JURNAL ILMU PENGETAHUAN DAN TEKNOLOGI KOMPUTER

VOL. 5. NO. 2 FEBRUARI 2020
P-ISSN: 2685-8223 | E-ISSN: 2527-4864

KAJIAN METODE METODE STEGANOGRAFI PADA DOMAIN SPASIAL

Gunawan Wibisono[1]; Tri Waluyo[2]; Erik Iman Heri Ujianto[3]

[1]Magister Teknologi Informasi
Universitas Teknologi Yogyakarta
http://uty.ac.id/
[1]gunawan.wibisono@student.uty.ac.id, [2]triwaluyo@student.uty.ac.id, [3]erik.iman@uty.ac.id

Abstract— *This paper contains a review of the spatial domain steganographic literature. The purpose of this paper is to provide knowledge about techniques or methods that exist in the spatial domain of steganography. Steganography is the science or technique for hiding secret messages in other messages so that the existence of the secret message cannot be accessed by others who do not have authority. There are several popular spatial domains of steganographic techniques, namely LSB (Least Significant Bit), which is mapping secret message bits in the rightmost bit (LSB) of each color pixel and PVD (Pixel Value Differencing) which in this method offers a larger message storage capacity , with better image quality compared to other methods in the spatial domain. Because privacy issues continue to develop along with various digital communication technologies, and increasingly strong security threats, steganography can play a role in society to maintain the confidentiality of both picture, voice and video messages. For this reason it is important for us to be aware of steganographic technology and its implications.*

Keywords*: LSB, PVD, Spatial, Steganography.*

Intisari— Makalah ini berisi tentang tinjauan literatur steganografi domain spasial. Tujuan dari makalah ini adalah memberikan pengetahuan tentang teknik atau metode yang ada dalam domain spasial steganografi. Steganografi adalah ilmu teknik atau seni untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat di-akses oleh orang lain yang tidak mempunyai kewenangan. Dalam Domain spasial steganografi ada beberapa teknik populer yaitu LSB *(Least Significant Bit)* yaitu memetakan bit-bit pesan rahasia pada bit paling kanan (LSB) dari setiap piksel warna dan PVD *(Pixel Value Differencing)* dimana dalam metode ini menawarkan kapasitas penyimpanan pesan yang lebih besar, dengan kualitas citra yang lebih baik dibandingkan dengan metode lain dalam domain spasial. Karena masalah privasi terus berkembang bersamaan dengan berbagai teknologi komunikasi digital, serta ancaman keamanan yang semakin kuat, maka steganografi dapat berperan dalam masyarakat untuk menjaga kerahasiaan baik pesan gambar, suara maupun video. Untuk alasan tersebut penting bagi kita menyadari teknologi steganografi dan implikasinya.

Kata Kunci*: LSB, PVD, spasial, steganografi.*

PENDAHULUAN

Keamanan dan kerahasiaan data merupakan salah satu aspek penting dari informasi. Pada era digital saat ini banyak terjadi kasus pencurian data maupun informasi. Dengan berkembangnya teknik pengambilan informasi secara ilegal, banyak orang mencoba untuk mengakses data yang bukan haknya. Informasi penting dan pribadi kadang kala tidak cukup hanya dengan proses enkripsi pada saat dikirim atau disimpan.

Dalam mengamankan (*security system*) data atau informasi dapat dibagi menjadi 2 yaitu penyembunyian informasi (*Information Hiding*) dan enkripsi informasi, penyembunyian informasi lebih dikenal dengan istilah steganografi dan tanda air (*watermarking*) sedangkan enkripsi informasi lebih dikenal dengan nama kriptografi.

Steganografi adalah salah satu alternatif solusi dalam mengamankan informasi yang bersifat penting dan pribadi. Istilah steganografi berasal dari bahasa Yunani, yaitu steganos yang berarti penyamaran atau penyembunyian dan graphein yang berarti tulisan. Jadi, steganografi bisa diartikan sebagai seni menyembunyikan pesan dalam data lain tanpa mengubah data yang ditumpanginya tersebut sehingga data yang ditumpanginya sebelum dan setelah proses penyembunyian hampir terlihat sama (Syawal, Fikriansyah, & Agani, 2016).

Steganografi banyak digunakan pada teknik komunikasi rahasia dimana data rahasia disembunyikan di beberapa multimedia objek seperti gambar, audio atau video (J. Singh, Kaur, & Garcha, 2015). Steganografi merupakan suatu cabang ilmu yang mempelajari tentang bagaimana menyembunyikan atau informasi rahasia didalam

informasi lainnya. Steganografi mempunyai sejarah yang hampir sama dengan kriptografi, keduanya banyak digunakan ketika zaman perang (Syahril & Jaya, 2019).

Steganografi adalah seni dan ilmu menggunakan obyek komunikasi digital sedemikian rupa sehingga menyembunyikan keberadaan informasi rahasia (Hussain, Wahab, Idris, Ho, & Jung, 2018)(Hussain et al., 2018)(Hussain et al., 2018)(Hussain et al., 2018). steganografi adalah seni dan ilmu menyembunyikan informasi dengan *embedding* pesan dalam suatu media digital, pesan yang tampaknya tidak berbahaya (David, Murtado, & Kasma, 2012).

Kriptografi berasal dari bahasa Yunani yang terdiri dari dua suku kata, *cryptos* yang berarti rahasia dan *graphein* yang berarti kata tulisan, secara umum dapat diartikan sebagai tulisan rahasia (Nurdin, 2017). Kriptografi didefinisikan sebagai ilmu untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode kode dan aturan aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya (Suhardi, 2016). Adanya kriptografi sebuah informasi dapat diacak atau disandikan menjadi informasi yang sulit atau bahkan tidak dipahami melalui sebuah proses yang dinamakan enkripsi (Murdani, 2017).

BAHAN DAN METODE

Dalam penyusunan artikel ilmiah ini, peneliti menggunakan metode studi pustaka, menurut Zed dalam (Supriyadi, 2017) studi pustaka atau kepustakaan dapat diartikan sebagai serangkaian kegiatan yang berkenaan dengan metode pengumpulan data pustaka, membaca dan mencatat serta mengolah bahan penelitian. Menurut Nazir dalam (T & Purwoko, 2017) Studi kepustakaan juga berarti teknik pengumpulan data dengan melakukan penelaahan terhadap buku, literatur, catatan, serta berbagai laporan yang berkaitan dengan masalah yang ingin dipecahkan. Studi pustaka yang dilakukan yaitu dengan cara mengeksplorasi dan menelaah jurnal baik nasional maupun internasional yang dianggap relevan dengan penelitian atau kajian.

HASIL DAN PEMBAHASAN

Steganografi bekerja dengan mengganti bit tidak berguna atau tidak digunakan, dimana media digital berupa file (seperti grafik, suara, teks, HTML) dengan potongan yang berbeda. Obyek komunikasi bisa berupa media pembawa apa saja seperti perangkat *smartphone* atau layanan sosial media misalkan *facebook*, *browser* dan lainnya yang digunakan untuk komunikasi rahasia.

Menurut Munir dalam (Anwar, 2018) steganografi memiliki kriteria yang harus diperhatikan dalam penyembunyian data, image, teks dan suara antara lain yaitu :

a) *Fidelity*, Mutu penampung tidak jauh berubah. Setelah penambahan data rahasia, hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam tersebut terdapat data rahasia.
b) *Robustness*, Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada penampung (seperti pengubahan kontras, penajaman, pemempatan, rotasi, pembesaran gambar, pemotongan, enkripsi dan sebagainya). Bila pada dilakukan operasi pengolahan, maka data yang disembunyikan tidak rusak.
c) *Recovery*, Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*), dimana tujuan steganografi adalah data hiding, maka sewaktu waktu data rahasia di dalam penampung harus dapat diambil kembali untuk digunakan lebih lanjut.

Pada kriteria *fidelity*, terdapat pengujian yang dapat memberikan nilai terhadap mutu penampung. Pengujian ini adalah pengujian MSE (*Mean Square Error*) dan PSNR (*Peak Signal to Noise Radio*),

1) Pengujian MSE (*Mean Square Error*)

Pengujian MSE dilakukan untuk menentukan nilai rata rata kuadrat dari jumlah kuadrat absolute *error* antara *cover image* dengan citra stego, sebelum menentukan PSNR (*Peak Signal to Noise Radio*). Terdapat rumus dalam menghitung MSE, sebagai berikut (Zainal, Pagar, & Bandarlampung, 2016) :

$$MSE_{AVG}=\frac{MSE_R+MSE_G+MSE_B}{3} \quad \text{..... (1)}$$

Keterangan:
MSE_{AVG}= Nilai rata rata MSE *cover image*
MSE_R = Nilai MSE warna merah
MSE_G = Nilai MSE warna hijau
MSE_B = Nilai MSE warna biru

2) Pengujian PSNR (*Peak Signal to Noise Radio*)

Pengujian PSNR (*Peak Signal to Noise Radio*) digunakan untuk mengukur kualitas citra yang dihasilkan. Metode PSNR adalah ukuran perbandingan antara nilai piksel cover image dengan nilai piksel pada citra stego yang

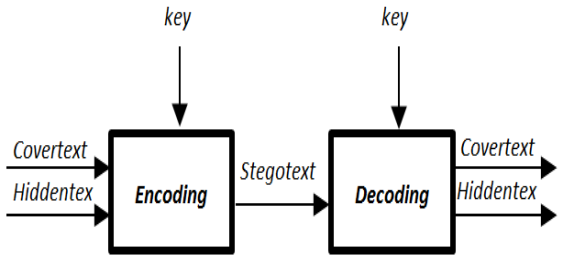
Terakreditasi Sinta Peringkat 3 (Sinta 3) berdasarkan SK Dirjen Penguatan RisBang Kemenristekdikti Nomor 28/E/KPT/2019, Tanggal 26 September 2019

dihasilkan. Rumus untuk perhitungan PSNR (*Peak Signal to Noise Radio*) sebagai berikut [10] :

$$PSNR=10\log10(\frac{255^2}{MSE}) \quad \text{.....(2)}$$

Keterangan :
PSNR = Nilai PSNR citra digital
MSE = Nilai *Mean Square Error* dari citra

Cara kerja steganografi menurut Krisnawati dalam (Anti, Kridalaksana, & Khairina, 2017) digambarkan sebagai berikut:



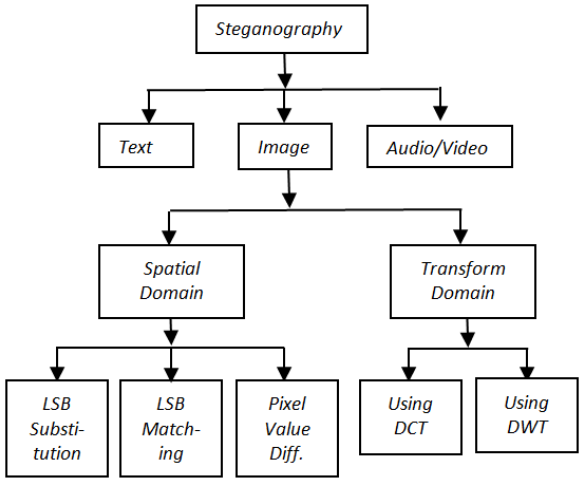
Sumber : (Anti et al., 2017)
Gambar 1. Cara Kerja Steganografi Secara Umum

Pada Gambar 1. Dijelaskan bahwa penyisipan pesan ke dalam covertext dinamakan encoding, sedangkan ekstraksi pesan stegotext dinamakan decoding. Kedua proses ini memerlukan kunci rahasia (stegokey) agar hanya pihak yang berhak saja yang dapat melakukan penyisipan dan ekstraksi pesan.

Ada beberapa istilah penting dalam steganografi menurut (Kaur, 2015) antara lain :

- Cover-Object : Objek asli yang digunakan untuk menyembunyikan informasi.
- Message : Informasi / pesan aktual yang disembunyikan, pesan dapat berupa teks atau gambar.
- Stego-Object : Menyisipkan pesan atau informasi rahasia ke dalam Cover Object.
- Stego-Key : Kunci yang digunakan untuk menyisipkan atau mengekstraksi pesan dari Cover-Object dan Stego-Object, kunci dapat berupa hurf angka ataupun simbol.

Menurut Mukesh Garg, et.al terdapat dua jenis steganografi menurut domainnya, yaitu domain spatial dan domain frekuensi (transform) (N. Singh, 2017). Domain domain tersebut dijelaskan secara hiraki pada Gambar 2., steganografi mampu menangani informasi berupa text, gambar dan audio video. Kedua domain tersebut lebih sering digunakan pada informasi berupa gambar.



Sumber : (Nichal, Jadhav, Pingale, Mohite, & Ponde, 2015)
Gambar 2. Tipe Dasar Steganografi

A. Domain spasial

Didalam domain spasial ada beberapa teknik yang digunakan, Salah satu tekniknya adalah LSB. *Least Significant Bit* (LSB) memetakan bit-bit pesan rahasia pada bit paling kanan (LSB) dari setiap piksel warna. Pada susunan bit didalam sebuah byte (1 byte = 8 bit) , ada bit yang paling berarti (*most significant bit* atau MSB) dan bit paling kurang berarti (*least significant bit* atau LSB) (Yatini & Nurwiyati, 2015), karena yang dirubah hanya LSB, maka perubahan gambar tidak akan mudah dilihat oleh indra pengelihatan manusia (Darmawan & Bayu Atmaja, n.d.). Metode LSB dikelompokan menjadi 2 yaitu subtitusi dan pencocokan, subtitusi (*Subtitution*) adalah mengganti semua bit LSB piksel dari gambar sampul dengan bit rahasia. Metode ini menanamkan bit rahasia panjang tetap dalam LSB piksel panjang tetap yang sama. Meskipun teknik ini sederhana, umumnya menyebabkan distorsi yang nyata ketika jumlah bit yang tertanam untuk setiap piksel melebihi tiga. Sedangkan pencocokan (*Matching*) adalah adalah memodulasi nilai piksel dengan menambahkan ± 1 untuk mencocokkan bit paling signifikan dengan bit pesan rahasia.

Sebagai contoh byte **1**1010010, pada angka bit 1 (angka pertama dan cetak tebal) merupakan *most significant bit* (MSB) , sedangkan angka bit 0 (angka terakhir dan cetak tebal) merupakan *least significant bit* (LSB) Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut

(Yatini & Nurwiyati, 2015).

Contoh lain dalam penerapan metode *least significant bit* (LSB) adalah sebagai berikut (Yatini & Nurwiyati, 2015) :

a) 1 bit LSB

Misalkan segmen piksel-piksel citra/gambar sebelum penambahan bit-bit adalah:

00110011 10100010 11100010 10101011 00100110 10010110 11001001 11111001 10001000 10100011

Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi 1 bit terakhir dari segmen piksel-piksel citra menjadi (digaris bawahi):

00110011 10100011 11100011 10101010 00100110 10010111 11001000 11111001 10001001 10100011

Perubahan maksimal pada setiap piksel citra adalah 1.

b) 2 bit LSB

Misalkan segmen piksel-piksel citra/gambar sebelum penambahan bit-bit adalah:

00110011 10100010 11100010 10101011 00100110

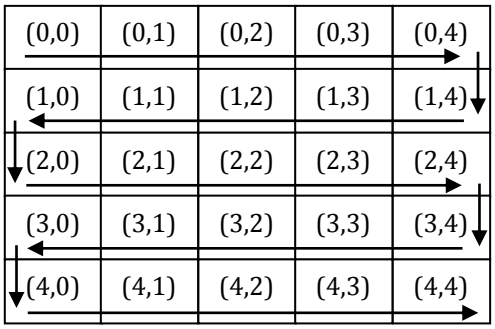
Pesan rahasia (yang telah dikonversi ke sistem biner) misalkan '1110010111', maka setiap bit dari pesan tersebut menggantikan posisi 2 bit terakhir dari segmen piksel-piksel citra menjadi (digarisbawahi):

00110011 10100010 11100001 10101001 00100111

Perubahan maksimal pada setiap piksel citra adalah 3.

Metode *Pixel Value Differencing* (PVD) juga merupakan metode yang ada di domain spasial. Metode ini menawarkan kapasitas penyimpanan pesan yang lebih besar, dengan kualitas citra yang lebih baik dibandingkan dengan metode lain. Untuk menambah tingkat keamanan dari informasi yang akan disisipkan kedalam citra, steganografi dapat dikombinasikan dengan enkripsi, sehingga informasi yang disisipkan tidak akan mudah dibaca oleh orang yang tidak bertanggung jawab (Rahim, 2016). Cara kerja metode PVD ini adalah dengan cara membagi media yang akan disisipi pesan menjadi blok blok piksel yang bertetangga. Blok-blok dibentuk dari dua buah piksel yang berdekatan atau bertetangga. Bit–bit pesan yang akan disisipkan dihitung dengan besarnya kedua piksel tersebut (Masruri, Kusrini, & Sunyoto, 2019).

Menurut Wu dan Tsai dalam (Masruri et al., 2019) *pixel value differencing* (PVD) menghitung selisih nilai dua piksel yang bertetangga, dimana hasil selisih kedua piksel tersebut nantinya akan digunakan untuk menyisipkan pesan yang disembunyikan. Proses urutan perhitungan piksel dimulai dari titik (0,0) yaitu pada piksel paling kiri atas seperti pada gambar berikut ini :



Sumber: (Masruri et al., 2019)

Gambar 3. Proses urutan perhitungan antar piksel citra pada *pixel value differencing*

Rahim dalam (Masruri et al., 2019) menjelaskan bahwa proses penyisipan dilakukan dengan cara membandingkan dua piksel yang bertetangga dengan inisialisasi P_i dan P_{i+1} dan menggunakan persamaan sebagai berikut :

$$d = | Pi - Pi + 1 | \quad (3)$$

Metode ini menggunakan skema Wu dan Tsai yang digunakan untuk mengetahui terdapat di range mana selisih antar kedua piksel tersebut, skema Wu dan Tsai sebagai berikut:

$$R=\{[0,7],[8,15],[16,31],[32,63],[64,127],[128,255]\} \quad (4)$$

Setelah diketahui letak *range* nya, maka jumlah bit pesan yang disisipkan dapat diketahui dengan persamaan sebagai berikut:

$$t = | \text{Log2 } Wi | \quad (5)$$

Wi adalah nilai selisih perbandingan dua piksel yang merupakan range dari d. Penyisipan dilakukan dengan mengambil sebanyak t-bit pesan yang akan disisipkan. Selanjutnya menurut Nofriansyah, et al dalam (Masruri et al., 2019) perlu dihitung nilai differencing value yang baru untuk penyisipan kedalam citra dengan persamaan sebagai berikut :

$$di = li + b \quad (6)$$

di adalah nilai terkecil dari skema Wu dan Tsai, letak range selisih perbandingan dua piksel yang baru. li adalah batas bawah range dua piksel lokasi

Terakreditasi Sinta Peringkat 3 (Sinta 3) berdasarkan SK Dirjen Penguatan RisBang Kemenristekdikti Nomor 28/E/KPT/2019, Tanggal 26 September 2019

penyisipan pesan. b adalah konversi biner dari bit pesan.

Proses ekstraksi pada metode PVD ini adalah mencari selisih P_i dan P_{i+1} untuk mengetahui d. Kemudian mengidentifikasi posisi d pada skema Wu dan Tsai R untuk mengambil nilai l_i dan u_i. Setelah mengetahui keduanya, kemudian mencari nilai $Wi = u_i - l_i+1$ dan $t_i = {}^2\log(W_i)$ untuk mengetahui jumlah bit pesan yang disisipkan. Kemudian menghitung $d_i = d - l_i$, kemudian konversi di ke biner dengan panjang t_i. Hasil konversi di dengan panjang biner t_i adalah pesan yang disembunyikan (Masruri et al., 2019).

LSB dan PVD merupakan metode yang sering digunakan dalam domain spasial steganografi, metode lain dalam domain ini antara lain adalah (Hazra, Haldar, Mukherjee, & Chakraborty, 2018)

- *Edges based data embedding method* (EBE)
- *Random pixel embedding method* (RPE)
- *Mapping pixel to hidden data method*
- *Labelling or conectivity method*
- *Pixel intensity based method*
- *Texture based method*
- *Histogram shifting methods*
- *Gray level modification* (GLM)
- *Quantization index modulation* (QIM)
- *Multiple-based Notational System* (MBNS)
- *The Multi Bit Plane Image Steganography* (MBPIS)

B. Domain Transform

Teknik transformasi atau frekuensi domain didasarkan pada manipulasi transformasi ortogonal gambar dari gambar itu sendiri. Teknik domain transformasi cocok untuk memproses gambar sesuai dengan konten frekuensi. Prinsip di balik metode domain frekuensi peningkatan gambar terdiri dari komputasi transformasi kesatuan diskrit 2-D gambar, misalnya DFT 2-D, memanipulasi koefisien transformasi oleh operator M, dan kemudian melakukan transformasi terbalik.

Transformasi ortogonal dari gambar memiliki dua komponen magnitudo dan fase. Besarnya terdiri dari konten frekuensi gambar. Fase ini digunakan untuk mengembalikan gambar kembali ke domain spasial. Transform domain biasa memungkinkan operasi pada konten frekuensi gambar, dan karenanya konten frekuensi tinggi seperti tepi dan informasi halus lainnya dapat dengan mudah ditingkatkan (Sharma & Kumar, 2015).

Steganografi dapat digunakan dalam pengiriman data yang bersifat rahasia dan dapat diaplikasikan antara lain seperti (Hazra et al., 2018) :

- *Printer* Modern
- E *Commerce*
- Layanan Intelijen
- Steganogarfi yang didistribusikan
- Tantangan Online

KESIMPULAN

Didalam domain spasial terdapat dua metode yang sering digunakan yaitu *Least Significant Bit* (LSB) dan *Pixel Value Defferencing* (PVD), kedua metode tersebut sering digunakan karena pada citra yang diisikan pesan rahasia terlihat samar perbedaannya antara citra sebelum disisipi dengan citra yang sudah disisipi. Karena masalah privasi terus berkembang bersamaan dengan berbagai teknologi komunikasi digital, serta ancaman keamanan yang semakin kuat, maka steganografi dapat berperan dalam masyarakat untuk menjaga kerahasiaan baik pesan gambar, suara maupun video. Untuk alasan tersebut penting bagi kita menyadari teknologi steganografi dan implikasinya.

REFERENSI

Anti, U. A., Kridalaksana, A. H., & Khairina, D. M. (2017). Steganografi Pada Video Menggunakan Metode Least Significant Bit (LSB) Dan End Of File (EOF). *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *12*(2), 104. https://doi.org/10.30872/jim.v12i2.658

Anwar, N. (2018). PERANCANGAN STEGANOGRAFI HIDDEN MESSAGE DENGAN METODE LEAST SIGNIFICANT BIT INSERTION (LSB) BERBASIS MATLAB. *Jurnal Algoritma, Logika Dan Komputasi*, *1*(1). https://doi.org/10.30813/j-alu.v1i1.1107

Darmawan, & Bayu Atmaja, I. D. M. (n.d.). *ANALISIS DAN PERBANDINGAN TEKNIK WATERMARKINGCITRA DIGITAL MENGGUNAKAN METODE BLOCK BASEDDCT DAN LSB*.

David, Murtado, A., & Kasma, U. (2012). Steganografi Pada Citra Bmp 24-Bit Menggunakan Metode Least Significant Bit. *Universitas Brawijaya*, *2*(1), 71–80.

Hazra, T. K., Haldar, M., Mukherjee, M., & Chakraborty, A. K. (2018). *A Survey on Different Techniques for Covert Communication Using Steganography*. *20*(2), 42–52. https://doi.org/10.9790/0661-2002024252

Hussain, M., Wahab, A. W. A., Idris, Y. I. Bin, Ho, A. T. S., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46–66. https://doi.org/10.1016/j.image.2018.03.012

Kaur, R. K. B. (2015). A Study and Review of Techniques of Spatial Steganography. *International Journal of Science and Research (IJSR)*, *4*(4), 3198–3203.

Masruri, N. H., Kusrini, K., & Sunyoto, A. (2019). Meningkatkan Keamanan Pesan Menggunakan Enkripsi Arnold Cat Map Dan Steganografi Pixel Value Differencing. *Semnasinotek*, *3*(1), 113–118. Kediri: Universitas Nusantara PGRI Kediri.

Murdani. (2017). Perancangan Aplikasi Keamanan Data Teks Menggunakan Algoritma Merkle Hellman Knapsack. *Jurnal Pelita Informatika*, *16*(3), 302–305.

Nichal, P. A., Jadhav, M. A., Pingale, M. K., Mohite, M. C., & Ponde, M. S. (2015). A Novel Steganography Scheme via the use of Alpha channel. *IJIREEICE*, *3*(4), 18–21. https://doi.org/10.17148/ijireeice.2015.3404

Nurdin, A. P. N. (2017). Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition. *Jesik*, *3*(Januari-Juni 2017 ISSN:2447-5290), 1–11.

Rahim, R. (2016). PENYISIPAN PESAN DENGAN ALGORITMA PIXEL VALUE DIFFERENCING DENGAN ALGORITMA CAESAR CIPHER PADA PROSES STEGANOGRAFI. *TIMES*, *5*(1), 6–11.

Sharma, S., & Kumar, U. (2015). Review of Transform Domain Techniques for Image Steganography. *International Journal of Science and Research (IJSR) ISSN (Online Index Copernicus Value Impact Factor*, *4*(5), 194–197.

Singh, J., Kaur, G., & Garcha, M. K. (2015). Review of Spatial and Frequency Domain Steganographic Approaches. *International Journal of Engineering Research & Technology (IJERT)*, *4*(06), 1122.

Singh, N. (2017). Survey Paper on Steganography. *International Refereed Journal of Engineering and Science (IRJES)*, *6*(1), 68–71.

Suhardi. (2016). Aplikasi Kriptografi Data Sederhana Dengan Metode Exlusive-or (Xor). *Teknivasi*, *03*, 23–31.

Supriyadi, S. (2017). Community of Practitioners: Solusi Alternatif Berbagi Pengetahuan antar Pustakawan. *Lentera Pustaka: Jurnal Kajian Ilmu Perpustakaan, Informasi Dan Kearsipan*, *2*(2), 83. https://doi.org/10.14710/lenpust.v2i2.13476

Syahril, M., & Jaya, H. (2019). Aplikasi Steganografi Pengamanan Data Nasabah di Standard Chartered Bank Menggunakan Metode Least Significant Bit dan RC4. *Seminar Nasional Sains & Teknologi Informasi (SENSASI)*, 505–509.

Syawal, M. F., Fikriansyah, D. C., & Agani, N. (2016). Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB. *Jurnal TICOM*, *4*(3), 91–99.

T, A. M., & Purwoko, B. (2017). Studi Kepustakaan Mengenai Landasan Teori Dan Praktik Konseling Expressive Writing. *Jurnal BK Unesa*, *8*(1), 1–8.

Yatini, I., & Nurwiyati, F. W. (2015). Algoritma Least Significant Bit Untuk Analisis Steganografi. *Seminar Nasional Informatika*.

Zainal, J., Pagar, A., & Bandarlampung, N. K. (2016). *Implementasi Teknik Steganografi Least Significant Bit (Lsb) Dan Kompresi Untuk Pengamanan Data Pengiriman Surat Elektronik*. *10*(2), 1–7.

Terakreditasi Sinta Peringkat 3 (Sinta 3) berdasarkan SK Dirjen Penguatan RisBang Kemenristekdikti
Nomor 28/E/KPT/2019, Tanggal 26 September 2019