	0
4	File PDF yang mengandung gambar	10	8	2
5	File PDF yang mengandung teks dan gambar	10	8	2
Total		**50**	**46**	**4**

Dari tabel rekapitulasi total hasil pengujian dari berbagai jenis file PDF diperoleh hasil sebagai berikut:

a) Proteksi

Dari 10 sampel file percobaan proteksi terhadap file faktur penjualan elektronik berbasis PDF diperoleh hasil 10 yang berarti tingkat keberhasilan untuk proteksi tingkat keakuratannya adalah 100 % dan termasuk dalam kategori "Sangat Baik".

b) Verifikasi

Untuk proses verifikasi terhadap berbagai macam jenis file PDF dengan total sampel 50 buah file hasilnya adalah sebagai berikut:

1. Jumlah total sampel file PDF adalah 50 buah file;
2. Jumlah total berhasil diverifikasi adalah 46 buah file; dan
3. Jumlah yang gagal untuk diverifikasi adalah sebanyak 4 buah file.

Dari hasil verifikasi di atas diperoleh keberhasilan proses pengujian verifikasi dapat dihitung prosentasenya sebagai berikut:

46/50 * 100 = 92 %

Maka dapat disimpulkan bahwa hasil pengujian verifikasi tingkat keakuratannya mencapai 92 % dan termasuk dalam kategori "Sangat Baik".

Faktor kegagalan verifikasi disebabkan karena ukuran file yang melebihi kapasitas yang diperbolehkan oleh sistem.

4.4. Hasil Pengujian Kualitas Sistem

Berdasarkan analisis data yang diperoleh dari kuesioner, rekapitulasi hasil pengujian kualitas berdasarkan empat aspek kualitas perangkat *purwarupa* aplikasi ISO 9126.

Tabel 4 Hasil Perhitungan Akhir 4 Kategori.

Aspek	Skor Aktual	Skor Ideal	% Skor Aktual	Kriteria
Functionality	275	350	78.57%	Baik
Reliability	220	250	88.00%	Sangat Baik
Usability	334	350	95.33%	Sangat Baik
Efficiency	192	200	96.00%	Sangat Baik
Total	**1021**	**1150**	**88.45%**	**Sangat Baik**

$$\%\text{Skor Aktual} = \frac{1021}{1150} \times 100\% = 88.78\%$$

Dari hasil akhir pengujian didapat hasil skor aktual sebesar 88.78% dan memiliki kriteria "Sangat baik", ini berarti aplikasi yang dibuat sebagian besar sudah memenuhi kebutuhan.

4.5. Kesimpulan Pengujian Kualitas Menggunakan Tools

Berdasarkan hasil pengujian menggunakan ketiga tools diatas yaitu *YSlow, Acunetix, OWASP ZAP Proxy* sebagai berikut:

1. Response Time (Waktu Respon) Sistem

Dari hasil pengujian untuk karateristik pengujian *response time* (waktu respon) dari sistem untuk satu kali *request* hasilnya adalah 1.47 detik sehingga dapat disimpulkan bahwa waktu respon dari sistem terhadap permintaan dari pengguna "Baik".

2. Keamanan (Security)

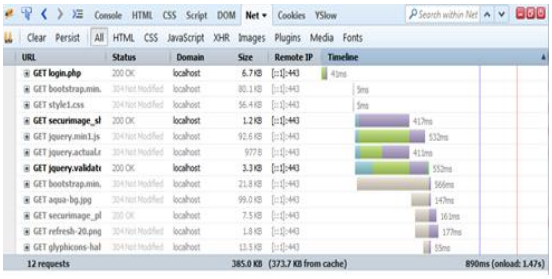
Dari hasil pengujian untuk karakteristik *security* atau keamanan sistem berdasarkan pengujian menggunakan aplikasi *Acunetix Web Vulnerability Scanner* versi 8 diperolah hasil sebagai berikut:

1. Ditemukan hasil 0 untuk kriteria *High* untuk resiko keamanan.
2. Ditemukan hasil 0 untuk kriteria *Medium* untuk resiko keamanan.
3. Ditemukan hasil 0 untuk kriteria *Low* untuk resiko keamanan.
4. Ditemukan hasil 3175 untuk kriteria *Information* untuk resiko keamanan.

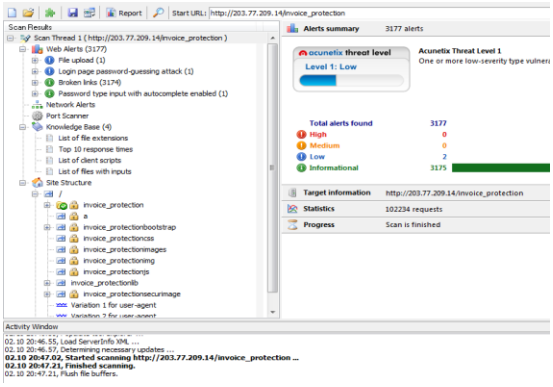
Sedangkan dengan tools *OWASP ZAP Proxy* versi 2.2.2 diperoleh hasil sebagai berikut:

1. Ditemukan hasil 0 untuk kriteria *High Priority alert*
2. Ditemukan hasil 0 untuk kriteria *Medium Priority alert*
3. Ditemukan hasil 2 untuk kriteria *Low Priority alert*
4. Ditemukan hasil 1 untuk kriteria *Informational Priority alert.*

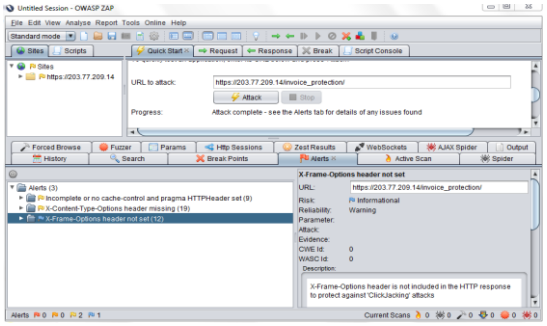
Kesimpulan dari hasil pengukuran dengan menggunakan tools *Acunetix Web Vulnerability Scanner* untuk kriteria *functionality* sub *security* (keamanan) yang mengadaptasi dari ISO 9126 maka dapat disimpulkan hasilnya "Baik" karena ditemukan ada 0 poin resiko keamanan pada kriteria Medium dan hasil 3175 poin untuk resiko keamanan pada kriteria *Low* (rendah) atau sifatnya *informational*. Begitu juga kesimpulan dari hasil pengujian *OWASP ZAP Proxy* 2.2.2 untuk kriteria *functionality sub security* (keamanan) yang mengadaptasi dari ISO 9126 maka dapat disimpulkan hasilnya "Baik".



Gambar 18 Tampilan hasil pengujian akses *respons time* dengan YSlow.



Gambar 19. Hasil pengujian keamanan dengan *Acunetix Web Vulnerability Scanner*.



Gambar 20 Tampilan pengujian keamanan dengan *OWASP ZAP Proxy.*

Setelah dilakukan percobaan menggunakan Aplikasi steganografi dengan metode *End Of File* dan Enkripsi menggunakan algoritma Rindjael *file E-Invoice* berbasis pdf dapat disisipkan kode rahasia yang sudah dienkrip dan file *E-Invoice* pdf tersebut tidak mengalami kerusakan dan dapat dibuka dengan baik dan secara visual tidak ada perbedaan dengan file *E-Invoice* pdf yang tidak disisipkan dengan kode rahasia.

V. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Dari uraian bab pertama hingga bab terakhir, maka dapat diambil kesimpulan sebagai berikut:

1. Penggunaan proteksi dengan menggunakan metode *hybrid* dengan *QR Code*, steganografi yang dipadu dengan teknik Kriptografi dengan enkripsi Advanced Encryption Standard (AES) Rijndael membuat dokumen Faktur Penjualan elektronik berbasis PDF menjadi lebih aman dan dapat terjaga keasliannya serta dapat terdeteksi ketika ada pihak-pihak yang melakukan perubahan pada faktur penjualan elektronik berbasis file *Portable Document Format* (PDF).
2. Dengan adanya purwarupa sistem proteksi dan verifikasi yang dibuat dari sisi internal perusahaan dapat memberikan proteksi atau perlindungan terhadap file faktur penjualan elektronik berbasis PDF sebelum dikirim ke pelanggan dan di sisi eksternal atau pelanggan dapat melakukan verifikasi terhadap keaslian faktur elektronik yang diterima karena sistem menyediakan fasilitas verifikasi dapat diakses secara *online* melalui *internet*.

5.2. Saran

Saran untuk penelitian lebih lanjut dan penyempurnaan penelitian tentang aplikasi ini adalah sebagai berikut:

1. Penelitian dengan membuat sistem di sisi pengguna sehingga proses pengolahan faktur dari pengirim ke penerima bisa dilakukan secara otomatis (B2B) tanpa perantara email ataupun proses manual dari user pelanggan (sistem ke sistem) yang tentu saja dibutuhkan sebuah mekanisme sistem yang standard dan aman baik secara format data maupun jalur komunikasi sehingga lebih meningkatkan keamanan dan otomatisasi proses.
2. Dibuat tampilan khusus untuk *smartphone* atau aplikasi *native* untuk *smartphone* berbasis sistem operasi *mobile device* seperti IOS, Android ataupun *Windows Phone* untuk proses verifikasi dari sisi pelanggan.
3. Penelitian tentang teknik steganografi harus lebih disempurnakan dan dikembangkan lagi khususnya untuk file PDF agar tidak terdeteksi dan tidak dapat dihancurkan oleh *software* untuk membaca atau memodifikasi file PDF.
4. Untuk mengimplementasikan sistem proteksi dan verifikasi keaslian faktur penjualan elektronik berbasis PDF perlu dilakukan pengadaan *hardware* dan *software* yang belum tersedia untuk menunjang kinerja dari sistem informasi baik dari sisi *server* maupun klien, *hardware* untuk *webserver* dan *database server* dan komputer pengguna haruslah sesuai dengan kebutuhan sistem. Infrastruktur jaringan diperlukan terutama karena sistem berbasis *online* berbasis *internet* maka IP *address public* harus tersedia agar sistem dapat diakses oleh pengguna dari *internet*.

DAFTARPUSTAKA

[1] Rm Aidil Fitri Yadi, Proses Pembuatan Dokumen Invoice Dan Packing List Dalam Penjualan Ekspor Batu Bara Pada Pt. Bukit Asam (Persero) Tbk Di Bandar Lampung, Fakultas Ekonomi Dan Bisnis, Universitas Lampung, 2014.

[2] Sweed Bank, Description of electronic invoice service provided by Swedbank, AB and technical requirements for the electronic invoice format, Electronic invoice format version 1.0, 2008.

[3] Esker, White Paper: Best-Practice Automation of Invoice Delivery from ERP Systems: Keeping Customers Satisfied While Making the Move, White Paper, 2007.

[4] Harold F. Tipton, CISSP & Micki Krause, CISSP, Information Security Management Handbook: Fifth Edition, Auerbach Publications, 2002.

[5] Sattarova Feruza Y. and Prof.Tao-hoon Kim, IT Security Review: Privacy, Protection, Access Control, Assurance and System Security, International Journal of Multimedia and Ubiquitous Engineering, Vol. 2, No. 2, April, 2007.

[6] Tom Carlson, Senior Network Systems Consultant, CISSP, Information Security Management: Understanding ISO 17799, INS Whitepaper, Info Security Mgmt.: ISO 17799, Oktober 2001.

[7] La Midjan, Sistem Informasi Akuntansi I, Edisi kedelapan, Penerbit Lingga Jaya, Bandung Definisi Faktur, 2001.

[8] European Commission, Report from the Commission on the application in 2008 of Regulation (EC) No 1049/ 2001 of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents 2009. 331, final, 2 Juli 2009.

[9] Chamber of Commerce, Recommendations for the practical application of electronic invoicing for VAT. The Czech National Forum on Electronic Invoicing, 2012.

[10] Foryszewski, S., The evolution of b2b electronic invoicing, Credit Control, 27(4/5), 35-38, 2006.

[11] Kaliontzoglou, A., Boutsi, P., Polemi, D., eInvoke: Secure e-Invoicing based on web services. Electronic Commerce Research, 6, 337–353, 2006.

[12] Kotler, Philip, Dipak C.Jain, Suvit Maesincee, Marketing Moves: A New Approach To Profits, Growth, and Renewal, Harvard Business School Press, Boston Massachusetts, 2002.

[13] Judy Strauss, Raymond Frost, E-Marketing, 5th edition, Pearson Education, Prentice Hall, 2008.

[14] Budi Sutedjo Dharma Oetomo, Perspektif e-Business: Tinjauan Teknis, Manajerial, dan Strategi, Penerbit Andi Yogyakarta, Yogyakarta, 2001.

[15] Denso-Wave incorporated Website. ND. Bar code to 2D Code. (Online). (Diakses dari www.qrcode.com/aboutqr-e.html tanggal 10 Maret 2011).

[16] Kas. Thomas, PDF Intro ,Volume Number: 15 (1999), Issue Number: 9, Column Tag: Emerging Technologies, http://www.mactech.com/articles/mactech/Vol.15/15.09/PDFIntro/index.html, Vol.15, 15.09, (Diakses pada 17 Desember 2014).

[17] www.gnostice.com, Spesifikasi File PDF, (Diakses pada 17 Desember 2014).

[18] www.simpopdf.com, PDF File Structure, http://www.simpopdf.com/resource/pdf-file-structure.html, (Diakses pada 17 Desember 2014).

[19] Jati Sasongko, Pengamanan Data Informasi menggunakan Kriptografi Klasik, Jurnal Teknologi Informasi DINAMIK Volume X, No.3, September 2005: 160-167 I, ISSN: 0854-9524, 2005.

[20] Ary Budi Warsito, Lusi Fajarita, Nazori AZ, Proteksi Keamanan Dokumen Sertifikat File Jpeg Pada Perguruan Tinggi Dengan Menggunakan Steganografi Dan Kriptografi, ISSN: 2085-725X, Jurnal Telematika MKom Vol.4 No.1, Maret 2012.

[21] Sandro Sembiring, Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File, ISSN: 2301-9425, Pelita Informatika Budi Darma, Volume: IV, Nomor: 2, Agustus 2013.

[22] Adnan Abdul-Aziz Gutub, King Saudi University, Saudi, Arabia, Pixel Indicator Technique for RGB Image Steganography, Journal of Emerging Technologies in Web Intelligence, Vol.2, No.1, February, 2010.

[23] Navjot Kaur, Dr. Rajiv Mahajan, A Survey on Embedded Extended Visual Cryptography Scheme, International Journal Of Engineering Sciences & Research Technology, IJESRT, October 2013.

[24] Mohammed Abutaha, et.al. Survey Paper: Cryptography is The Science of Information Security, Communication Theory of Secrecy Systems, Vol.5, No.3, Juli 2011.

[25] Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid, Symmetric Algorithm Survey: A Comparative Analysis, IQRA University, Main Campus, Defense View, Karachi, International Journal of Computer Applications (0975- 8887) Volume 61–No.20, January 2013, 2013.

[26] Yusuf Kurniawan, Adang Suwandi Ahmad, M. Sukrisno Mardiyanto, Iping Supriana, Sarwono Sutikno, Analisis Sandi Diferensial terhadap AES, DES dan AE1, PROC. ITB Sains & Tek. Vol. 38 A, No. 1, 2006, 73-88, 2006.

[27] Didi Surian, Algoritma Kriptografi AES Rijndael, Jurnal Teknik Elektro, TESLA Vol.8, No.2, 97-101, Oktober 2006.

[28] Rinaldi Munir, Kriptografi ,Penerbit Informatika, Hal 304, 2006.

[29] ISO/IEC FDIS 9126-1, Information Technology-Software Product Quality

Part 1 - Quality Model, International Standard, 2000.

[30] Ralph M. Stair, George W. Reynolds, Principles of Information Systems, A Managerial Approach, Ninth Edition, Professor Emeritus, Florida State University, 2010.

[31] Effy OZ, Management Information Systems, Sixth Edition, The Pennsylvania State University, Great Valley, 2009.

[32] Oxford Dictionary, http://www.oxforddictionaries.com/us/definition/american_english/hybrid, Definisi hybrid, (Diakses tanggal 21 Desember 2014).

[33] I-Shi Lee and Wen-Hsiang Tsa. A new approach to covert communication via pdf, Signal Processing Journal, 90:557-565, 2010.

[34] Hongmei Liu, Lei Li, Jian Li, and Jiwu Huang. Three novel algorithms for hiding data in pdf_les based on incremental updates. Technical report, Sun Yat-sen University, Guangzhou, China, 2007.

[35] Shangping Zhong, Xueqi Cheng, and Tierui Chen. Data hiding in a kind of pdf texts for secret communicationl, International Journal of Network Security, 4(1):17-26, 2007.

[36] Fahimeh Alizadeh, Nicolas Canceill, Sebastian Dabkiewicz, Diederik Vandevenne, Using Steganography to hide messages inside PDF files, SSN Project Report, December 30, 2012.

[37] Ana Wahyuni, Aplikasi Kriptografi Untuk Pengamanan E-Dokumen Dengan Metode *Hybrid*: Biometrik Tandatangan Dan DSA (*Digital Signature Algorithm*), 2011.

[38] Eko Ariwibowo, Aplikasi Pengamanan Dokumen Office Dengan Algoritma Kriptografi Kunci Asimetris ElGamal. Yogyakarta: Universitas Ahmad Dahlan Yogyakarta, 2008.

[39] Ari Muzakir, Pemanfaatan dan Implementasi Library XMLSEC Untuk Keamanan Data Pada XML Encryption, Seminar Nasional Informatika 2013 (semnasIF 2013) ISSN: 1979-2328 UPN Veteran Yogyakarta, 18 Mei 2013.

[40] Supriyono, Pengujian Sistem Enkripsi-Dekripsi Dengan Metode Rsa Untuk Pengamanan Dokumen, JFN, Vol 2 No. 2, November 2008, ISSN 1978-8738, 2008.

[41] Moedjiono, Pedoman Penelitian, Penyusunan dan Penilaian Tesis (V.5), Jakarta: Universitas Budi Luhur, 2012.

[42] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif dan R&D, Bandung: Alfabeta, 2012.