PENGGUNAAN DAN PEMANFAATAN APLIKASI KEAMANAN DOCUMENT DIGITAL PADA SEBUAH PERUSAHAAN DEGAN TEHNIK ALGORITMA STEGANOGRAFI DAN ALGORITMA KRIPTOGRAFI

Ade Priyatna , Sanwani , Besus Maula Sulthon

STMIK Nusa Mandiri

Pada era digital dan industri 4.0 seperti sekarang ini yang semuanya serba digital atau elektronik termasuk dalam hal dokumen , *dokumen elektronik sendiri merupakan informasi yang direkam atau disimpan dengan cara yang memerlukan perangkat komputer atau perangkat elektronik lain untuk menampilkan ,menafsirkan atau memprosesnya. Dokumen-dokumen tersebut bisa berupa teks, grafik atau spreadsheet atau jenis dokumen yang lainnya. Seiring dengan perkembangan teknologi saat ini yang semakin maju pesat, keamanan menjadi factor yang sangat penting pada sebuah perusahaan untuk menghindari terjadinya tindak pencurian informasi oleh pihak-pihak yang tidak bertanggung jawab dalam hal ini bisa dalam bentuk pencurian dokumen penting secara elektronik. Salah satu cara yang bisa digunakan untuk mengamankan dokumen digital adalah memanfaatkan teknologi Steganografi dan Kriptografi dengan menggunakan algoritma Discrete Cosine Transform (DCT) dan algoritma Advanced Encryption Standard (AES-192). Tujuan penggunaan dan pemanfaatan aplikasi ini untuk mengamankan sebuah data atau file yang akan disembunyikan pada file image cover. Sebelum disisipkan dengan file image cover, file tersebut dilakukan proses enkripsi pesan text terlebih dahulu dengan kunci secara simetris menggunakan algoritma AES-192. Manfaat yang didapatkan dalam aplikasi ini adalah kerahasiaan informasi atau data pada sebuah perusahfaan tersebut bisa terjaga dengan baik dan aman. Dengan menggunakan dan memanfaatkan aplikasi ini diharapkan dapat membantu untuk menjaga kerahasiaan informasi atau data kususnya dokumen pada perusahaan tersebut.*

Keyword : *Digital , Steganografi, Industri 4.0, Discrete Cosine Transform, Keamanan, Kriptografi, Data, Advanced Encryption Standard, Dokumen*

PENDAHULUAN

Kemudahan pada dokumen digital atau elektronik yang fleksibel untuk bisa diedit, digandakan ataupun didistribusikan oleh siapapun membuat semakin banyak orang cenderung bekerja pada dokumen berbasis digital atau elektronik dibandingkan dengan bekerja menggunakan dokumen konvensional. Pada saat ini di dalam industri 4.0 yang mempunyai ciri kemudahan dan efisiens dalam melakukan sesuatu. Definisi mengenai Industri 4.0 beragam karena masih dalam tahap penelitian dan pengembangan , Industri 4.0 adalah transformasi komprehensif dari keseluruhan aspek produksi di industri melalui penggabungan teknologi digital dan internet dengan industri konvensional menurut Angela Merkel dalam (Telaah et al., 2018) , karenanya begitu banyak hal kususunya dokumen digital atau elektronik yang dibuat dengan mudah melalui alat seperti komputer dan dibarengi dengan berkembangnya banyak aplikasi pengolah data kusus untuk dokumen.

Pada kasus tertentu, ada beberapa dokumen tersebut yang mungkin bisa di katagorikan sebagai dokumen rahasia. Dokumen ini hanya dapat dibaca atau diberikan oleh dan untuk orang-orang tertentu. Tentunya perkembangan tersebut mempunyai dampak , salah satu dampak negative dalam perkembangan teknologi adalah adanya pencurian data, yang merupakan salah satu masalah serius dan ditakuti oleh para pengguna jaringan komunikasi di perusahaan, Dengan adanya pencurian data maka aspek keamanan dalam pertukaran informasi serta penyimpanan data dianggap sangat penting (Hasugian, 2017). Oleh karenanya diperlukan sebuah mekanisme atau metode untuk bagaimana caranya mengamankan dokumen elektronik tersebut.

Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang tidak bersifat rahasia (Hasugian, 2017). Yang pertama adalah data yang tidak bersifat rahasia, ini biasanya tidak akan terlalu diperhatikan, justru yang harus diperhatikan adalah data yang bersifat rahasia, karena di mana setiap informasi yang ada didalamnya bisa sangat berharga bagi pihak siapapun yang membutuhkannya, karena data tersebut bisa dengan mudah untuk digandakan.

Seperti yang kita ketahui bersama , akhir-akhir ini terjadi sebuah pencurian data kependudukan di lembaga Komisi Pemilihan Umum (KPU) , disebutkan bahwa ada sekitar 2,3 Juta data kependudukan telah di ambil oleh orang yang tidak bertanggung jawab , data yang telah dicuri ini bisa di manfaatkan untuk berbagai macam hal , seperti registrasi simcard baru yang artinya kasus penipuan dan cloning sebuah nomor bisa semakin merebak dan mudah terjadi (Aida, 2020)

Karenanya muncul sebuah ide yang mendasari pada permasalahan tersebut, yaitu untuk memanfaatkan sebuah sistem keamanan yang dapat melindungi data yang dianggap penting dengan sebuah penyandian data, serta membuat sebuah kunci rahasia untuk bisa mengakses data tersebut yang nantinya akan sulit untuk di deteksi oleh pihak yang tidak mempunyai atau mengetahui kunci akses ke file tersebut.

TINJAUAN PUSTAKA

Teknologi saat ini membuat pekerjaan bisa dikerjakan dengan cepat, akurat dan efisien serta mudah sehingga banyak dokumen penting yang disimpan dalam bentuk digital , keamanan dokumen digital tersebut harus dijaga dengan baik dalam penyimpanan maupun dalam pengiriman informasinya , sehingga nantinya tidak bisa disalahgunakan oleh pihak yang tidak berhak atas dokumen tersebut yang nantinya bisa menyebabkan kerugian pada perusahaan. Dengan menggabungkan teknik kriptografi dan steganografi maka pemanfaatan aplikasi ini dapat menghasilkan ukuran file enkripsi lebih kecil sehingga proses penyisipan lebih cepat dan memberikan keamanan dokumen digital lebih baik yang ada pada perusahaan (Andani & Fithri, 2017)

Tujuan dari pemanfaatan teknologi ini adalah untuk menyembunyikan dan merahasiakan data dengan cara yang tidak memungkinkan siapapun untuk mendeteksi ataupun membuka dan

memanfaatkan data tersebut. Secara umum, teknik steganografi yang baik harus memiliki visual statistik yang baik dan payload yang memadai. Dengan melakukan enkripsi pada sebuah data , maka data tersebut akan sulit untuk di manfaatkan secara langsung dari orang yang tidak bertanggung jawab , karena data tersebut harus disusun ulang dan diperlukan tehnik tertentu ataupun kunci untuk membuat ataupun membuka data tersebut seperti aslinya.
Ada tiga unsur penting pada kriptografi yaitu pembangkitan kunci, enkripsi dan deskipsi.Pada kriptografi di kenal sebuah algoritma yaitu block chiper yang didalamnya terdapat AES (*Andvanced Encyption Standard*) yang merupakan bagian dari *Modern Symmetric Key Cipher*, algoritma ini menggunakan kunci yang sama saat proses enkripsi dan deskripsi sehingga data yang kita miliki akan sangat sulit dimengerti. Teknik algoritma tersebut digunakan untuk mengkonversi data dalam bentuk kode-kode tertentu agar informasi yang tersimpan tidak bisa di ketahui siapa pun kecuali orang-orang yang berhak. Oleh karena itu, sistem keamanan data sangat di perlukan untuk menjaga kerahasian informasi agar tetap terjaga (Nurnaningsih & Permana, 2018)

Telah dilakukan pengujian pada suatu model pengamanan dokumen yang bisa digunakan sebagai salah satu instrumen sistem pengamanan pada dokumen khususnya untuk dokumen teks. Adapun prinsip pengamanan dokumen ini adalah bagaimana caranya sistem dapat mengamankan proses penyimpanan dan pengiriman dokumen. Tahap pertama dokumen dalam bentuk teks dienkripsi sehingga dokumen tersebut tidak dapat dibaca oleh siapapun karena teks telah berubah menjadi susunan huruf yang teracak. Dokumen tersebut jika ingin dibaca kembali oleh pemilik dokumen, maka dokumen tersebut harus dibuka dengan dekripsi. Dalam penelitian ini, metode yang digunakan adalah metode RSA, dimana metode tersebut menggunakan perhitungan matematika yang rumit dan disertai dengan kunci pengaman awal (dengan private key maupun dengan public key) sehingga sangat sulit untuk ditembus oleh orang yang tidak berkepentingan.Hasil pengujian ini menunjukkan bahwa sistem dapat menyimpan dan mengirimkan dokumen baik pengiriman melalui internet maupun intranet dalam bentuk susunan huruf yang terenkripsi dan mengembalikan ke bentuk dokumen semula dengan cara dekripsi (Benny, 2017)

Dokumen Digital

Dokumen sendiri merupakan sebuah sarana informasi dari satu orang ke orang lain atau beberapa orang dan dari suatu kelompok ke orang lain ataupun kelompok lain. Dokumen digital sendiri merupakan setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto atau sejenisnya (Pabokory et al., 2016)

Keamanan Data

Secara definisi keamanan data adalah usaha untuk melindungi dan menjamin tiga aspek terpenting dalam dunia siber yaitu :

1. Kerahasiaan data.
2. Keutuhan data.
3. Ketersediaan data.

(Gunawan, 2020)

Steganografi

Steganografi sendiri merupakan suatu ilmu atau seni dalam menyembunyikan informasi dengan memasukkan informasi tersebut ke dalam pesan lain (Niswati, 2012)

Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi menurut Rinaldi Munir dalam (Hasugian, 2017)

MATERIAL AND METHODS

Pada penelitian ini metode yang digunakan adalah dengan melakukan metode penelitian kepustakaan, wawancara dan observasi di perusahaan sedangkan metode pada pengembangan sistem yang digunakan adalah dengan tahapan seperti analisis, desain, implementasi dan perawatan.

Metode Pustaka

> Metode ini dilakukan untuk mengumpulkan data atau informasi dengan mencari referensi berupa jurnal, artikel dan situs internet mengenai metode yang akan digunakan.

Wawancara dan Observasi

> Melakukan interaksi langsung terhadap objek penelitian dan langsung mengobservasinya yang kemudian data atau informasi yang diperoleh untuk di analisis dan dipelajari.

Metode Algoritma Steganografi Discrete Cosine Transform (DCT)

Tujuan dari penggunaan metode steganografi adalah untuk menyembunyikan pesan dalam pesan berbahaya lainnya dengan cara yang tidak memungkinkan musuh apapun bahkan untuk mendeteksi bahwa ada pesan kedua. secara umum, teknik steganografi yang baik harus memiliki visual/imperceptibility statistik yang baik dan payload yang cukup (Alatas, 2009). Metode steganografi membutuhkan dua aspek utama yaitu media penyimpan dan informasi rahasia yang akan disembunyikan. Metode steganografi sangat berguna jika digunakan pada komputer karena banyak format file digital yang dapat dijadikan media untuk menyembunyikan pesan. Pada steganografi digital menggunakan media digital sebagai wadah penampung seperti teks, citra, suara, dan video. Data rahasia yang disembunyikan juga dapat berupa teks, citra, suara, ataupun video (Ridwan et al., 2020)

Discrete Cosine Transform (DCT) adalah tehnik yang digunakan untuk mengubah sebuah sinyal menjadi komponen sebuah frekuensi dasar. Discrete Cosine Transform (DCT) termasuk metode steganography pada Algorithms and Transformation yang menyembunyikan data dalam fungsi matematika.

DCT mempunyai dua sifat utama untuk kompresi citra dan video yaitu :
a. Mengkonsentrasikan energi citra ke dalam sejumlah kecil koefisien (energi compaction).
b. Meminimalkan saling ketergantungan diantara koefisien-koefisien (decorrelation).

Discrete Cosine Transform dari sederet u,v bilangan real s(u,v), u = 0, … ,n-1, dan v = 0,…,m-1 dirumuskan pada persamaan 1 sebagai berikut (Baskurt, 1990)

$$S(u,v) = \frac{2}{\sqrt{mn}} C(u)C(v) \sum_{y=0}^{n-1} \sum_{x=0}^{n-1} S(x,y) \cos\left[\frac{(2x+1)u\pi}{2n}\right] \cos\left[\frac{(2y+1)v\pi}{2m}\right]$$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}}, & u = 0 \\ 1, & u \neq 0 \end{cases} \quad ; \quad u = u, v$$

Gambar 1 : *Rumus Forward Discrete Cosine Transform 2D*

Pada setiap element dari hasil transformasi s (x,y) merupakan hasil dot product atau inner product dari masukan S(u,v) dan basis vektor[4]. Faktor konstanta dipilih sedemikian rupa sehingga basis vektornya orthogonal dan ternormalisasi. DCT juga dapat diperoleh dari produk vektor (masukan) dan n x n matriks orthogonal yang setiap baris dan kolom merupakan basis vektor.

Metode Algoritma Kriptografi Advanced Encryption Standart (AES-192)
Standar enkripsi dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat terdiri atas 3 blok cipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Data Encryption Standard (DES) (Khan, 2015).
Setiap 3 blok chiper pada AES-128, AES-192 dan AES-256 mempunyai perbedaan pada jumlah key dan jumlah putaran keterangan pada tabel 1.

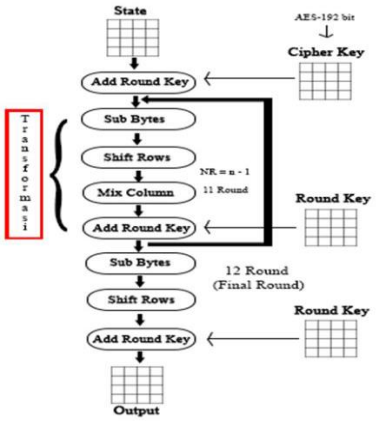
Tabel 1 : Perbandingan Jumlah Round dan Key pada Tipe

AES **Tipe**	**Jumlah Key (NK)**	**Ukuran Blok (Nb)**	**Jumlah Putaran (Nr)**
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Sumber : (Bouillaguet et al., 2012)

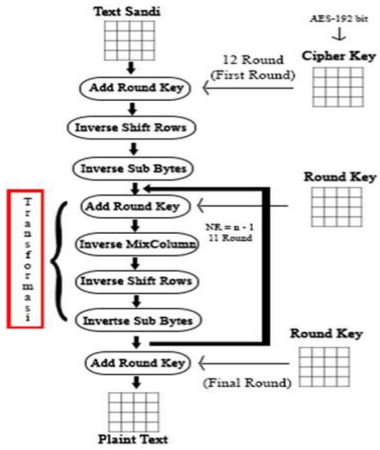
Pada dasarnya, operasi Advanced Encryption Standard (AES) dilakukan terhadap *Array Of Byte* dua dimensi yang disebut *State*. *State* mempunyai ukuran NROWS x NCOLS. Pada awal

enkripsi, data masukan yang berupa in0, in2, in4 ,in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 disalin ke dalam *Array State*.



Sumber : (Primartha, 2011)
Gambar 2 : Proses Enkripsi AES – 192

Proses Enkripsi pada gambar 1 dimulai dari AddRoundKey. AddRoundKey yaitu mengkobinasikan sebuah Chiperkey dan State dengan menggunakan operator XOR (Saputra & Kusumaningsih, 2018). Yang kedua Sub Bytes adalah menukar isi matriks dengan baris dan kolom pada tabel S-Box. Di bawah ini adalah contoh tabel S-Box. Yang ke tiga Shift Rows adalah sebuah proses melakukan pergeseran pada setiap elemen blok/tabel yang dilakukan per barisnya. baris pertama tidak dilakukan pergeseran, baris kedua dilakukan pergeseran 1 byte, baris ketiga dilakukan pergeseran 2 byte dan baris ke-empat dilakukan pergeseran 3 bytes. Berikutnya Mix Column adalah mengalikan tiap elemen dari Blok Chiper dengan matriks yang sudah ditentukan. Pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan Dot Product lalu perkalian keduanya dimasukkan ke dalam sebuah Blok Chiper baru. Bila sudah dikalikan semua dengan matriks yang sudah ditentukan. Maka terbentuk hasil Polynomial dengan bentuk biner dan hasil itu di gabungkan dengan rumus perkalian Mix Column pada setiap tahap perkalian matriks. Dan yang terakhir Add Round Key adalah mengkombinasikan Chiperteks yang sudah ada dengan Chiperkey dihubungkan pada operator XOR (Hakim & Utami, 2014)



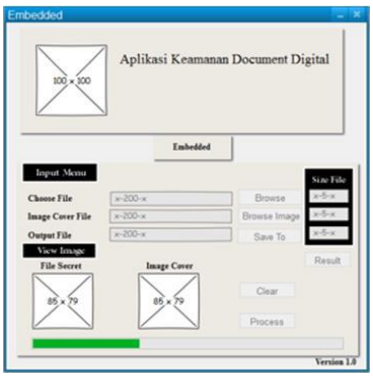
Sumber : (Primartha, 2011)
Gambar 3 : Proses Deskrip AES – 192

Proses Deskrip pada gambar 3 dimulai dari InvMixColumns yaitu Setiap kolom dalam state dikalikan dengan matrik yang sudah ditentukan pada perkalian dalam AES-192, berikutnya

InvShiftRows adalah transformasi byte yang berkebalikan dengan transformasi ShiftRows. Pada transformasi InvShiftRows, dilakukan pergeseran bit ke kanan sedangkan pada ShiftRows dilakukan pergeseran bit ke kiri. Yang ketiga InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan tabel Inverse S-Box dan yang terakhir AddRoundKey adalah mengkombinasikan chiperteks yang sudah ada dengan chiperkey dihubungkan pada operator XOR.

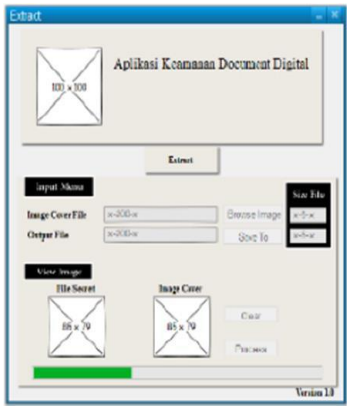
HASIL DAN PEMBAHASAN

Perancangan akan dibuat dua tampilan ata desain yaitu tampilan layar Embed dan tampilan layar Extract. Pada rancangan *embedded* gambar 3 dibawah dijelaskan tentang bagaimana *user* melakukan sebuah penyisipan pada *file rahasia* dengan *file cover* sehingga dapat menghasil *stego image* atau *output* gambar. Saat melakukan proses *user* diminta untuk memasukan *password* sepanjang 8 *character* dan akan dilakukan sebuah proses enkripsi yaitu AES-192. setelah selesai melakukan proses enkripsi akan disisipkan dengan menggunakan Discrete Cosine Transform.



Sumber : (Sukarno, 2013)
Gambar 4 : *Rancangan Layar Embed*

Setelah penjelasan dari rancangan layar porses *embedded*. Gambar 4 adalah gambar dari rancangan layar *extract*.



Sumber : (Sukarno, 2013)

Gambar : 5 *Rancangan Layar Extract*

Pada rancangan layar *form extract* hampir sama dengan racangan layar *embedded* hanya saja ada beberapa perbedaan seperti tidak adanya choose *file secret* dikarenakan hanya mengeluarkan *file* asli dari *stego image*.

implementasi dan uji coba dari sistem yang akan dibuat. Bab ini akan menjelaskan tentang hasil dari proses *embed* dan *extract* berdasarkan uji yang telah disiapkan dengan berbagai uji coba *file Cover* dengan *file document* pada algoritma kripstografi AES-192 dan algoritma steganografi Discrete Cosine Transform (DCT). Pada bab ini juga akan membuat suatu evaluasi dari pengujian program tersebut. Evaluasi tersebut bertujuan agar selanjutnya progam ini akan dikembangkan kembali menjadi lebih baik lagi dan lebih berguna bagi yang menggunakan atau *user*. Tabel 2 menunjukani proses pengujian dari sample gambar atau *file Cover*.

Tabel 2 : File Sample Cover

NO	Gambar Cover	Nama File	Ukuran Pixel	Ukuran Gambar
1		Sample 1.JPEG	1920 x 1200	180 KB
2		Sample 2.JPG	2880 x 1800	699 KB
3		Sample 3.JPG	640 x 640	128 KB
4		Sample 4.JPG	640 x 640	104 KB

Sumber : (Ridwan et al., 2020)

Pada sampel tabel 2 menggunakan 4 sampel *file cover* dengan masing-masing ukuran pixel tinggi dan lebar yang berbeda-beda berekstensi tipe *file* jpg. Kemudian sampel *file cover* diatas akan dilakukan uji coba untuk melakukan penyisipan pada *file* dokumen *pdf, xlsx* dan *docx* dengan *file cover* sebagai media penampung. Dalam pengujian kali ini akan dibahas antara

proses *embed* dan *extract* antara *file document*. Tabel 3 adalah hasil uji coba pada percobaan *file* dokumen pada *file cover*.

Tabel 3: Pengujian Embed file docx,xlsx dan pdf

No.	File Secret		File Gambar		Waktu Embed (Seconds)
	Nama File	Ukuran	Nama File	Ukuran	
1	smo 1-30 des.docx	28 KB	Sample 1.jpeg	179 KB	199.09
2	smo 1-30 des.docx	28 KB	Sample 2.jpg	699 KB	245.23
3	smo 1-30 des.docx	28 KB	Sample 3.jpg	128 KB	155.33
4	smo 1-30 des.docx	28 KB	Sample 4.jpg	104 KB	156.09
5	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	Sample 1.jpeg	179 KB	136.91
6	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	Sample 2.jpg	699 KB	198.58
7	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	Sample 3.jpg	128 KB	96.65
8	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	Sample 4.jpg	104 KB	95.14
9	CORPORATE SECRETARY.pdf	17 KB	Sample 1.jpeg	179 KB	34.51
10	CORPORATE SECRETARY.pdf	17 KB	Sample 2.jpg	699 KB	77.22
11	CORPORATE SECRETARY.pdf	17 KB	Sample 3.jpg	128 KB	11.70
12	CORPORATE SECRETARY.pdf	17 KB	Sample 4.jpg	104 KB	12.28

Sumber : (Ridwan et al., 2020)

Pada hasil pengujian *embed* dapat dilihat pada tabel dibawah ini dengan menggunakan sebuah PSNR dan MSE.

Tabel 4 : Hasil Pengujian *Embed*

NO	Format Dokumen	Stego File		PSNR (db)	MSE (db)
		Nama File	Ukuran		
1	DOCX	Stego Gambar 1.Jpeg	1.33 MB	50.3366	0.6018
2		Stego Gambar 2.JPG	7.57 MB	53.3827	0.2984
3		Stego Gambar 3.JPG	885 KB	43.7495	2.7424
4		Stego Gambar 4.JPG	813 KB	43.1658	3.1369
5	XLSX	Stego Gambar 1.Jpeg	1.31 MB	51.0571	0.5098
6		Stego Gambar 2.JPG	7.56 MB	53.8033	0.2709
7		Stego Gambar 3.JPG	878 KB	44.6986	2.2041
8		Stego Gambar 4.JPG	803 KB	44.1296	2.5126
9	PDF	Stego Gambar 1.Jpeg	1.29 MB	51.8329	0.4264
10		Stego Gambar 2.JPG	7.55 MB	54.2310	0.2455
11		Stego Gambar 3.JPG	874 KB	45.7243	1.7404
12		Stego Gambar 4.JPG	794 KB	45.1793	1.9731

Total	**581.2907**	**16.6623**

Sumber : (Ridwan et al., 2020)

Hasil pengujian diatas pada saat selesai melakukan *embed* dapat ditarik kesimpulan bahwa rata-rata PSNR $\frac{\mathbf{581.2907}}{12} = 48.4409db$ dan MSE $\frac{\mathbf{16.6623}}{12} = 1.3885db$ kualitas citra yang dilakukan penyisipan adalah **baik** dengan rata-rata > **40db** dari 12 sample dari tipe *file* dokumen yang berbeda-beda.

Tabel 5 : Hasil Pengujian Extract

NO.	Stego File		Hasil Extract	Ukuran	Waktu (Seconds)
	Nama File	Ukuran			
1	Stego Gambar 1.Jpeg	1.33 MB	smo 1-30 des.docx	28 KB	44.25
2	Stego Gambar 2.JPG	7.57 MB	smo 1-30 des.docx	28 KB	94.91
3	Stego Gambar 3.JPG	885 KB	smo 1-30 des.docx	28 KB	16.08
4	Stego Gambar 4.JPG	813 KB	smo 1-30 des.docx	28 KB	15.40
5	Stego Gambar 1.Jpeg	1.31 MB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	34.51
6	Stego Gambar 2.JPG	7.56 MB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	77.22
7	Stego Gambar 3.JPG	878 KB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	11.70
8	Stego Gambar 4.JPG	803 KB	Master 1-30 TARAKAN SEPT 2015.xlsx	22 KB	12.28
9	Stego Gambar 1.Jpeg	1.29 MB	CORPORATE SECRETARY.pdf	17 KB	27.0
10	Stego Gambar 2.JPG	7.55 MB	CORPORATE SECRETARY.pdf	17 KB	50.88
11	Stego Gambar 3.JPG	874 KB	CORPORATE SECRETARY.pdf	17 KB	7.77
12	Stego Gambar 4.JPG	794 KB	CORPORATE SECRETARY.pdf	17 KB	8.61

Sumber : (Ridwan et al., 2020)

Hasil pengujian diatas pada saat selesai melakukan *extract.* Dapat ditraik kesimpulan bahwa tidak terjadi perubahan *size file* yang di*extract*. Sehingga *file* tersebut sama seperti aslinya.

KESIMPULAN

Sesuai dengan pembahasan mengenai penggunaan dan pemanfaatan aplikasi keamanan untuk document digital menggunakan algoritma steganografi discrete cosine transform (DCT) dan algoritma kriptografi advanced encryption standard (AES-192), diharapkan dengan penerapan dokumen elektronik yang berbasis metode dan algoritma stegnografi DCT dan Kriptografi AES-192 bisa melindungi informasi didalamnya terhadap orang-orang yang tidak mempunyai kepentingan maka dengan ini dapat disimpulan antara lain yaitu

1. Dengan adanya aplikasi pengamanan dokumen digital menggunakan algoritma steganografi discrete cosine transform (DCT) dan algoritma kriptografi advanced encryption standard (AES-192) dapat mengamankan data atau informasi yang ada di Perusahaan bisa terjaga kerahasiaan datanya dari orang yang tidak bertanggung

2. waktu yang digunakan untuk melakukan proses embed dan extract berbanding lurus dengan ukuran file yang diproses. Semakin besar ukuran file yang diproses maka semakin lama proses embed dan extract, semakin kecil ukuran file yang diproses, semakin cepat porses embed dan extract dilakukan.

3. dengan adanya aplikasi steganografi dan kriptografi, proses penyimpan informasi menjadi lebih aman sehingga tidak mengakibatkan kecurigaan akan adanya dokumen rahasia.

4. Proses extract dengan password yang asli akan mengembalikan file menjadi file semula tanpa mengalami perubahan sedikitpun.

Penelitian ini masih jauh dari sempurna dan masih perlu banyak perbaikan dan pengembangan supaya menjadi lebih baik lagi. Adapun saran untuk pengembangan dari penelitian ini antara lain

1. waktu proses embed dan extract file yang rata-rata berukuran besar diharapkan dapat berjalan lebih cepat pada hardware yang lebih baik.
2. dikembangkan menggunakan algoritma steganograi yang lebih baik, agar ukuran file hasil embed diharapkan dapat menjadi lebih kecil lagi.
3. aplikasi ini diharapkan dapat ditingkatkan kinerjanya sehingga file cover tidak hanya file gambar png, jpg dan bmp saja, namun file cover lainnya serta dapat juga file lainya seperti (*.ppt, *.xlsx, *.pdf, dll) dan *cover* (*.gif, *.mp3, *.mp4, dll).

REFERENCES

Aida, N. R. (2020). *Jutaan Data Kependudukan di DPT Pemilu 2014 Milik KPU Diduga Bocor, Apa Bahayanya?* https://www.kompas.com/tren/read/2020/05/22/165000465/jutaan-data-kependudukan-di-dpt-pemilu-2014-milik-kpu-diduga-bocor-apa

Alatas, P. (2009). Implementasi teknik steganografi dengan metode lsb pada citra digital. *Universitas Gunadarma*, 1–11. http://www.gunadarma.ac.id/library/articles/graduate/computer-science/2009/Artikel_11104284.pdf

Andani, I. S., & Fithri, D. L. (2017). Aplikasi Pengamanan Dokumen Digital Menggunakan Algoritma Kriptografi Advanced Encryption Standard (Aes-128), Kompresi Huffman Dan Steganografi End Of File (Eof) Berbasis Desktop Pada Cv. Karya Perdana. *Prosiding SNATIF*, *1*, 269–276. https://doi.org/10.1016/0143-148X(80)90013-0

Baskurt, A. (1990). Numerical image compression using the discrete cosine transform. *Signal Processing*, *19*(4), 346. https://doi.org/10.1016/0165-1684(90)90166-v

Benny, L. (2017). *Analisis Dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks Dengan Menggunakan Metode Rsa*. *1*(April P-ISSN : 2541-1322), 15–23. http://jurnal.polgan.ac.id/index.php/remik/article/view/10116

Gunawan, I. (2020). *Keamanan Data : Teori dan Implementasi* (Issue January).

Hakim, E. L., & Utami, F. H. (2014). *Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4*. *10*(1), 1–7. http://jurnal.unived.ac.id/index.php/jmi/article/download/226/203

Hasugian, A. H. (2017). *Implementasi Algoritma Hill Cipher*. *August 2013*, 115–122.

Khan, A. (2015). *PRACTICAL*.

Niswati, Z. A. I. (2012). *STEGANOGRAFI BERBASIS LEAST SIGNIFICANT BIT (LSB) Abstrak . Penelitian ini bertujuan untuk menerapkan metode LSB untuk menyisipkan pesan gambar ke gambar grayscale . Hal ini diperlukan karena sering terjadi bahwa pesan gambar dikirim adalah pesan rahasi*. *5*(2), 181–191.

Nurnaningsih, D., & Permana, A. A. (2018). Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes). *Jurnal Teknik Informatika*, *11*(2), 177–186. https://doi.org/10.15408/jti.v11i2.7811

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2016). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*(1), 20. https://doi.org/10.30872/jim.v10i1.23

Primartha, R. (2011). Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES). *Sriwijaya Journal of Information Systems*, *3*(2).

Ridwan, M. K., Pattipeilohy, W. F., & Sanwani, S. (2020). Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (Dct) Pada Perusahan Alat Berat. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *5*(2), 177–182. https://doi.org/10.33480/jitk.v5i2.1033

Saputra, D. A., & Kusumaningsih, D. (2018). *IMPLEMENTASI KEAMANAN DATABASE MENGGUNAKAN ALGORITMA AES-192 PADA PT GURITA LINTAS SAMUDERA*.

1(3), 884–888.

Sukarno, A. S. (2013). Pengembangan Aplikasi Pengamanan Dokumen Digital Memanfaatkan Algoritma Advance Encryption Standard, RSA Digital Signature dan Invisible Watermarking. *Prosiding Seminar Nasional Aplikasi Teknologi Informasi (SNATI) 2013*, 1–8, ISSN:1907-5022.

Telaah, I., Aspek, K., & Arah, D. A. N. (2018). *Industri 4.0: telaah klasifikasi aspek dan arah perkembangan riset*. *13*(1), 17–26.