ANTIVIRUS: Jurnal Ilmiah Teknik Informatika (p – ISSN: 1978 – 5232; e – ISSN: 2527 – 337X)
Vol. 16 No. 1 Mei 2022, pp. 25 – 38

OPTIMASI TEKNIK STEGANOGRAFI AMELSBR PADA EMPAT *BIT* TERAKHIR DENGAN *COVER IMAGE* BERWARNA

Muhammad Alfin Fikri[1)], F.X. Ferdinandus[2)]
[1, 2)]Fakultas Teknologi Informasi, Institut Sains dan Teknologi Terpadu Surabaya (ISTTS),
Surabaya, Jawa Timur 60284, Indonesia
e-mail: fikrialfin@gmail.com[1)], ferdi@stts.edu[2)]

Abstrak* :** *Pertumbuhan transmisi data yang dinamis di era modern membutuhkan pertukaran data yang aman. Biasanya yang digunakan untuk pertukaran data yang aman adalah steganografi atau kriptografi. Steganografi adalah teknik yang robust untuk melindungi data tersembunyi dari akses yang tidak sah (unauthorized access) dengan memasukkannya ke dalam cover object, tanpa mengubah kualitas dari cover object.* ***Tujuan: *Penelitian ini mengusulkan optimasi teknik steganografi Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) dengan memodifikasi setidaknya empat bit yang akan diganti. Sayangnya, steganografi seringkali terdeteksi oleh mata manusia, apalagi jika mengalami modifikasi penggantian bit. Untuk mengatasi masalah ini, peneliti telah mengoptimalkan AMELSBR pada empat bit terakhir dengan Cover Image Berwarna.* ***Metode:*** *Secara khusus, peneliti mengoptimalkan AMELSBR sehingga dapat menggunakan 4 bit terakhir dalam cover image. Peneliti membagi skema percobaan berdasarkan per bit yang diganti, yaitu satu bit, dua bit, tiga bit, dan empat bit. Cover object yang tercakup dalam penelitian ini adalah citra berwarna (cover image), yang dibagi menjadi empat kelas: citra abstrak, citra pemandangan, citra binatang, dan citra buah.* ***Hasil:*** *Peneliti dapat meminimalkan Mean Squared Error menjadi setidaknya 1 dan Rasio Peak-to-Signal menjadi setidaknya di bawah 35 dB dalam pekerjaan ini. Peneliti juga menguji citra stego (stego image) sebagai hasil akhir dari proses steganografi AMELSBR menggunakan uji kecerahan, kontras, pengubahan ukuran, noise, dan blur.* ***Kesimpulan:*** *Hasil eksperimen telah membuktikan bahwa AMELSBR yang dioptimalkan sebagai teknik steganografi dapat diandalkan untuk penyisipan teks pada cover image tanpa menggunakan kriptografi sebagaimana dimaksud dalam penggunaan standar.*

Kata Kunci—AMELSBR, Steganografi, Mean Squared Error, Peak-to-Signal Error

Abstract* :** *The dynamic growth of data transmission in the modern age needs a safe interchange of data. Usually used for secure data exchange is steganography or cryptography. Steganography is a well-established technique for protecting hidden data from unauthorized access into a cover object in such a fashion that it is easily imperceptible to human eyes.* ***Purpose: *This work proposes an optimization towards Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) by modifying at least four bits to be replaced. Sadly, steganography is often detectable by human eyes, especially if underwent such bit replacement modification. To solve this problem, we have optimized AMELSBR on the last 4 bits with Color Cover Image.* ***Method:*** *Specifically, we optimized AMELSBR so it can use the last 4 bit in cover image. We divided the experiment scheme based on per replaced bit, namely one bit, two bits, three bits, and four bits. The object covered in this work is colored images, divided into four classes: abstract images, landscape images, animal images, and fruit images..* ***Results:*** *We were able to minimize Mean Squared Error into at least 1 and Peak-to-Signal Ratio into at least under 35 dB in this work. We also tested the stego images as the end result of the AMELSBR steganography process using brightness, contrast, resize, noise, and blur.* ***Conclusion:*** *The experimental results have proven that AMELSBR which is optimized as a steganographic technique can be relied upon to insert text on the cover image without using cryptography as intended in standard use.*

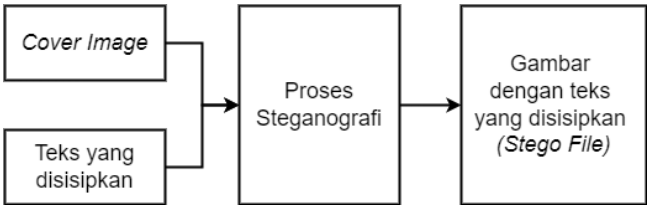
Keywords—AMELSBR, Steganography, Mean Squared Error, Peak-to-Signal Error

I. PENDAHULUAN

PESAN yang terenkripsi dalam kriptografi biasanya menggunakan kunci enkripsi yang hanya diketahui oleh pengirim dan penerima [1], [2]. Dengan demikian, tidak ada yang bisa membaca pesan kecuali yang mempunyai kunci enkripsi [3]. Di sisi lain, transmisi pesan terenkripsi mungkin dengan segera menarik kecurigaan peretas, dan pesan terenkripsi dapat dicegat, diserang, atau diterjemahkan dengan cepat. Pendekatan steganografi dirancang untuk mengatasi kekurangan sistem kriptografi. Teknik steganografi

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

adalah seni dan ilmu berkomunikasi untuk menyembunyikan keberadaan komunikasi dalam media tertentu [4]. Media yang pertama kali digunakan dengan steganografi adalah citra. Namun, steganografi juga dapat digunakan untuk suara, teks, dan bahkan video [5]. Metode steganografi secara keseluruhan digambarkan pada Gambar 1 sebagai diagram blok sederhana. Sebagai masukan untuk prosedur steganografi, dibuat data awal *(cover image)* dan pesan teks yang akan disisipkan. Prosedur ini kemudian pada proses menggunakan teknik steganografi lalu menghasilkan output dalam sebuah citra dengan pesan teks yang disematkan ke dalam citra *(stego image)*.



Gambar 1. Alur Steganografi secara Umum

Least Significant Bit (LSB) adalah pendekatan umum untuk menjalankan teknik steganografi karena konsep yang dimiliki cukup sederhana [6]. Beberapa atau semua *byte* dalam *bit* ke-8 dari *cover image* dapat diubah menjadi *bit* untuk memasukkan pesan tersembunyi. Cara kerja LSB relatif mudah, mula-mula dengan mengubah citra dan pesan menjadi *bit biner*. Lalu, LSB mencari *bit* yang tidak signifikan dan mengganti *bit* tersebut kedalam *bit* pesan yang telah diubah menjadi *biner*. Namun, pada kasus LSB hanya mengganti *bit* yang paling belakang. Pendekatan LSB memiliki keuntungan sebagai berikut: LSB relatif cepat dan lugas dan menjadi teknik yang bekerja dengan baik dengan *cover image* dengan warna *grayscale*. Selain itu, pendekatan ini juga rentan terhadap perubahan citra, dan sering menghasilkan *noise* dan *cropping* yang berlebihan pada hasil *stego image* [7].

Metode steganografi *Adaptive Minimum Error Least Significant Bit Replacement* (AMELSBR) adalah varian dari metode LSB. Pada penelitian terdahulu yang membahas tentang AMELSBR hanya berfokus kepada ketahanan kualitas citra yaitu di *bit* 1 terakhir yang diganti dan penelitian ini mencoba untuk meneliti jika dua hingga empat *bit* terakhir diganti masih relevan pada teknik AMELSBR. Maka dari itu, peneliti bereksperimen pada satu *bit*, dua *bit*, tiga *bit*, dan empat *bit* terakhir yang akan diganti. Penggantian bit ini lantas menjadi empat skema penelitian. Pertimbangan dari pergantian *bit* sedikit demi sedikit ini kemudian dijabarkan menjadi empat skema penelitian. Nilai biner yang dibuat oleh sisipan teks tidak akan melebihi nilai biner yang diberikan oleh *cover image*. Selanjutnya, format ekstensi penyisipan teks adalah teks biasa (TXT), sedangkan format ekstensi *cover image* dan *stego image* dibatasi untuk citra .PNG. Empat skema sendiri merupakan varian *bit* yang akan diganti dari bit pertama hingga varian *bit* keempat. Hasilnya akan dilakukan perbandingan untuk mengetahui bit mana yang paling optimal untuk menyimpan pesan dan mempertahankan gambar.

Penelitian optimasi steganografi ini dilakukan menggunakan teknik AMELSBR. Temuan peneliti adalah, pada *stego image*, tidak ditemukan perbedaan nyata dengan *cover image*. Secara praktis, hasil *stego image* dapat mengurangi dugaan penyisipan pesan tersembunyi pada sebuah citra. Perbedaan ini peneliti temukan dengan melakukan uji ketahanan. *Mean Squared Error* (MSE) pada angka kurang dari satu dan *Peak Signal-to-Noise Ratio* (PSNR) lebih dari 35 dB adalah standar tujuan pengujian untuk menentukan ketahanan manipulasi citra terhadap pesan tersembunyi dalam *stego image*.

Penelitian ini memiliki dua kontribusi utama. Yang pertama adalah mengatasi ketidakseimbangan kualitas *cover image* prosedur steganografi. Setelah dilakukan steganografi, perubahan kualitas citra dapat menimbulkan kecurigaan saat menggunakan *stego image* yang berbeda dari *cover image*. Namun, AMELSBR dapat mengatasi masalah ini. Hasil optimasi AMELSBR terjadi dalam uji ketahanan *stego image*, yang dapat menahan berbagai faktor pengujian, menghasilkan nilai distorsi keseluruhan minimal yang tidak menimbulkan kecurigaan. Selanjutnya, jumlah *bit* yang ditukar pada *cover image* melebihi jumlah substitusi

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

standar AMELSBR, empat bit terakhir. Penelitian ini memberikan empat skema penelitian yang masing-masing mempertimbangkan penggantian per satu *bit*, dua *bit*, tiga *bit*, dan empat *bit* terakhir. Kontribusi kedua adalah peneliti menguji ketahanan teknik AMELSBR yang dioptimalkan dalam menjaga kualitas *stego image* agar tidak menyimpang terlalu jauh dari *cover image*, bahkan setelah dilakukan uji manipulasi citra yang meliputi kecerahan, kontras, ubah ukuran, noise, dan blur.

Studi ini disusun sebagai berikut: Bagian 1 memperkenalkan definisi steganografi, penggunaan AMELSBR, dan kontribusi penelitian. Sementara itu, beberapa penelitian sebelumnya sebagai bahan referensi disajikan pada Bagian 2. Selanjutnya pada Bagian 3, terdapat metodologi penelitian peneliti yang melakukan optimasi pada AMELSBR. Bagian 4 memberi gambaran hasil eksperimen dan pembahasan optimasi AMELSBR, dilanjutkan dengan Bagian 5 yang berisi kesimpulan.

II. TINJAUAN PUSTAKA

Praktik penyembunyian materi informasi dalam konten multimedia seperti citra, audio, dan video, disebut sebagai *Embedding* dalam steganografi [8], [9]. Steganografi dan kriptografi berbeda dalam cara steganografi menyematkan informasi sementara kriptografi menyimpan informasi. Sulit untuk mengambil informasi tanpa proses yang dikenali dalam steganografi karena elemen tersembunyi. Steganalisis adalah proses pendeteksian steganografi [4]. Dalam steganalisis, warna gambar yang sangat baik dan kapasitas data yang sesuai adalah dua kualitas penting dari pendekatan steganografi.

MSE dan PSNR adalah dua teknik validasi dalam steganalisis [10]. Bagian ini membahas berbagai penelitian sebelumnya yang mengusulkan menggunakan teknik validasi MSE dan PSNR. Selanjutnya, bagaimana keduanya digunakan untuk memvalidasi *stego image*. Penelitian sebelumnya juga menyarankan bahwa *cover image* dengan ekstensi .PNG harus digunakan sebagai pengganti .JPG atau .BMP.

A. *Penelitian Terdahulu*

Pada tahun 2018, Manaseer dkk. bereksperimen dengan steganografi menggunakan standar LSB. Manaseer dkk. memilih tiga foto hitam putih (B&W) yang diketahui berukuran 512×512 piksel untuk *cover image*. Melalui uji coba berulang, Manaseer juga memantau MSE, PSNR, dan total *bit* yang diganti. "HelloWorld" adalah pesan teks yang terkandung dalam eksperimen. Meskipun nilai MSE dan PSNR memiliki hasil yang baik (0,00049591 untuk MSE dan 91,1768 dB untuk PSNR), perlu diperhatikan bahwa pesan yang disematkan relatif singkat dan perlu diperluas ke beberapa paragraf [11].

Citra dalam format PNG memiliki *stego image* yang lebih unggul daripada format .JPG dan BMP. Hasil penelitian Arya dan Soni disajikan pada Tabel 1 adalah citra BMP memiliki PSNR tertinggi (53,20 dB) diikuti oleh citra PNG (53,07 dB). Namun, angka dalam MSE lebih baik dibuktikan dengan PNG (0,31) dan BMP (0,31). Sedangkan skor JPG relatif rendah, baik di PSNR (37,68) maupun MSE (11,17). Secara umum, semakin kecil nilai MSE maka nilainya menjadi semakin baik. Namun, semakin besar nilai PSNR maka nilainya menjadi semakin baik [12].

Tabel 1. Ringkasan Hasil Penelitian Arya dan Soni [12]

Format Gambar	PSNR (DB)	MSE
PNG	53,07	0,31
BMP	53,20	0,31
JPG	37,68	11,17

Pada tahun 2020, Alabaichi dkk. mempublikasikan hasil pemanfaatan pendekatan LSB dengan teknik *Secret Map* (SM) dalam proses penyisipan pesan teks. Alabaichi menggunakan total 4 citra berwarna sebagai *cover image*. Alabaichi memisahkan MSE dan PSNR berdasarkan warna dasar RGB: merah (*Red*), hijau (*Green*), dan biru (*Blue*) [13]. Penelitian Alabaichi hanya menggunakan data teks berupa satu kalimat yang diulang sebanyak 50.000 kali untuk setiap karakter. Tabel 2 menggambarkan temuan penelitian Alabaichi

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

dkk, di mana skor MSE terbaik adalah 1,0852 dan hasil PSNR terbesar adalah 47,8098, untuk satuan warna hijau.

Tabel 2. Ringkasan Hasil Penelitian Alabaichi [13]

PSNR (DB)	MSE
R = 47,5509	R = 1,1518
G = 47,8098	G = 1,0852
B = 47,5859	B = 1,1426

Berdasarkan penelitian sebelumnya, dapat disimpulkan bahwa AMELSBR dapat memperbarui dan meningkatkan LSB dalam pendekatan steganografi. Penelitian sebelumnya berusaha untuk mengimbangi hasil AMELSBR dengan menggabungkan LSB dengan berbagai pendekatan lain. Alih-alih LSB digabungkan dengan pendekatan lain, eksperimen ini menggunakan metode AMELSBR terbaru. Penggunaan citra berwarna sebagai *cover image* juga lebih baik untuk implementas daripada *cover image* yang *grayscale*, oleh karena *cover image grayscale* tidak memiliki hasil yang baik dalam pengujian ketahanan dan tidak mengandung fluktuasi *bit* dalam piksel, yang membantu dalam proses steganografi.

Pada penelitian sebelumnya, diusulkan penggunaan MSE dan PSNR untuk memvalidasi hasil steganografi AMELSBR, yang menjadi referensi untuk pekerjaan ini. Selanjutnya, teori yang peneliti ajukan didukung oleh penelitian sebelumnya, di mana nilai MSE terbaik ditunjukkan dari nilai terendah dan di bawah angka satu. Sebaliknya, nilai PSNR terbaik disajikan dari nilai tertinggi dan lebih dari 35 dB. Karena citra secara umum tidak memiliki kompresi citra, peneliti memilih citra dengan kompresi *lossless*, dimana dibuktikan dari penelitian sebelumnya, bahwa kompresi terbaik adalah *cover image* dengan format ekstensi PNG. Kompresi *lossy* dari JPEG dan JPG akan membebani selama proses steganografi.

B. Least Significant Bit

Secara singkat, ide *Least Significant Bit* (LSB) tidak terbatas implementasinya pada steganografi. LSB menggunakan *bit* terkecil atau terlemah dalam urutan biner. *Bit* terkecil umumnya *bit* paling kiri atau paling kanan dalam bilangan bulat biner, tergantung pada arsitektur komputer. Arsitektur disebut sebagai "little-endian" jika LSB terletak di ujung kanan sirkuit biner. Arsitektur disebut sebagai "big-endian" jika LSB terletak di ujung kiri sirkuit biner [14] [15].

Pada penelitian ini, LSB digunakan dalam konteks steganografi. Dalam hal ini, deskripsi keseluruhan adalah teknik steganografi citra yang menyembunyikan pesan dalam citra dengan mengganti *bit* terkecil dari setiap piksel dengan *bit* pesan teks [16]. Jika terdapat citra digital dalam bentuk array piksel 2D, maka setiap piksel memiliki nilai berdasarkan jenis dan kedalamannya. Pada penelitian yang menjelaskan tentang konversi pesan bahwa konversi pesan ke nilai desimal dan selanjutnya ke biner dapat dilakukan menggunakan tabel pengkodean ASCII. Teknik konversi pesan ini kemudian diulang untuk setiap nilai piksel. Setelah mengonversi piksel ke biner, peneliti menggunakan strategi penelitian 1 *bit*, 2 *bit*, 3 *bit*, dan 4 *bit* untuk mengganti setiap *bit* paling tidak signifikan dengan *bit* pesan secara berurutan. Peneliti membalikkan metode untuk memecahkan kode *stego image* yang disandikan. Peneliti mengumpulkan dan menyimpan *bit* terakhir dari setiap piksel, lalu mengelompokkan setiap delapan *bit*. Untuk mendapatkan pesan yang disembunyikan, setiap kelompok ditransformasikan kembali menjadi karakter ASCII [17].

Secara umum, steganografi menyimpan intensitas setiap piksel pada *cover image grayscale* menggunakan 8 *bit*. Bidang *bit* adalah bidang yang dihasilkan oleh *bit* yang sama dari setiap piksel dalam *cover image grayscale*. Jika tekstur acak terjadi pada bidang *bit* yang lebih signifikan, tekstur acak juga akan ditampilkan pada bidang *bit* yang kurang signifikan pada titik yang sama. Akibatnya, area tekstur acak di setiap bidang *bit* yang kurang penting lebih besar daripada tekstur acak di setiap bidang *bit* yang lebih signifikan. Efeknya akan hilang jika pesan tersebut terkandung dalam *bit-plane* tertentu yang bukan yang paling signifikan. Kedua, ketidakpastian tekstur di suatu bidang terus menurun dari bidang *bit* yang paling signifikan ke bidang *bit* yang paling tidak penting. Ketika *k-least significant bit* di setiap piksel dari *cover image* digunakan untuk menyematkan pesan, *k-least significant bit-planes* disajikan dengan tekstur acak, dan derajat tekstur acak dengan cepat bergeser dari *k-bit-plane*. ke bidang *bit* $k - 1$. Akibatnya, fenomena kedua juga akan lenyap.

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

$$TD = \sum_{(i,j)\in W}|x(i,j) - x(i,j+1)| + \sum_{(i\times j)\in W}|x(i,j) - x(i+1,j)| \quad (1)$$

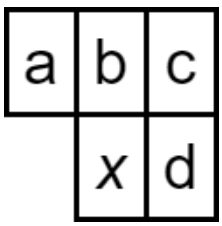
Berdasarkan fungsi densitas pada Persamaan 1, model steganalitik akan diusulkan untuk melakukan *decode* pada *stego image* dari proses LSB. Variabel W menjadi jendela $w \times w$ dalam citra biner. Transisi berarti perubahan 1-ke-0 atau 0-ke-1 dari dua piksel tetangga. *Transition Density* (TD), yang diwakili oleh W, adalah jumlah transisi horizontal dan vertikal di W. Selanjutnya, $x(i,j)$ adalah nilai piksel dari (i,j) . Ketika $w = 5$, TD memiliki *value* [0,40]. Ketika W adalah area konstan (semua 0 atau semua 1), TD memiliki *value* 0.

C. AMELSBR

Intensitas setiap piksel pada *cover image grayscale* direpresentasikan dengan total 256 level. Jika ditanamkan $(k < 8)$ *bit* pesan dalam sebuah piksel, maka diperlukan ubahan *k*-LSB dari piksel yang menghasilkan lebih sedikit kesalahan daripada mengganti *k-bit* lain, dengan kesalahan maksimum $2k - 1$. Ini karena ada $2(8 - k)$ tingkat keabuan dengan nilai yang sama pada *k-bit* paling tidak signifikan sebagai *k-bit* pesan dalam total 256 tingkat keabuan. Untuk mengurangi kesalahan penyematan, peneliti mengganti tingkat piksel dengan yang memiliki kesalahan paling kecil dengan tingkat keabuan asli. Metode sederhana ditawarkan untuk meniadakan kesalahan penyematan. Metode ini akan mengubah $(k + 1)$ LSB dan mencari masalah penyematan. Kemudian, untuk mengganti yang asli, peneliti memilih skala abu-abu dengan lebih sedikit kesalahan penyematan. Fase ini meliputi metode penyesuaian yang disebut metode *Minimum Error Least Bit Replacement* (MELSBR) dan terdiri dari dua bagian. Kesalahan maksimum dapat dibatasi hingga 2 menggunakan pendekatan MELSBR *(k-1)*. Namun, atribut *Adaptive* harus diimplementasikan untuk menjadi *Adaptive Minimum Error Least Bit Replacement* atau AMELSBR.

Pesan harus disisipkan di bagian tekstur acak setiap bidang *bit* untuk mencegah pengaruh atribut *cover image*. Pendekatan steganografi adaptif berdasarkan metode MELSBR disarankan untuk memanfaatkan kekhasan lokal. Pertama, kapasitas penyisipan pesan maksimum untuk setiap piksel pada *cover image* ditentukan. Sebagai contoh, jumlah pesan yang akan disematkan lebih sedikit dari seluruh kapasitas penyisipan yang disediakan oleh *cover image*. Dalam hal ini, pendekatan dispersi ditawarkan untuk mencegah penyematan semua pesan di wilayah lokal. Karena *stego image* pada akhirnya dilihat oleh manusia, sangat bermanfaat untuk menyelidiki sifat-sifat sistem visual manusia (*Human Visual System* atau HVS) [18].

Perubahan pada komponen frekuensi tinggi tidak dapat terdeteksi oleh mata manusia. Komponen frekuensi tinggi yaitu dengan mencirikan tepi dan karakteristik tajam lainnya dalam sebuah citra. Komponen ini menunjukkan bahwa kapasitas *embedding* setiap piksel dipengaruhi oleh fluktuasi tingkat keabuan dari piksel terdekatnya atau piksel tetangga yang sering dinotasikan sebagai x. *Mask* spasial yang digambarkan pada Gambar 2 digunakan untuk menilai varians tingkat keabuan *D* di piksel tetangga *x*.



Gambar 2. Mask Spasial untuk Evaluasi Variasi Nilai Keabuan dari piksel tetangga *x*

Fitur AMELSBR menunjukkan bahwa kapasitas penyisipan setiap piksel ditentukan oleh fluktuasi tingkat keabuan dari piksel terdekat. *Mask* spasial yang digambarkan pada Gambar 2 digunakan untuk menilai fluktuasi tingkat keabuan *D* di sekitar piksel *x*. *D* dinyatakan dalam Persamaan 2 untuk setiap piksel *x*, di mana *a*, *b*, *c*, dan *d* adalah tingkat keabuan dari piksel sekitar *x*.

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

$$D = \max\{a, b, c, d\} - \min\{a, b, c, d\} \quad (2)$$

$$K = \lfloor log_2(D) \rfloor \quad (3)$$

Kapasitas penyisipan *K* dari *x* piksel adalah jumlah *bit* minimum untuk menyimpan nilai *D* dikurangi satu (1). Sehingga *K* dapat dirumuskan dalam Persamaan 3. Yang menjadi perhatian adalah bahwa jumlah pesan rahasia yang disematkan akan meningkat seiring dengan meningkatnya derajat variasi logaritmik. Menurut sifat pencahayaan HVS, semakin besar nilai abu-abu, semakin banyak perubahan yang dilakukan pada nilai abu-abu. Sehingga, hasilnya akan semakin terlihat perubahan kualitas *stego image* dibandingkan dengan *cover image*. Berdasarkan properti ini, Lee dan Chen menetapkan batas atas *U* dari kapasitas penyisipan untuk setiap piksel seperti pada Persamaan 4, di mana *X* adalah nilai abu-abu dari piksel *x* [19].

$$U = \lfloor log_2(X) \rfloor - 1 \quad (4)$$

$$P = \frac{AM}{C} \quad (5)$$

Darwis mencatat perbedaan dan keunggulan algoritma AMELSBR dibandingkan pendahulunya dalam publikasinya [10]. LSB adalah metode steganografi yang sederhana. Pesan yang disisipkan ke dalam *cover image* di bagian akhir bit yang kurang bermakna sehingga modifikasi *cover image* tidak berpengaruh pada hasil akhir *stego image*. Setiap *byte* ukuran citra panjangnya adalah 8 *bit*. *Bit* pesan ditempatkan sebagai *bit* terakhir pada *cover image* menghasilkan perubahan *stego image* yang hampir identik dengan *cover image* yang digunakan. Dalam pendekatan AMELSBR Lee dan Chen, bilangan bulat acak dengan nilai [0,1] dibuat untuk setiap piksel untuk menentukan apakah piksel tersebut dapat digunakan untuk menyisipkan pesan. Prosedur ini dilakukan untuk menyebarkan pesan yang tersembunyi pada *cover image*. Rasio *embedding*, dilambangkan dengan *P*, juga ditentukan dalam Persamaan 5 di mana *AM* adalah jumlah pesan yang akan disematkan dan *C* adalah kemampuan prediktif *embedding* dari *cover image*. Piksel digunakan untuk memasukkan pesan jika nomor acak lebih kecil dari *P*. Jika *cover image* secara tidak sengaja diserang untuk mendapatkan pesan yang disematkan, Lee dan Chen menyisipkan beberapa *bit* acak dalam piksel yang tidak digunakan untuk menyematkan pesan.

Tabel 3. Algoritma AMELSBR menurut Lee dan Chen

1.	Memprediksi kapasitas penyisipan *C* pada *cover image*
2.	Menghitung lebar, tinggi, dan ukuran citra dari *cover image*
3.	Menghitung rasio *embedding*
4.	Memilih secara acak area tersembunyi dari *cover image*, dan masukkan pesan teks
5.	Pindai citra sampul dari kiri atas ke kanan bawah. Untuk setiap *x* piksel di bagian tempat pesan disisipkan, peneliti melakukan langkah-langkah berikut:
	a. Hasilkan bilangan acak *r* dengan $0 \leq r \leq 1$
	b. Menggunakan Persamaan 2 dan 3 untuk mengevaluasi kapasitas penyisipan *(K)* dan batas atas penyisipan *(U)* dari *x*.
	c. Kemudian, ambil $K^* = \min(K, U)$
	d. IF $(r \leq p)$, memasukkan pesan $K^* - bit$ di *bit* signifikan terkecil dari *x*,
	e. menyesuaikan bit $(K+1)^{th}$ serta memeriksa kesalahan penyematan
	f. ELSE, masukkan $\left((r^*100) mod\ K^*\right)$ pesan acak per *bit*.

Beberapa informasi yang digunakan dalam tahap penyisipan diperlukan pula dalam langkah ekstraksi. Ambang batas, jenis pesan, tinggi dan lebar *cover image*, skema enkripsi, strategi kompresi, dan sebagainya adalah bagian dari proses ekstraksi. Sebelumnya, Lee dan Chen memisahkan piksel *cover image* menjadi dua bagian. Yang pertama digunakan untuk menyematkan informasi tersembunyi, sedangkan yang kedua digunakan untuk menyematkan pesan. Komponen pesan tersembunyi dipilih secara acak. Sedangkan bagian

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

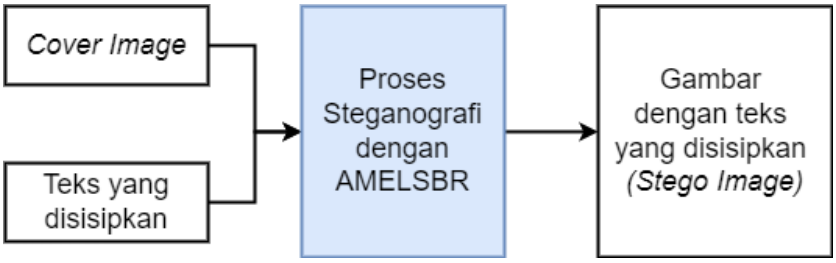
pesan yang disematkan diproses secara berurutan untuk setiap baris. Keuntungan dari skema tersebut adalah bahwa setiap teknik *digital signature* seperti steganografi dapat digunakan pada bagian pesan yang disematkan dan *signature* yang disematkan di wilayah pesan tersembunyi. Dengan menggunakan sistem *digital signature*, penerima dapat mengonfirmasi bahwa pesan tersebut benar. Ringkasan dari penjelasan tersebut dapat digambarkan pada Tabel 3 yang merupakan penggambaran seluruh proses AMELSBR.

III. METODOLOGI PENELITIAN

Bagian bab ini menjelaskan alur eksperimen yang peneliti lakukan pada optimasi AMELSBR. Peneliti membaginya pada proses *encode* dan *decode*.

A. *Optimasi AMELSBR pada Proses Encode*

Gambar 3 menggambarkan diagram blok diagram dari arsitektur sistem peneliti untuk proses *encode*. Menurut Gambar 3, peneliti memasukkan *cover image* dan pesan teks yang akan disisipkan ke dalam proses steganografi menggunakan AMELSBR, sehingga menghasilkan *stego image*. Sebagai tambahan, pesan teks yang dapat dimasukkan ke dalam gambar termasuk pesan teks bebas yang memiliki urutan panjang. Pesan teks yang akan disisipkan adalah lagu kebangsaan Indonesia Raya yang memiliki pengulangan yang panjang sehingga berdampak pada hasil validasi MSE dan PSNR.



Gambar 3. Alur *Encoding* dengan AMELSBR yang dioptimasi

Langkah-langkah AMELSBR yang peneliti optimasi adalah sebagai berikut: Pertama, *cover image* dibagi menjadi beberapa blok berukuran 3 × 3 piksel. Kedua, seperti yang ditunjukkan pada Persamaan 6 dihitung nilai variasi warna, di mana *CV* adalah variasi warna.

$$CV = round\left\{\frac{|C-A|+|A-B|+|B-C|+|C-D|}{4}\right\} \quad (6)$$

$$K = round(|log_2 V|) \quad (7)$$

Ketiga, dengan menggunakan Persamaan 7 kapasitas penyisipan steganografi dihitung di mana *K* adalah kapasitas penyisipan piksel *P* dalam *bit*. Keempat, dengan menggunakan Persamaan 8 dan 9 peneliti menghitung nilai kesalahan penyisipan di mana *G* adalah nilai kesalahan. *S* adalah nilai absolut. *P(x,y)* adalah nilai piksel *P* asli. $P'(x\,,y)$ adalah nilai piksel *P* tanpa mengubah *bit* pada barisan $K+1$. $P''(x,y)$ adalah nilai piksel *P* dengan mengubah *bit* pada barisan *K+1*.

$$G_1 = S[P(x,y) - P'(x,y)] \quad (8)$$
$$G_2 = S[P(x,y) - P''(x,y)] \quad (9)$$

Langkah kelima adalah memeriksa perlu tidaknya perubahan pada *bit K+1*, dengan syarat pertama adalah jika $G_1 < G_2$, maka $P(x,y)$ akan digantikan oleh $P'(x,y)$. Kedua, jika $G_1 > G_2$, maka $P(x,y)$ akan diganti dengan $P''(x,y)$. Langkah-langkah penilaian viabilitas steganografi menjadi subyek pengujian steganografi yang dihubungkan dengan fitur-fitur dasar steganografi.

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

Ketahanan adalah salah satu kualitas ini. Pengujian kualitas adalah objek adalah *cover image* dan outputnya adalah *stego image* yang dibuat dengan proses steganografi, terutama dengan membandingkan *cover image* dengan *stego image* yang memiliki pesan tersembunyi. Sebagai tambahan, Gambar 4 memberikan bagian dari data *cover image* untuk kelas buah. Gambar 4 juga menggambarkan *cover image* kaya warna yang peneliti evaluasi menggunakan steganografi AMELSBR yang dioptimasi.

Gambar 4. *Cover Image* dari data dengan kelas Buah

B. Optimasi AMELSBR pada Proses Decode

Pengujian manipulasi citra dengan *brightness*, *contrast*, *resize*, *noise*, dan *blur* yang dilakukan di akhir proses *decoding*. Sedangkan untuk proses *encoding*, pengujian dilakukan dengan MSE yang ditunjukkan pada Persamaan 10.

$$MSE = \frac{1}{N}\sum|y(n) - x(n)|^2 \tag{10}$$

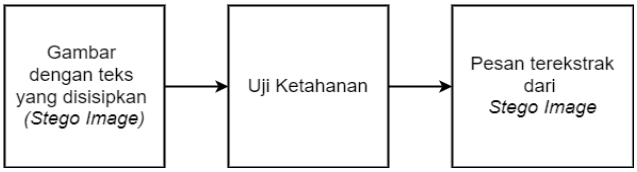
MSE adalah teknik untuk menghitung kuadrat *error* antara *cover image* dan *stego image*. Semakin rendah angka MSE maka semakin baik kualitas *stego image*. Meskipun kualitas citra tidak berubah di antara keduanya, *stego image* tetap dapat menghasilkan citra yang sebanding dengan *cover image*, tetapi dengan pesan tersembunyi yang disisipkan dengan benar. Secara global, nilai MSE dikatakan sangat baik jika kurang dari atau sama dengan satu.

Selain MSE, peneliti juga menggunakan pendekatan *Peak Signal-to-Noise Ratio* (PSNR). Pendekatan PSNR dengan membandingkan nilai tertinggi *stego image* terhadap besarnya nilai MSE yang mencerminkan tingkat *noise* pada *cover image* dengan mencari perbedaan distorsi antar frame. PSNR juga digunakan untuk membandingkan kualitas *cover image* sebelum dan sesudah penyisipan pesan.

$$PSNR = 10log_{10}\frac{255^2}{MSE} \tag{11}$$

Nilai PSNR dinyatakan dalam desibel (dB) dan diukur menggunakan Persamaan 11. Nilai PSNR yang kurang dari 30 dB menunjukkan kualitas yang agak rendah dan distorsi yang dihasilkan oleh proses steganografi mudah terlihat. *Stego image* yang berkualitas tinggi di sisi lain harus ditargetkan untuk mendapatkan nilai PSNR lebih besar dari 35 dB [20].

DOI: https://doi.org/10.35457/antivirus.v16i1.1967



Gambar 5. Alur *Decoding* dengan Uji Ketahanan

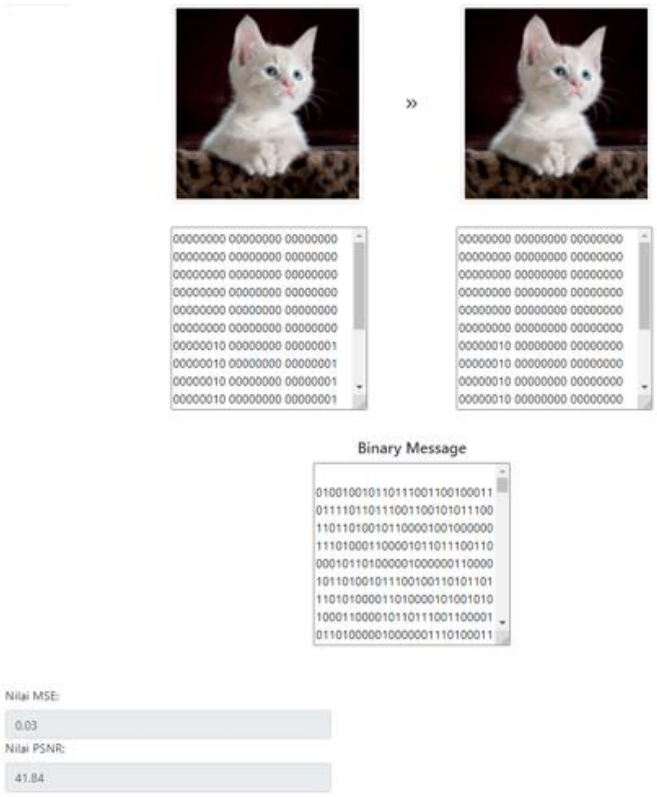
Gambar 5 merupakan diagram blok yang disederhanakan untuk uji ketahanan proses *decoding*. Persentase pengujian kemudian dipilih dengan masing-masing berdasarkan kecerahan *(stego image brightness)*, kontras *(stego image contrast)*, *resize*, *blur*, dan *noise*. Semua pengujian ini bertujuan untuk mengekstrak pesan yang diambil dari *stego image*. Jika pesan yang diambil cocok dengan pesan yang disematkan, *stego image* telah lulus uji yang relevan. Pada penelitian ini, tidak ada kombinasi uji ketahanan yang digunakan untuk membatasi jumlah skema penelitian.

IV. HASIL DAN PEMBAHASAN

Bagian bab ini menyajikan hasil dari proses steganografi *encoding* dan *decoding* menggunakan teknik steganografi AMELSBR yang telah peneliti optimasi.

A. Hasil Stego Image

Gambar 6 menggambarkan hasil *stego image* dari salah satu *cover image* untuk menunjukkan nilai MSE dan PSNR. Nilai MSE dan PSNR dari masing-masing *cover image* yang melalui prosedur steganografi AMELSBR teroptimasi akan dijelaskan secara rinci pada sub-bagian berikutnya. Gambar 6 juga menunjukkan bagaimana hasil dari *cover image*, *stego image*, dan pesan teks ditransformasikan ke dalam bentuk biner. Secara sekuensial dari Gambar 7 merupakan penyajian ilustrasi citra *stego image* dari skema penelitian masing-masing dengan penggantian 1 *bit*, 2 *bit*, 3 *bit*, dan 4 *bit*. Jika dilihat dengan pandangan semata, hasil dari Gambar 7 memiliki perbedaan warna yang cukup minim dibandingkan dengan *cover image* asli (Gambar 4). Namun pengujian ketahanan citra akan dilanjutkan pada sub-bagian berikutnya.



Gambar 6. Hasil MSE dan PSNR dari *Stego Image* dan Transformasi Teks ke Biner

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

Gambar 7. Hasil *Stego Image* dengan Penggantian a) 1 *bit*, b) 2 *bit*, c) 3 *bit*, d) 4 *bit*

B. Hasil Uji Ketahanan

Tabel 4 menampilkan nilai MSE dan PSNR dari 46 *cover image* yang diperoleh dari *platform* berbagi citra Unsplash. Berdasarkan Tabel 4, hampir semua *stego image* memiliki nilai MSE yang layak kurang dari satu, kecuali untuk *cover image* nomor 13 dengan metode penggantian 4 *bit* yang memiliki nilai MSE terburuk yaitu 2,44. Demikian pula, hampir semua *stego image* memiliki nilai PSNR yang layak yaitu kurang dari 35 dB, kecuali untuk *cover image* nomor 13 dengan metode penggantian 3 *bit* yang memiliki nilai PSNR paling buruk adalah 23,21 dB. Sebagai tambahan, pemisahan kategori pada *cover image* tidak mempengaruhi hasil tes MSE dan PSNR.

Tabel 4. Algoritma AMELSBR menurut Lee dan Chen

#	1-bit		2-bits		3-bits		4-bits	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
1	0,01	49,79	0,02	44,4	0,06	39,47	0,39	31,12
2	0	52,71	0,02	44,9	0,05	40,47	0,4	31,1
3	0	50,38	0,01	46,76	0,01	47,11	0,18	34,48
4	0,03	42,94	0,18	34,47	0,59	29,34	2,4	23,1
5	0,01	49,6	0,02	43,22	0,04	41,41	0,36	31,55
6	0	51,43	0,01	47,89	0,03	42,91	0,19	34,4
7	0,01	50,02	0,02	44,22	0,04	40,81	0,4	31,01
8	0	51,12	0,01	45,36	0,03	42,56	0,36	31,53
9	0	53,82	0,01	47,09	0,03	43,06	0,22	33,61
10	0,01	48,83	0,04	40,57	0,02	43,28	0,28	32,67
11	0	53,24	0,01	47,33	0,03	42,66	0,35	31,63
12	0,03	41,84	0,14	35,62	0,78	28,17	1,7	24,78
13	0,24	33,28	0,5	30,06	1,27	26,03	2,44	23,21

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

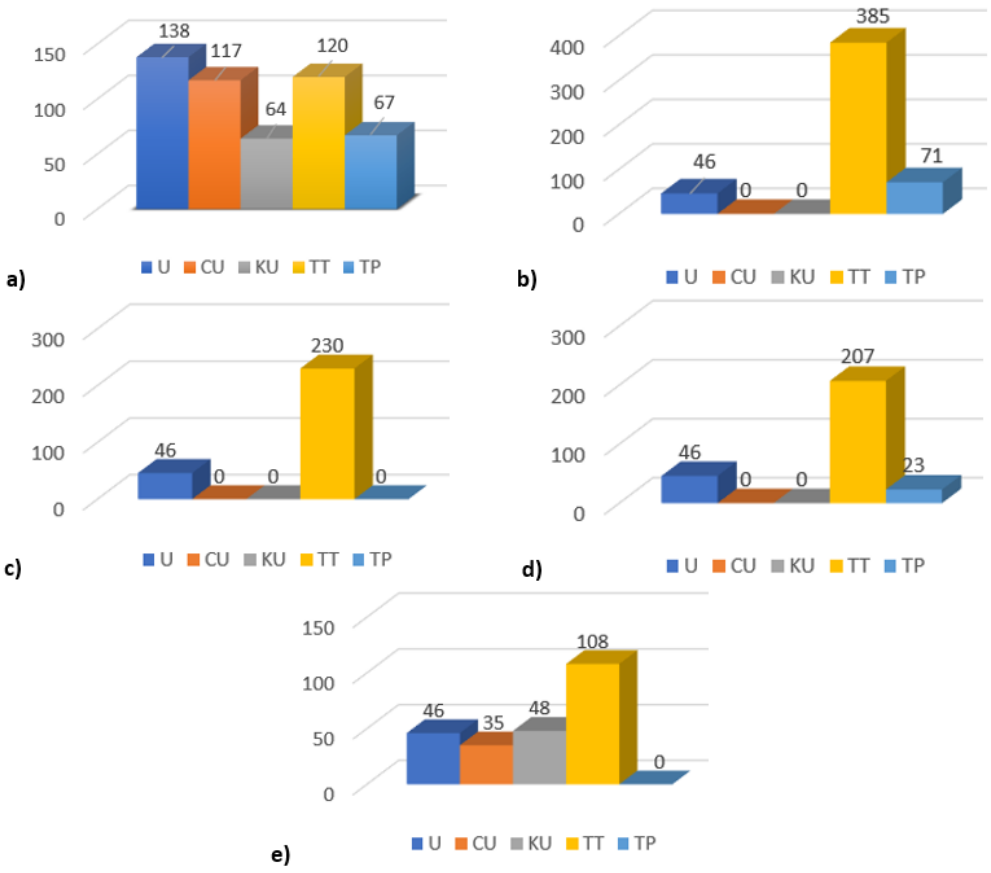
#	1-bit		2-bits		3-bits		4-bits	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
14	0	52,65	0,01	47,49	0,03	42,65	0,26	32,89
15	0	53,52	0,01	45,63	0,02	43,6	0,23	33,5
16	0,01	49,67	0,02	45	0,03	42,74	0,25	33,11
17	0	50,47	0,03	42,96	0,03	42,34	0,37	31,37
18	0	52,05	0,03	42,7	0,04	40,81	0,42	30,84
19	0	52,8	0,01	46,51	0,04	41,22	0,46	30,48
20	0	52	0,02	44,41	0,04	40,91	0,45	30,54
21	0	52,36	0,02	44,32	0,03	42,28	0,53	29,82
22	0	52,96	0,02	44,98	0,03	42,53	0,37	31,42
23	0	53,05	0,01	45,41	0,02	45,13	0,21	33,8
24	0	51,67	0,01	45,63	0,02	43,34	0,36	31,5
25	0	54,54	0,01	46,99	0,04	40,84	0,19	34,25
26	0	50,9	0,02	44,48	0,03	42,66	0,27	32,82
27	0	53,43	0,01	47,14	0,02	44,49	0,07	38,52
28	0	51,34	0,02	45,2	0,04	40,84	0,09	37,67
29	0	50,35	0,01	46,92	0,03	41,84	0,34	31,72
30	0,01	48,96	0,02	43,49	0,04	40,8	0,34	31,74
31	0	50,86	0,01	46,62	0,06	39,59	0,31	32,12
32	0,01	49,71	0,01	45,76	0,08	38,1	0,31	32,12
33	0	51,58	0,01	45,36	0,02	43,28	0,09	37,47
34	0	50,09	0,02	44,73	0,04	41,62	0,35	31,64
35	0,01	47,81	0,02	44,96	0,08	37,97	0,87	27,93
36	0	60,64	0	51,97	0,04	40,56	0,07	38,63
37	0	55,32	0,01	46,98	0,02	44,69	0,16	34,92
38	0	52,07	0,02	45,24	0,04	41,45	0,26	32,99
39	0	51,16	0,01	46,97	0,01	45,82	0,1	37,08
40	0	50,71	0,01	45,51	0,03	42,62	0,26	32,84
41	0	52,91	0,01	45,94	0,03	42,02	0,31	32,22
42	0	51,48	0,02	44,65	0,03	42,11	0,08	37,87
43	0	53,43	0,01	46,89	0,02	43,55	0,24	33,27
44	0	50,49	0,02	44,5	0,03	42,29	0,32	31,99
45	0	53,72	0,02	44,12	0,05	39,89	0,94	27,36
46	0	52,11	0,02	44,91	0,08	38,06	0,35	31,59

Tabel 5. Informasi Notasi dari Uji Ketahanan

Notasi	Arti Notasi	Angka Kuantitatif
U	Utuh	100%
CU	Cukup Utuh	70%-99%
KU	Kurang Utuh	50%-69%
TT	Tidak dapat Terbaca	20%-49%
TP	TP	0%

Simbol U (Utuh) pada Tabel 5 menunjukkan kapasitas pengujian untuk memulihkan/mengekstrak pesan tersembunyi secara utuh pada persentase tersebut. Sementara CU (Cukup Utuh) menunjukkan bahwa pesan dapat diekstraksi di seluruh tingkat. KU (Kurang Utuh) menunjukkan bahwa pesan dapat dipulihkan pada tingkat yang kurang lengkap. TT (Tidak Terbaca) menunjukkan bahwa pesan yang diekstraksi tidak dapat dibaca. TP (Tidak ada Pesan) menunjukkan bahwa tidak ada pesan yang dapat diekstraksi. Sebagai catatan, notasi yang telah diindikasikan sebagai pengukuran kualitatif dari berbagai metode pengujian juga digunakan, seperti yang terlihat pada Gambar 8.

DOI: https://doi.org/10.35457/antivirus.v16i1.1967



Gambar 8. Jumlah *Stego Image* dalam Tingkat Ekstraksi Berbeda pada Uji a) Kecerahan, b) Kontras, c) Resize, d) Blur, e) *Noise*

Berdasarkan Gambar 8a, dapat dilihat bahwa *stego image* memiliki berbagai tingkatan dalam mengembalikan pesan tersembunyi pada pengujian kecerahan. Dari total 8 rasio kecerahan yaitu dengan 140% hingga 0%, masing-masing dengan langkah per 20% dikalikan dengan total 46 *stego image* yaitu sama dengan 506 *stego image.* Pesan tersembunyi yang dapat dipulihkan sepenuhnya adalah 138 citra atau sekitar 27,27%. Sedangkan pesan tersembunyi yang dapat diekstraksi pada tingkat yang cukup utuh adalah 117 citra atau 23,12% dari total *stego image*. Pesan tersembunyi yang dapat diekstraksi pada tingkat tidak lengkap dan tidak terbaca adalah 64 citra (12,65%), dan 120 citra (23,72%). Pesan tersembunyi yang tidak bisa diekstrak sama sekali adalah 67 citra atau 13,24%.

Berdasarkan Gambar 8b terlihat bahwa *stego image* seringkali tidak dapat mengembalikan pesan yang tersembunyi pada pengujian kontras. Dari total 8 rasio kontras dengan 140% hingga 0% dengan masing-masing langkah per 20% dikalikan dengan total 46 *stego image* yaitu sama dengan 506 *stego image*. Pesan tersembunyi yang dapat dipulihkan sepenuhnya adalah 46 citra atau sekitar 9,09%. Sedangkan pesan tersembunyi yang dapat diekstraksi pada level tidak dapat terbaca sebanyak 385 citra atau 76,09% dari total *stego image*. Pesan tersembunyi yang tidak dapat diekstrak sama sekali terdapat pada 71 citra atau 14,03%.

Gambar 8c menunjukkan hasil pengujian dengan skema per persentase dengan pengubahan ukuran atau *resize*, mulai dari 100% (lebih besar), hingga mencapai 0% (ukuran sebenarnya). Berdasarkan Gambar 13, terlihat bahwa *stego image* tidak dapat mengatasi uji *resize* dalam mengembalikan pesan tersembunyi. Dari total 6 rasio *resize* dengan 100% menjadi 0% dengan masing-masing langkah per 20% dikalikan dengan total 46 *stego image* yaitu sama dengan 276 *stego image*. Pesan tersembunyi yang dapat dipulihkan sepenuhnya adalah 46 citra atau sekitar 16,67%. Sedangkan pesan tersembunyi yang dapat diekstraksi pada level tidak dapat terbaca sebanyak 230 citra atau 83,33% dari total *stego image*.

Berdasarkan Gambar 8d terlihat bahwa *stego image* seringkali tidak dapat mengembalikan pesan yang disembunyikan pada pengujian *blur*. Dari total 6 rasio *blur* dengan 100% hingga 0% dengan masing-masing

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

langkah per 20% dikalikan dengan total 46 *stego image* yaitu sama dengan 276 *stego image*. Pesan tersembunyi yang dapat dipulihkan sepenuhnya adalah 46 citra atau sekitar 16,67%. Sedangkan pesan tersembunyi yang dapat diekstraksi pada level tidak dapat terbaca sebanyak 207 citra atau 75% dari total *stego image*. Pesan tersembunyi yang tidak bisa diekstrak sama sekali adalah 23 citra atau 8,33%.

Gambar 8e menunjukkan hasil pengujian dengan skema per persentase *noise*, mulai dari 20% yaitu *noise* tertinggi, hingga mencapai 0% yaitu tanpa *noise*. Gambar 15 dapat dilihat bahwa *stego image* memiliki berbagai tingkatan dalam mengembalikan pesan yang tersembunyi dengan pengujian *noise*. Dari total lima rasio *noise* dengan 20% hingga 0% dengan masing-masing langkah per 5% dikalikan dengan total 46 *stego image* yaitu sama dengan 230 *stego image*. Pesan tersembunyi yang dapat dipulihkan sepenuhnya adalah 46 citra atau sekitar 20%. Pesan tersembunyi yang dapat dikembalikan pada tingkat cukup utuh dan kurang utuh adalah 35 citra (15,22%) dan 48 citra (20,87%). Sedangkan pesan tersembunyi yang dapat diekstraksi pada level tidak dapat terbaca adalah 108 citra atau 46,96% dari total *stego image*.

V. KESIMPULAN

Penelitian ini mendeskripsikan alur dan hasil eksperimen steganografi unik pada media citra menggunakan metode AMELSBR. Dalam percobaan ini, AMELSBR dioptimalkan dengan mengganti hingga 4 *bit* terakhir. Peneliti merancang aplikasi AMELSBR yang mampu mengganti hingga 4 *bit* terakhir dari sebuah citra. Input citra atau *cover image* umumnya akan mengalami distorsi yang luar biasa untuk menyisipkan pesan teks. Memburuknya distorsi pada *stego image* ditunjukkan dengan nilai MSE yang tinggi dan PSNR yang rendah. Namun, pada percobaan ini peneliti mengoptimalkan AMELSBR sehingga *stego image* secara keseluruhan memiliki hasil yang baik (terbaik pada angka 0 untuk MSE dan angka 60,64 dB untuk PSNR). Bahkan dengan mata telanjang, skema penggantian dari satu hingga 4 *bit* menunjukkan *stego image* yang mirip dengan *cover image*.

Karena citra secara umum tidak memiliki kompresi citra, peneliti memilih citra dengan kompresi *lossless*. Kompresi *lossy* dari JPEG dan JPG akan membebani selama proses steganografi. Ini dapat menyebabkan nilai MSE dan PSNR yang buruk karena kemampuannya untuk membuat ulang citra berdasarkan perkiraan piksel terdekat dan tidak dapat mencocokkan citra aslinya. Dari format, PNG dianggap memiliki kompresi *lossless* terbaik dengan piksel warna yang lebih tinggi.

Selain itu, dalam menyiapkan dataset *cover image* yang mengalami proses steganografi, peneliti merekomendasikan data citra yang tidak memiliki warna dominan hitam. Berdasarkan eksperimen peneliti yang belum disiapkan pada rancangan awal seperti pada bab-bab sebelumnya, peneliti menemukan bahwa gambar berwarna hitam ini menunjukkan kompatibilitas yang buruk dengan steganografi, sebagaimana dibuktikan oleh skema penggantian empat *bit* untuk *cover image* nomor 13. Hasil *stego image* dianggap baik jika nilai MSE dibawah 1 dan nilai PSNR diatas 35 dB. Sedangkan pada *cover image* nomor 13, angka MSE hanya mencapai 2,44, dan PSNR hanya mencapai 23,21 dB. Sehingga, peneliti menyimpulkan bahwa *cover image* dengan berbagai warna memiliki uji ketahanan yang lebih baik dibandingkan *cover image* dengan warna dominan hitam. Sebagai tambahan, kategori citra (abstrak, buah, hewan, dan pemandangan) sebagai *cover image* juga tidak memiliki peran dalam mempengaruhi nilai uji ketahanan.

DAFTAR PUSTAKA

[1] K. Sharma, A. Aggarwal, T. Singhania, D. Gupta, and A. Khanna, "Hiding Data in Images Using Cryptography and Deep Neural Network," *arXiv Prepr. arXiv1912.10413*, 2019.

[2] X. Liang, Z. Yan, and P. Zhang, "Security, Privacy, and Anonymity in Computation, Communication, and Storage," *Int. Conf. Secur. Priv. Anonymity Comput. Commun. Storage (SpaCCS 2016)*, vol. 1, pp. 155–167, 2016, doi: 10.1007/978-3-319-72395-2.

[3] M. Barbosa *et al.*, "SoK: Computer-aided Cryptography," 2021.

[4] F. Sidik, F. E. Febriansyah, and others, "Perbandingan Metode Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR) dan Discrete Cosine Transform untuk Steganografi Citra Digital," *J. Komputasi*, vol. 6, no. 1, 2018.

DOI: https://doi.org/10.35457/antivirus.v16i1.1967

[5] M. Saravanan and A. Priya, "An Algorithm for Security Enhancement in Image Transmission Using Steganography," *J. Inst. Electron. Comput.*, vol. 1, no. 1, pp. 1–8, 2019.
[6] O. Rachael, S. Misra, R. Ahuja, A. Adewumi, F. Ayeni, and R. Mmaskeliunas, "Image Steganography and Steganalysis based on Least Significant Bit (LSB)," in *Proceedings of ICETIT 2019*, Springer, 2020, pp. 1100–1111.
[7] B. Hasan Saghir, E. A. Elmutalib Ahmed, G. Zen A. Salh, and A. H. Mansour, "A Spatial Domain Image Steganography Technique Based on Pseudorandom Permutation Substitution Method using Tree and Linked List," *Int. J. Eng. Trends Technol.*, vol. 23, no. 4, pp. 209–217, 2015, doi: 10.14445/22315381/ijett-v23p240.
[8] M. Kalita, T. Tuithung, and S. Majumder, "A New Steganography Method Using Integer Wavelet Transform and Least Significant Bit Substitution," *Comput. J.*, vol. 62, no. 11, pp. 1639–1655, Nov. 2019, doi: 10.1093/comjnl/bxz014.
[9] J. Hashim, A. Hameed, M. J. Abbas, M. Awais, H. A. Qazi, and S. Abbas, "LSB Modification based audio steganography using advanced encryption standard (AES-256) technique," in *2018 12th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, 2018, pp. 1–6.
[10] D. Darwis, N. B. Pamungkas, and others, "Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness," in *Journal of Physics: Conference Series*, 2021, vol. 1751, no. 1, p. 12039.
[11] S. Manaseer, A. Aljawawdeh, and D. Alsoudi, "A New Image Steganography Depending On Reference and LSB," *Int. J. Appl. Eng. Res. ISSN 0973-4562 Vol.*, vol. 12, pp. 1950–1955, 2017.
[12] A. Arya and S. Soni, "Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method," *Int. J. Comput. Sci. Trends Technol.*, vol. 6, no. 2, pp. 160–165, 2018.
[13] A. Alabaichi, M. A. A. K. Al-Dabbas, and A. Salih, "Image Steganography using Least Significant Bit and Secret Map Techniques," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 1, 2020.
[14] C. Arun and S. Murugan, "Design of Image Steganography using LSB XOR Substitution Method," in *2017 International Conference on Communication and Signal Processing (ICCSP)*, 2017, pp. 674–677.
[15] P. N. de Souza and P. Gladyshev, "Inference of Endianness and Wordsize From Memory Dumps," in *European Conference on Cyber Warfare and Security*, 2017, pp. 619–627.
[16] G. K. Soni, A. Rawat, S. Jain, and S. K. Sharma, "A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm with LSB Watermark Technique," in *Smart Systems and IoT: Innovations in Computing*, Springer, 2020, pp. 483–492.
[17] A. Pradhan, K. R. Sekhar, and G. Swain, "Digital image steganography using LSB substitution, PVD, and EMD," *Math. Probl. Eng.*, vol. 2018, 2018.
[18] L. Widyawati, I. Riadi, and Y. Prayudi, "Comparative Analysis of Image Steganography using SLT, DCT and SLT-DCT Algorithm," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, pp. 169–182, 2020.
[19] Y.-K. Lee and L.-H. Chen, "An Adaptive Image Steganographic Model based on Minimum-Error LSB Replacement," in *Ninth National Conference on Information Security*, 1999, pp. 8–15.
[20] Q. M. Hussein, "New Metrics for Steganography Algorithm Quality," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 02, 2020.

DOI: https://doi.org/10.35457/antivirus.v16i1.1967