Seminar Nasional Inovasi dan Pengembangan Teknologi Terapan (SENOVTEK)
Cilacap, 20 Oktober 2022; pp: 53-61

Pengamanan File Lampiran Pada Email Berbasis TLS Menggunakan Algoritma AES dan LSB

Security of Attachment Files in TLS-Based Emails Using AES and LSB Algorithms

Lekso Budi Handoko[1*], Chaerul Umam[2]
[1,2] Program Studi Teknik Informatika, Universitas Dian Nuswantoro
Email: [1]handoko@dsn.dinus.ac.id, [2]chaerul@dsn.dinus.ac.id

*Penulis korespondensi: **handoko@dsn.dinus.ac.id**

ABSTRAK

Seiring dengan berkembangnya era teknologi pada dunia digital yang semakin pesat, semakin berkembang pula kejahatan yang mungkin terjadi dalam dunia digital. Salah satu permasalahan yang cukup berbahaya adalah terjadinya pencurian. Pada dunia digital, pencurian data sangat mungkin terjadi, termasuk pencurian data yang penting bahkan tidak penting sekalipun. Penelitian ini akan membahas terkait pencurian data yang dapat terjadi pada proses pengiriman email. Pihak server email seperti Google, dengan produknya yaitu Gmail, memanfaatkan *Transport Layer Security* (TLS) sebagai sistem keamanannya dan menghasilkan sebuah aplikasi yang dapat dipergunakan untuk itu. Tetapi, ternyata sistem keamanan tersebut tidak dapat bekerja dengan optimal jika salah satu dari penerima atau pengirim tidak menggunakan TLS sebagai sistem keamanannya. Kriptografi dan Steganografi merupakan metode yang dapat memaksimalkan fungsi dari pengamanan data email tersebut. Pada penelitian ini, digunakan *Advanced Encryption Standard* (AES) sebagai metode dari Kriptografi, dan *Least Significant Bit* (LSB) yang merupakan metode dari Steganografi. Salah satu hal baik yang didapat dari digunakannya LSB adalah LSB tidak menggunakan terlalu banyak proses komputasi, yang dimana hal ini akan meringankan kinerja perangkat yang juga akan melakukan proses AES. Hasil yang didapat dari penelitian ini adalah proses pengamanan data pada email yang memanfaatkan AES dan LSB berhasil mengantisipasi kekurangan dari penggunaan TLS.

Kata kunci: *Email, Transport Layer Security, Advanced Encryption Standard, Least Significant Bit*

ABSTRACT

Along with the development of the technological era in the increasingly rapid digital world, the crimes that may occur in the digital world are also growing. One of the problems that is quite dangerous is the occurrence of theft. In the digital world, data theft is very possible, including the theft of important or even unimportant data. This study will discuss data theft that can occur in the process of sending email. Email servers such as Google, with their product, Gmail, use Transport Layer Security (TLS) as a security system and produce an application that can be used for it. However, it turns out that the security system cannot work optimally if one of the recipients or senders does not use TLS as a security system. Cryptography and Steganography are methods that can maximize the function of securing the email data. In this research, Advanced Encryption Standard (AES) is used as a method of Cryptography, and Least Significant Bit (LSB) which is a method of Steganography. One of the good things that can be obtained from using LSB is that LSB does not use too many computational processes, which will reduce the performance of devices that will also perform AES processes. The results obtained from this study are the process of securing data on email using AES and LSB successfully anticipates the shortcomings of using TLS.

Keywords: email, transport layer security, advanced encryption standard, least significant bit.

1. PENDAHULUAN

Teknologi terus berkembang dari tahun ke tahun, seiring dengan perkembangannya tersebut, tingkat bantuan yang diberikan teknologi kepada manusia juga semakin meningkat. Salah satu perkembangan teknologi yang paling terasa manfaatnya adalah perkembangan teknologi pada bidang komunikasi sebagai sarana pertukaran informasi. Ada beberapa faktor yang merupakan pengaruh dalam perkembangan teknologi, beberapa faktor tersebut adalah: kecepatan jaringan internet yang meningkat, biaya yang perlu dikeluarkan untuk membayar tagihan internet menurun, dan semakin luas jangkauan internet yang bisa digunakan dimanapun dan kapanpun dengan mudah terlebih bisa digunakan dengan hanya menggunakan *smartphone* saja. Beberapa faktor tersebutlah yang menjadikan pengguna teknologi dan internet semakin meningkat setiap tahunnya. Peningkatan penggunaan teknologi dan internet tersebut juga dibarengi dengan naiknya tingkat kejahatan internet yang terjadi. Dimana kejahatan tersebut dilakukan oleh pihak-pihak yang tidak bertanggung jawab dengan tujuan untuk kepentingan diri sendiri. Salah satu jenis kejahatan pada internet yang akan dibahas pada penelitian ini adalah tindakan *Phising. Phising* merupakan suatu kegiatan kejahatan internet dengan tujuan untuk mencuri data pribadi dari korban [1]. Informasi pribadi yang bersifat privasi atau bahkan sangat rahasia, dapat menjadi ancaman yang berbahaya bagi korban *phising*. Jika korban *phising* merupakan suatu instansi atau organisasi tertentu, dampak kerugian yang akan diakibatkan dari Tindakan *phising* tersebut akan semakin besar.

Saat ini, email merupakan salah satu media pertukaran informasi yang cukup penting hingga wajib dimiliki oleh perorangan bahkan instansi. Seringnya pertukaran informasi rahasia, termasuk kalimat hingga media yang dibagikan dapat bersifat sangat rahasia [2]. Penyedia layanan email saat ini sudah sangat mengerti bahwa bentuk perlindungan terhadap keamanan data dan komunikasi pelanggannya sangat dibutuhkan, sehingga mereka juga mengembangkan sistem keamanan khusus untuk jasa situs email yang mereka sediakan. Salah satu jenis metode pengamanan yang banyak digunakan oleh penyedia layanan email adalah dengan menggunakan TLS [3][5]. Salah satu penyedia layanan email yang terkenal seperti Google, dengan produknya yaitu Gmail, juga menggunakan TLS sebagai metode untuk melindungi email penggunanya.

TLS atau *Transport-Layer Security* adalah suatu sistem yang memanfaatkan fase transit untuk melindungi email penggunanya [3]. TLS merupakan suatu teknologi yang membantu mengamankan dua pihak yang saling berkomunikasi melalui jaringan internet. Semua sesi kegiatan pengiriman email yang melalui SSL telah dienkripsikan dan hal tersebut membuat email semakain terjaga keamanannya. Pengamanan komunikasi melalui jaringan internet tidak hanya cukup jika pengamanan dilakukan hanya pada satu komputer, tetapi juga sebaikan proses pengamanan dilkakukan oleh antar dua komputer berbeda yang sedang saling berkomunikasi. Proses pengamanan yang dilakukan pada dua komputer jauh lebih penting karena aka nada lebih banyak ancaman kejahatan internet yang dating. Akan tetapi, masih ada kekurangan pada TLS yang digunakan oleh Gmail, yaitu sistem pengamanan TLS masih terbatas penggunaannya, masih ada beberapa penyedia layanan email yang belum menggunakna TLS baik dari pihak pengirim maupun penerima. Jika hanya salah satu pihak saja yang menggunakan TLS, maka sistem pengamanan TLS tidak akan dapat bekerja dengan baik. Pada Gmail sendiri masih ada sekitar 10% email yang tidak teramankan dengan baik oleh TLS. Cara lain yang dapat mengimbangi kinerja TLS untuk mengamankan data email penggunanya, adalah dengan memanfaatkan sistem pengamanan tambahan yang dapat dilakukan oleh pihak pengirim hingga diterima oleh pihak penerima [5].

Algoritma Kriptografi dan Steganografi merupakan algoritma yang sering digunakan untuk proses pengamanan data. Algoritma Kriptografi melakukan pengamanan data dengan cara mengacak isi pesan (yang bisa dibaca) yang dikirimkan menjadi pesan yang tidak bisa dibaca karena berisi huruf, angka, atau symbol abstrak. Pesan hanya akan dapat dibaca jika penerima pesan memiliki sistem yang dapat mengembalikan kembali pesan acak tersebut menjadi pesan yang dapat dibaca [6][8]. Sedangkan Algoritma Steganografi merupakan metode penyembunyian suatu pesan yang disisipkan pada media. Biasanya, media yang digunakan adlah media gambar. Salah satu Algoritma Kriptografi yang akan digunakan pada penelitian ini adalah Algoritma AES atau *Anvaced Encryption Satndard*. Pada saat ini, AES merupakan salah satu algoritma yang paling aman untuk digunakan dan telah menjadi standard dari proses pengamanan pesan. AES merupakan suatu bentuk pengembangan dari DES (*Data Encryption Standard*) karena telah muncul produk hardware yang mampu memecahkan pengamanan DES [9]. Berita terebut telah disampaikan oleh *National Institute Standards and Technology* pada Tahun 2001 lalu. Secara singkat, cara AES melakukan pengacakan pesan adalah dengan menukar bit pesan dengan bit khusus yang terdapat dalam S-box. Salah

satu keunggulan AES adalah proses enkripsi yang dilakukan AES dapat terjadi lebih cepat jika dibandingan dengan algoritma kriptografi terkenal lainnya seperti RSA dan *Blowfish*.

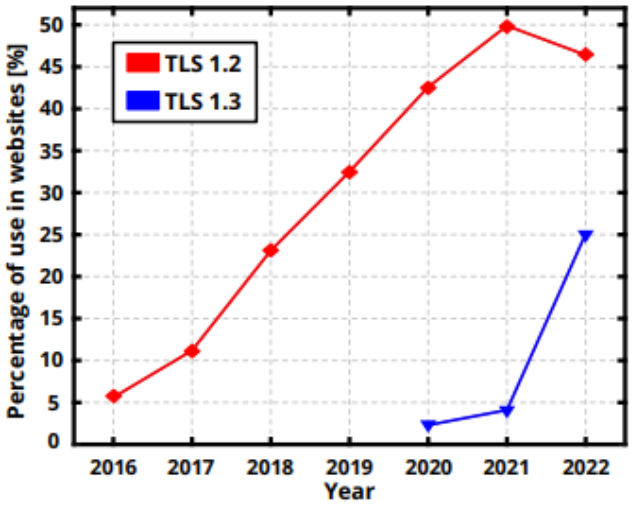
Sementara itu, untuk Alagoritma Steganografi, digunakan Algoritma LSB atau *Least Significant Bit*. Keunggulan yang cukup terkenal dari LSB adalah LSB tidak memiliki proses perhitungan yang rumit sehingga mudah diterapkan. Kelebihan lain yang dimiliki LSB adalah skor *imperceptibility* yang dihasilkan oleh LSB dapat mencapai skor tinggi. Dimana semakin tinggi skor yang dihasilkan, semakin sulit pula pesan yang disisipkan akan terdeteksi [10][13]. Cara kerja Algoritma LSB menyisipkan pesan ke dalam sebuah media adalah dengan menyisipkan bit pesan ke dalam bit terakhir setiap piksel dari media gambar. Proses kombinasi antara penggunaan AES dan LSB adalah, sebelum pesan disisipkan ke dalam media gambar, pesan akan terlebih dahulu diproses menggunakan Algoritma AES sehingga menghasilkan pesan acak. Pesan acak tersebut kemudian disisipkan ke media gambar yang digunakan.

Pada tahun 2018, Niria Laila dan Anita Sindar R. M. S [14] melakukan eksperimen yaitu mengimplementasikan Algoritma LSB pada media citra. Pada proses penyandian dan penyisipan pesan ke dalam citra, digunakan Metode *Affine Cipher*. Pada eksperimen ini, pesan yang dapat disisipkan hanya pesan yang memiliki format *.txt*, dan media citra yang digunakan harus memiliki format *bitmap* (BMP) dan JPEG. Hasilnya, dibandingkan antara media yang sama (sebelum dan sesuah disisipkan pesan), pada tampilan luar tidak terlihat adanya perbedaan, perbedaan yang terlihat secara kasat mata hanya pada ukuran file citra yang berbeda. Pada eksperimen tersebut, disimpulkan bahwa Algoritma LSB dapat menjadi solusi yang baik untuk melakukan proses penyisipan pesan. Pada tahun 2021, Buha Johannes Simbolon [15] melakukan eksperimen pembuatan aplikasi untuk menyisipkan pesan ke dalam file citra dengan menggunakan Algoritma LSB. Selain menggunakan Algoritma LSB, digunakan juga kombinasi Algoritma Kriptografi RC4 dan Base. Atau lebih dikenal dengan Algoritma Super Enkripsi yang dikombinasikan dengan Algoritma Steganografi LSB dengan melakukan penyisipan bit pesan ke dalah pixel data citra secara acak menggunakan PRNG atau *Pseudorandom Number Generator*. Hasil yang didapat dari eksperimen ini adalah berhasilnya pembuatan aplikasi penyisipan gambar menggunakan Algoritma LSB dengan menghasilkan citra (yang telah disisipkan) dengan hasil maksimal, dibuktikan dengan hasil penerapan sesuai dengan perancangan sistem yang dilakukan. Pada tahun 2018, Dian Novianto dan Yohanes Setiawan [16] mengembangkan aplikasi pengamanan informasi dengan menggunakan Algoritma LSB dan AES. Digunakan dua metode pengujian pada eksperimen tersebut, yaitu pengujian blackbox dan pengujian *fidelity*. Pengujian fidelity merupakan bentuk pengujian yang membandingkan perubahan ukuran gambar antara dua jenis ekstensi berkas gambar yang digunakan. Dua ekstensi itu adalah .png dan .bmp. Kesimpulan yang didapat dari eksperimen tersebut adalah, dengan menggunakan file citra berekstensi .png, terdapat perbedaan ukuran antara citra yang disisipi dengan jumlah karakter yang berbeda. Sementara file citra .bmp tidak memiliki perbedaam ukuran antara citra yang disisipkan dengan jumlah pesan yang berbeda. Tetapi, file berekstensi .bmp menghasilkan ukuran citra yang lebih besar daripada .png. Pada tahun 2018, Angga Aditya Permana dan Desi Nunaningsih [17] merancang aplikasi pengamanan data menggunakan Algoritma Kriptografi AES: *Rijndael*. Algoritma Kriptografi AES: *Rjindael* memiliki keunggulan pada proses pengoperasian yang tidak membutuhkan memori terlalu besar serta keefisiensian waktu yang diperlukan cukup cepat. Hasil pada eksperimen ini adalah berhasilnya dibuat sebuah aplikasi yang dapat melakukan pengacakan pesan dengan menggunakan Algoritma Kriptografi AES.

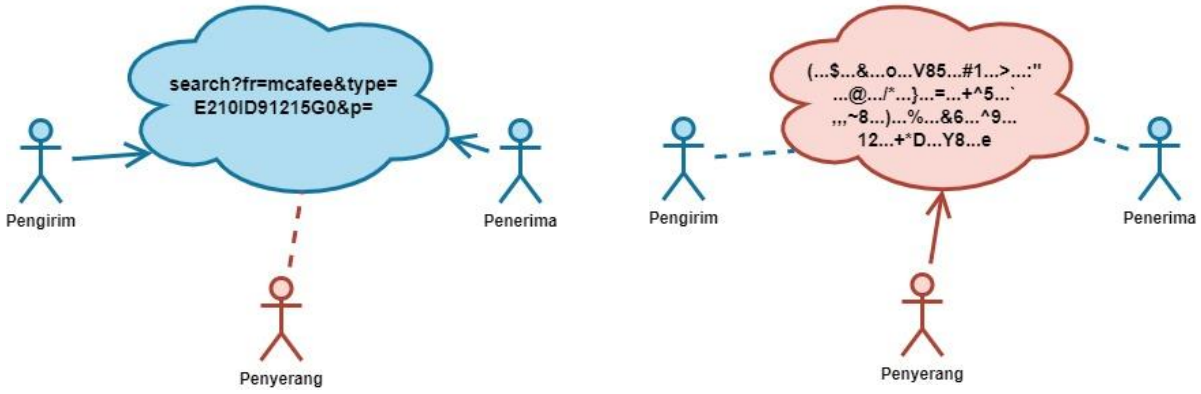
2. METODE PENELITIAN

2.1 Transport-layer Security (TLS)

Transport-layer Security merupakan sistem pengamanan yang telah dikembangkan sejak tahun 1995 dan masih terus berkembang. Saat ini, TLS dengan versi 1.3 merupakan versi paling baru yang tersedia. Hingga saat ini, TLS masih sulit ditemukan kekurangannya (yang sangat fatal). Sistem pengamanan data TLS dengan enkripsi end-to-end yang paling sering digunakan pada jaringan komputer [3], [4]. Gambar 1 menunjukkan ilustrasi dari presentase penggunaan TLS pada situs web, ilustrasi tersebut merupakan 79,4% dari kuartal pertama di tahun 2022. Pada Gambar 2, ditampilkan ilustrasi terkait bagaimana pesan yang terlihat oleh pengirim dan penerima, juga bagaimana penyerang melihat pesan jika pesan yang dikirim diberi pengamanan TLS. Dimana pengirim dan penerima, yang memiliki sistem enkripsi dan dekripsi untuk membaca pesan, sehingga pesan yang muncul akan dapat dibaca. Namun berbeda dengan penyerang, tanpa sistem enkripsi dan dekripsi yang berlaku antara pengirim dan penerima, penyerang hanya akan membaca pesan acak yang tidak dapat diartikan apa maksudnya.



Gambar -1. Presentasi penggunaan TLS pada situs website dari tahun 2016 hingga 2022



(a) Pesan yang terlihat oleh pengirim dan penerima (b) Pesan yang terlihat oleh penyerang

Gambar -2. Ilustrasi dari bagaimana pesan dengan pengamanan TLS terlihat oleh pengirim, penerima, dan penyerang

2.2 Advanced Encryption Standard (AES)

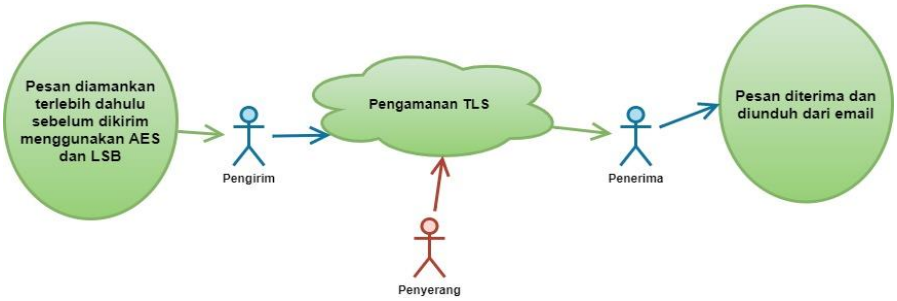
Advanced Enryption Standard atau disingkat AES, merupakan algoritma yang digunakan proses pengamanan data. Cara pengamanan datanya adalah dengan mengacak pesan, dan model pengacakan pesan merupakan tipikal dari proses pengamanan data yang dimiliki oleh Algoritma Kriptografi. Sistem yang digunakan pada Algoritma AES adalah sistem permutasi (P-box) dan substitusi (S-box). Algoritma tidak menggunakan jaringan Feistel seprti yang digunakan oleh block cipher pada umumnya [16], [18]. AES memiliki tiga jenis, yaitu AES-128, AES-192, dan AES-256. Faktor yang membedakan antara jenis AES yang satu dengan yang lainnya adalah berdasarkan panjang kunci yang digunakan oleh setiap jenisnya, dan digunakan sesuai kebutuhan.

2.3 Least Significant Bit (LSB)

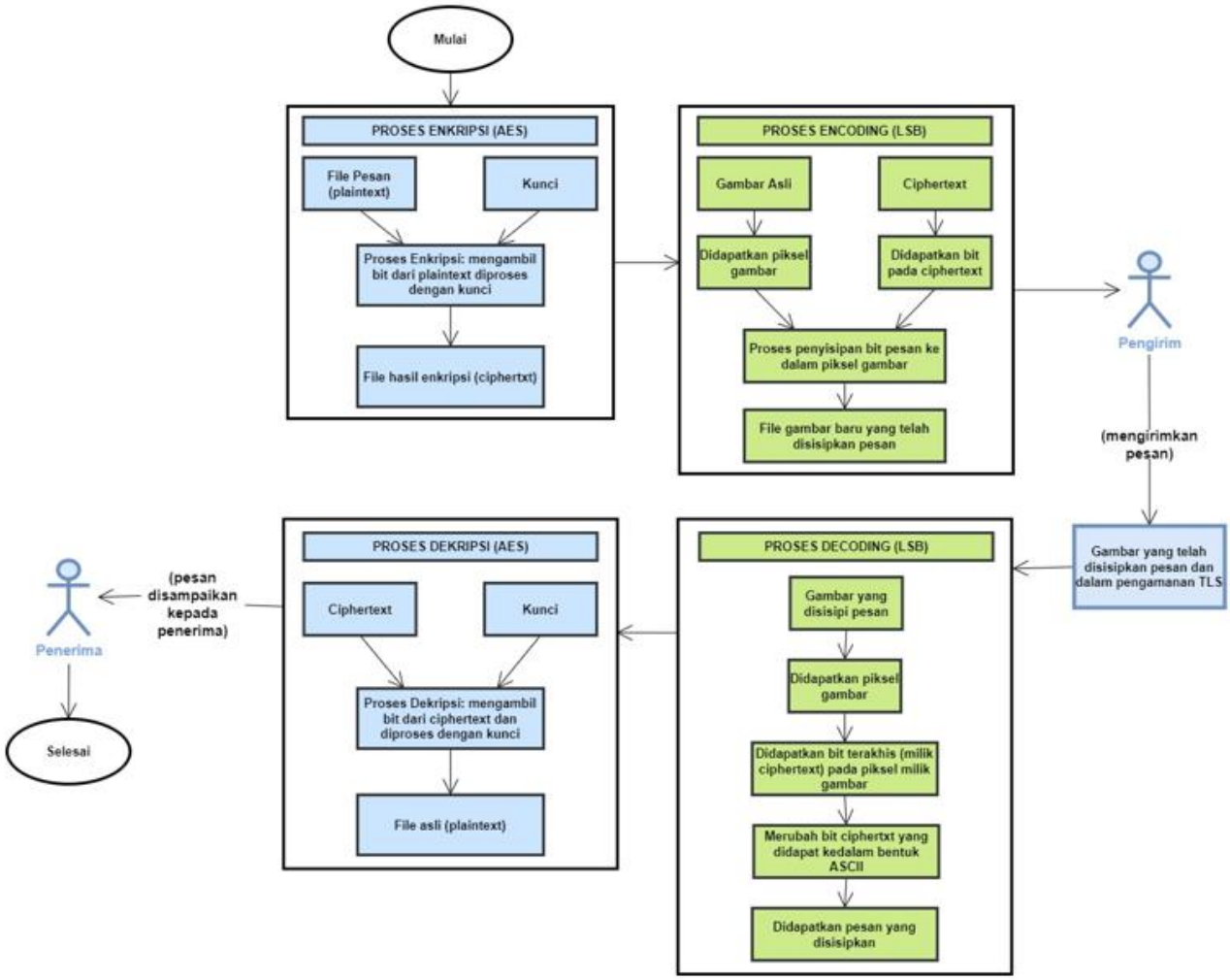
Least Significant Bit atau disingkat LSB, merupakan algoritma pengamanan pesan dengan teknik substitusi yang cara kerjanya adalah dengan menyisipkan pesan ke dalam suatu media, media tersebut bisa gambar atau bahkan video [6]. Penyisipan pesan merupakan tipikal metode pengamanan data dari Algoritma Steganografi. LSB merupakan bagian dari suatu barisan data biner yang memiliki nilai paling kecil, bisa dibilang juga paling tidak memiliki arti. Letak LSB biasanya ada di paling kanan suatu barisan bit. Contohnya, pada bilangan biner dari 215 adalah 11010111, dari bilangan biner tersebut, angka “1” yang berada di paling kanan merupakan bilangan LSB [19].

2.4 Kombinasi antara TLS, AES dan LSB

Sesuai dengan penjelasan sebelumnya, TLS merupakan sistem pengamanan yang dilakukan dari sisi penyedia layanan email. Salah satu kekurangannya adalah, jika pihak penerima tidak menggunakan sistem pengamanan TLS, makan TLS tidak dapat bekerja mengamankan pesan dari serangan kejahatan internet. Cara untuk mengantisipasi terjadinya hal tersebut adalah dengan mengkombinasikan sistem pengamanan dengan ditambahkan metode AES dan LSB yang berasal dari pihak pengirim. Gambar 3 menampilkan ilustrasi perancangan sistem yang akan dibuat.



Gambar -3. Ilustrasi perancangan sistem penggunaan TLS, AES dan LSB



Gambar -4. Ilustrasi proses kombinasi antara AES, LSD dan TLS dari awal hingga akhir

Berdasarkan ilustrasi yang ditampilkan pada Gambar 3, sebelum pesan dikirim oleh pengirim, terlebih dahulu pesan diamankan menggunakan Algoritma AES dan LSB. Kemudian, jika pengamanan TLS bekerja, maka pesan akan mendapatkan pengamanan ganda. Tetapi, jika pengamanan TLS tidak bekerja, pesan tetap dapat terlindungi karena sebelumnya telah diamankan terlebih dahulu menggunakan AES dan LSB.

Berdasarkan Gambar 4, sebelum pesan dikirimkan oleh pengirim, pesan terlebih dulu dilakukan proses enkripsi AES. Selanjutnya, pesan yang telah dienkripsi dan menjadi Ciphertext disisipkan ke dalam gambar dengan menggunakan Algoritma LSB. Gambar yang telah disisipi oleh pesan itulah yang akan dikirimkan oleh pihak pengirim ke pihak menerima melalui email. Melalui sistem email, pesan yang dikirimkan akan dilindungi menggunakan pengamanan TLS sampai diterima oleh pihak penerima. Kemudian pihak penerima menerima pesan tersebut yang melakukan proses decoding dan dekripsi supaya dapat membaca pesan yang dikirim.

2.5 Dataset Citra

Digunakan data citra yang didapatkan dari *Computer-Aided Engineering Website* milik *University of Wisconsin-Madison*. Digunakan sebanyak 6 gambar yang akan digunakan sebagai media penyisipan pesan. Media gambar yang digunakan merupakan media gambar berwarna RGB yang memiliki ekstensi .png. Proses penyisipan pesan akan dilakukan pada layer berwarna biru (*blue*). Gambar 5 menampilkan sampel data citra yang digunakan.

citra1.png citra2.png citra3.png citra3.png citra4.png citra5.png

Gambar -5. Sampel data citra yang akan digunakan sebagai media penyisipan pesan

3. HASIL DAN PEMBAHASAN

3.1 Analisa pada proses AES dan LSB

Digunakan kunci “Angka 2 ribu 18” dan ukuran citra sebesar 512*512 piksel. Tabel 1 di bawah ini menunjukkan nama file berisi pesan yang disisipkan ke dalam media citra yang disediakan. Beserta dengan ukuran file pesan dan gambar dalam KB.

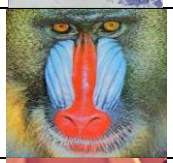
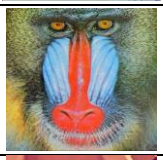
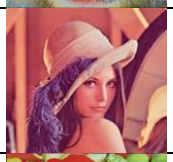
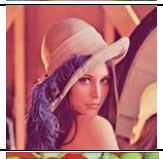
Tabel -1. Analisa proses AES dan LSB

No	Nama Citra	Nama File	Ukuran citra (KB)	Ukuran file (KB)	Waktu Keseluruhan (detik)
1	citra1.png	file1.pdf	451	30.51	3.10
2	citra2.png	file2.pdf	637	7.95	1.51
3	citra3.png	file3.txt	513	9.51	1.72
4	citra4.png	file4.txt	539	19.72	2.16
5	citra5.png	file5.jpg	173	30.81	3.14
6	citra6.png	file6.jpg	186	22.23	2.40

3.2 Pengujian MSE dan PSNR

Proses pengamanan data menggunakan LSB diuji dengan menggunakan perhitungan MSE dan PSNR. Objek yang diuji adalah citra yang telah disisipi oleh pesan. Dari dilakukannya pengujian tersebut, akan didapatkan nilai yang dapat memberitahu seberapa kuat proses pengamanan yang dilakukan. Proses pengamanan akan dinilai kuat jika nilai yang dihasilkan akan semakin kecil. Nilai PSNR merupakan nilai yang akan memberitahukan hasil seberapa kecil kemungkinan sebuah citra akan dicurigai disisipi oleh pesan. Pada Tabel 2 ditunjukkan hasil dari pengujian penyisipan pesan ke dalam gambar menggunakan LSB dengan menggunakan perhitungan MSE dan PSNR.

Tabel -2. Hasil tampilan citra sebelum dan sesudah disisipi citra beserta hasil nilai MSE dan PSNR

No	Citra Asli	Citra setelah disisi pesan	Nilai MSE	Nilai PSNR
1			0.1552	56.2222
2			0.0403	62.0831
3			0.0487	61.2540
4			0.1001	58.1243
5			0.4695	51.4145
6			0.3405	52.8099

3.3 Pengujian Keamanan Tambahan

Tabel -3. Hasil Pengujian Keamanan

No	Nama File	Diamankan dengan AES dan LSB	Diamankan dengan TLS	Keterangan
1	file1.pdf	Ya	Tidak	Pengamanan TLS gagal pada domain yahoo.co.jp
2	file1.pdf	Tidak	Tidak	Pengamanan AES-LSB gagal pemilihan file tidak menggunakan file explorer default
3	file2.pdf	Ya	Tidak	Pengamanan TLS gagal pada domain yahoo.co.jp
4	file2.pdf	Tidak	Tidak	Pengamanan AES-LSB gagal pemilihan file tidak menggunakan file explorer default
5	file3.txt	Ya	Tidak	Pengamanan TLS gagal pada domain yahoo.co.jp
6	file3.txt	Tidak	Tidak	Pengamanan AES-LSB gagal pemilihan file tidak menggunakan file explorer default
7	file4.txt	Ya	Tidak	Pengamanan TLS gagal pada domain yahoo.co.jp
8	file4.txt	Tidak	Tidak	Pengamanan AES-LSB gagal pemilihan file tidak menggunakan file explorer default
9	file5.jpg	Ya	Tidak	Pengamanan TLS gagal pada domain yahoo.co.jp
10	file5.jpg	Tidak	Tidak	Pengamanan AES-LSB gagal pemilihan file tidak menggunakan file explorer default
11	file6.jpg	Ya	Tidak	Pengamanan TLS gagal pada domain yahoo.co.jp
12	file6.jpg	Tidak	Tidak	Pengamanan AES-LSB gagal pemilihan file tidak menggunakan file explorer default

Selanjutnya dilakukan lagi pengujian terhadap proses pengamanan terhadap pesan yang dikirim. Pihak Google untuk produk Gmailnya, memberitahukan beberapa list dari domain yang tidak diamankan menggunakan pengamanan TLS, salah satunya adalah domain yahoo.co.jp. Pada Tabel 3 ditampilkan hasil pengiriman pesan ke domain yahoo.co.jp. Berdasarkan Tabel 2, ditampilkan hasil dari pengujian dengan dan tanpa pengamanan AES dan LSB pada pesan yang dikirim tanpa pengamanan TLS. Meskipun pesan tidak atau gagal mendapatkan perlindungan dari TLS, pesan yang telah melalui proses AES dan LSB dapat tetap terlindungi isi pesannya.

4. KESIMPULAN

Berdasarkan dari penelitian yang telah dilakukan, telah dihasilkan sebuah aplikasi yang dapat melakukan proses pengamanan tambahan pada pesan yang akan dikirim melalui email dengan menggunakan Algoritma Kriptografi AES dan Steganogradi LSB didapatkan hasil bahwa, pada percobaan pengiriman email berisi gambar yang telah disisipkan pesan ke domain yang tidak mendapat perlindungan TLS, pesan tersebut tetap dapat terlindungi isi kerahasiaan pesannya karena pesan telah mendapat perlindungan dari penggunaan AES dan LSB. Dari 60 kali percobaan yang dilakukan, 54 diantaranya berhasil dan 6 diantaranya tidak berhasil. Percobaan yang tidak berhasil dapat terjadi karena pesan yang dikirim melalui email menggunakan file explorer default pada tahap pemilihan file dan citra. Untuk penelitian selanjutnya, dapat dilakukan peningkatan kapasitas file sehingga dapat menampung payload data lebih dari 32 KB. Di sisi lain, aplikasi dapat dibuat lebih kompleks dengan menampilkan fitur enkripsi dekripsi file misalnya pada fitur export data melalui excel.

UCAPAN TERIMA KASIH

Penelitian ini merupakan luaran dari Penelitian Dasar Terapan Perguruan Tinggi (PDPT) Tahun 2022 sesuai SK dari Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM) Universitas Dian Nuswantoro.

DAFTAR PUSTAKA

[1] W. Khan, A. Ahmad, A. Qamar, M. Kamran, and M. Altaf, “SpoofCatch: A Client-Side Protection Tool Against Phishing Attacks,” *SECURITY*, no. April, pp. 65–74, 2021.

[2] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, “Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting,” *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[3] V. Frost, D. Tian, C. Ruales, V. Prakash, P. Traynor, and K. R. B. Butler, “Examining DES-based cipher suite support within the TLS ecosystem,” *AsiaCCS 2019 - Proc. 2019 ACM Asia Conf. Comput. Commun. Secur.*, pp. 539–546, 2019.

[4] U. Banerjee, S. Das, and A. P. Chandrakasan, “Accelerating post-quantum cryptography using an energy-efficient TLS crypto-processor,” *Proc. - IEEE Int. Symp. Circuits Syst.*, vol. 2020-October, pp. 1–5, 2020.

[5] M. Alwazzeh, S. Karaman, and M. N. Shamma, “Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat,” *J. Cyber Secur. Mobil.*, vol. 9, pp. 449–468, 2020.

[6] C. Irawan, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, “Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption,” in *International Conference on Informatics and Computational Sciences (ICICoS)*, 2017.

[7] Sangeeta and E. A. Kaur, “A Review on Symmetric Key Cryptography Algorithms,” *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 358–362, 2017.

[8] C. Irawan, D. R. I. Moses Setiadi, E. H. Rachmawanto, C. A. Sari, and M. Doheir, “Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security,” in *Journal of Physics: Conference Series*, 2019, vol. 1201, no. 1.

[9] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, “A performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size,” in *International Seminar on Application for Technology of Information and Communication*, 2017, no. October 2017.

[10] C. A. Sari, E. H. Rachmawanto, and E. J. Kusuma, “Good Performance Image Encryption Using Selective Bit T-DES on Inverted LSB Steganography,” *J. Ilmu Komput. dan Inf.*, vol. 12, no. 1, pp. 41–29, 2019.

[11] Lindawati and R. Siburian, “Steganography Implementation on Android Smartphone Using the LSB (Least Significant Bit) to MP3 and WAV Audio,” *Proc. - ICWT 2017 3rd Int. Conf. Wirel. Telemat.*

2017, pp. 170–174, 2017.

[12] F. Al Isfahani and F. Nugraha, "Implementasi Steganografi LSB dengan Enkripsi Base64 Pada Citra dengan Ruang Warna CMYK," *Sci. Comput. Sci. Informatics J.*, pp. 1–8, 2019.

[13] E. J. Kusuma, O. R. Indriani, C. A. Sari, E. H. Rachmawanto, and D. R. I. M. Setiadi, "An imperceptible LSB image hiding on edge region using des encryption," in *Proceedings - 2017 International Conference on Innovative and Creative Information Technology: Computational Intelligence and IoT, ICITech 2017*, 2018, vol. 2018-Janua.

[14] N. Laila and A. S. Rms, "IMPLEMENTASI STEGANOGRAFI LSB DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA Implementation of LSB Steganography with Vigenere Cipher Encryption in Image," *Comput. Sci. Informatics J.*, vol. 1, no. 2, pp. 47–58, 2018.

[15] B. J. Simbolon, "Steganografi Penyisipan Pesan Pada File Citra Dengan Menggunakan Metode LSB (Least Significant Bit)," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 1, pp. 1–6, 2021.

[16] D. Novianto and Y. Setiawan, "Aplikasi Pengamanan Informasi Menggunakan Metode Least Significant Bit (Lsb) dan Algoritma Kriptografi Advanced Encryption Standard (AES)," *J. Ilm. Inform. Glob.*, vol. 9, no. 2, pp. 83–89, 2019.

[17] A. A. Permana and D. Nurnaningsih, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *J. Tek. Inform.*, vol. 11, no. 2, pp. 177–186, 2018.

[18] C. A. Sari, E. H. Rachmawanto, and E. J. Kusuma, "Good Performance Images Encryption Using Selective Bit T-Des on Inverted Lsb Steganography," *J. Ilmu Komput. dan Inf.*, vol. 12, no. 1, p. 41, 2019.

[19] M. T. Elkandoz, W. Alexan, and H. H. Hussein, "Double-Layer Image Security Scheme with Aggregated Mathematical Sequences," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2019, pp. 1–7.