SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Jurnal & Penelitian Teknik Informatika
Volume 3 Nomor 1, Oktober 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Menjaga Kerahasiaan Data dengan Steganografi Kombinasi LSB-2 dengan LSB-3 Dan *Chess Board Pattern*

Nurul Khairina
Universitas Medan Area
Medan, Indonesia
nurulkhairina27@gmail.com

Muhammad Khoiruddin Harahap
Politeknik Ganesha Medan
Medan, Indonesia
choir.harahap@yahoo.com

***Abstrak*—** Steganografi merupakan bidang keamanan dengan pola kerja yang menyisipkan data ke dalam beberapa media digital, proses penyisipan ini bertujuan untuk menyembunyikan keberadaan data tersebut dari pihak yang tidak bertanggung jawab. Penelitian ini, menjabarkan kombinasi algoritma *Least Significant Bit* yang sudah dimodifikasi yaitu Algoritma *Least Significant Bit – 2* dan algoritma *Least Significant Bit – 3*. Pemaparan yang dilakukan adalah dengan mengkombinasikan kedua metode tersebut yang kemudian disisipkan ke dalam citra, dalam hal ini menggunakan format JPG, bit pesan akan disisipkan ke dalam salah satu piksel warna *Red*, *Green* dan *Blue*. Pola penyisipan yang dilakukan dengan *Chess Board Pattern*. Tingkat kerusakan citra diukur dengan metode *Mean Square Error* untuk melihat tingkat kerusakan citra apakah citra tersebut rusak atau tidak dengan batas ambang tertentu. Hasil penelitian ini memperoleh nilai MSE sebesar 1,2 %, dimana tidak terlihat adanya perubahan nilai warna yang signifikan dari citra hasil penyisipan terhadap citra asli.

Kata Kunci—steganografi; LSB – 2; LSB – 3; Mean Square Error

I. PENDAHULUAN

Menjaga kerahasiaan data merupakan hal yang sangat penting. Perkembangan teknologi yang semakin cepat dan semakin tidak terikuti, membuat kita harus selalu tanggap dalam menjaga kerahasiaan data. Perkembangan zaman juga seiring sejalan dengan perkembangan teknik-teknik menjaga kerahasiaan data, hal ini terlihat dari peran para peneliti dari berbagai negara yang terus memberikan kontribusinya dalam bidang ilmu keamanan data. Steganografi merupakan salah satu bidang ilmu yang populer, berbagai kombinasi dan modifikasi diterapkan untuk terus menemukan algoritma yang efisien dan memiliki tingkat keamanan data yang baik.

Penelitian sebelumnya pernah dilakukan oleh Nurul [1] penelitian ini membandingkan algoritma steganografi *Least Significant Bit* (LSB) dengan koordinat parabola dan dengan koordinat linear. Hasil penelitian ini menunjukkan bahwa algoritma LSB dengan koordinat parabola memiliki tingkat keamanan yang lebih tinggi, karena kerumitan koordinat kurva parabola yang digunakan.

Taronisokhi [2] melakukan kombinasi metode LSB-2 dengan algoritma kriptografi *triangle chain cipher*. Hasil penelitian menunjukkan bahwa kombinasi algoritma ini cukup aman dalam menjaga kerahasiaan data karena algoritma nya cukup rumit untuk dipercahkan.

Marwa [3] melakukan penyisipan pesan yang hanya terdiri dari enam bit, serta menggunakan metode LSB Braille. Hasil dari penelitian ini memiliki kapasitas maksimum dalam penyimpanan pesan dan tetap memiliki gambar yang berkulitas tinggi.

Dari beberapa pemaparan tentang penelitian terkait, pada penelitian kali ini, peneliti akan mengkombinasikan metode *Least Significant Bit* – 2 (LSB-2) dengan metode *Least Significant Bit* – 3 dengan model penyisipan seperti papan catur *(Chess Board Pattern)* untuk melihat seberapa besar tingkat kerusakan *stego* citra yang diukur dengan *Mean Square Error* (MSE).

II. LANDASAN TEORI

A. *Steganografi*

Steganografi menjadi sebuah ilmu pengetahuan atau seni dalam berkomunikasi. Pesan disampaikan dalam bentuk tersembunyi. Sistem *steganografi* menyembunyikan isi suatu pesan atau data ke dalam media yang lain yang tidak dapat di duga oleh orang biasa sehingga tidak menimbulkan kecurigaan kepada orang yang melihatnya, gambar 1 adalah ilustrasi dasar dari konsep steganografi [4]

HIS APPLES	**H**IS **APP**LES
ARE YELLOW	ARE **Y**ELLOW
BUT MINE	**B**UT MINE
ARE RED AND	ARE **R**ED AND
WORTH MORE	WOR**T**H MORE
ANY DAY	ANY **DAY**

Gambar 1. Pesan Steganogafi dan Pesan Tersembunyi
Sumber : avoision.com

B. *Algoritma Least Significant Bit (LSB)*

Dalam teori bilangan biner, 1 byte terdiri dari 8 bit. Bit yang terdepan memiliki makna bit yang paling berarti, sehingga disebut dengan *Most Significant Bit (MSB).* Sedangkan bit yang paling belakang, memiliki makna bit yang kurang berarti, sehingga disebut dengan *Least Significant Bit (LSB).*

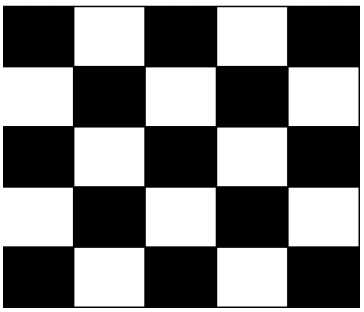
Algoritma LSB adalah salah satu algoritma yang sering digunakan pada *steganografi*, dalam proses penyisipan pesan, bit pesan akan disisipkan ke dalam bit yang paling akhir pada *pixel* citra. Berikut ini contoh penyisipan pesan huruf "N" ke dalam pixel citra, dengan metode LSB [1] :

Tabel 1. Penyisipan Pesan dengan LSB

Nilai Pixel Citra Asli	Biner Citra	LSB	Nilai Pixel Citra Baru
84	01010100	0101010**0**	84
78	01001110	0100111**1**	**79**
101	01100101	0110010**0**	**100**
95	01011111	0101111**0**	**94**
87	01010111	0101011**1**	87
98	01100010	0110001**1**	**99**
99	01100011	0110001**1**	99
100	01100100	0110010**0**	100

C. *Chess Board Pattern*

Teknik penyisipan pesan pada *pixel* citra sangat menentukan hasil *stego-image*, model *chess board pattern* adalah teknik penyisipan hasil modifikasi. Pesan akan disisipkan setiap kelang 1 *pixel*, sehingga akan berbentuk pola seperti papan catur *(chess board)* [5]



Gambar 2. *Chess Board Pattern*

D. *Mean Square Error (MSE)*

Mean Square Error (MSE) digunakan untuk mengukur berapa banyak nilai *pixel* dari *stego image* yang berbeda dengan citra aslinya. MSE dihitung dengan persamaan berikut [6] :

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2 \quad (1)$$

dimana :
I'(x,y) : Piksel citra hasil pemrosesan
I(x,y) : Piksel citra original
I : indeks matriks (Red = 1, Green = 2, Blue = 3)

III. METODOLOGI PENELITIAN

Pada penelitian ini, peneliti akan mengkombinasikan algoritma steganografi LSB-2 dan LSB-3 dengan teknik penyisipan mengikuti pola papan catur *(chess board).*

Algoritma LSB-2 dan LSB-3 merupakan hasil modifikasi dari algoritma *Least Significant Bit* (LSB). Algoritma LSB-2 melakukan penyisipan pesan pada bit ke-6, sementara algoritma LSB-3 akan melakukan penyisipan pesan pada bit ke-5.

Pada penyisipan pesan algoritma kombinasi LSB-2 dan LSB-3, bit pesan akan diambil 2 bit sekaligus dan disisipkan pada bit *pixel* citra urutan ke-5 dan ke- 6 secara bersamaan. Berikut ilustrasinya :

LSB-2 = 1 1 1 0 1 **0** 1 1
LSB-3 = 1 1 1 0 **1** 0 1 1
LSB-2 & LSB-3 = 1 1 1 0 **1 0** 1 1

Penyisipan sebuah huruf N dilakukan dengan terlebih dahulu melakukan konversi huruf N ke dalam ASCII dan bilangan biner. Sehingga diperoleh N = 78 = 01001110 (dalam biner). Berikut ini proses penyisipan pesan berupa huruf N :

Tabel 2. Penyisipan Pesan

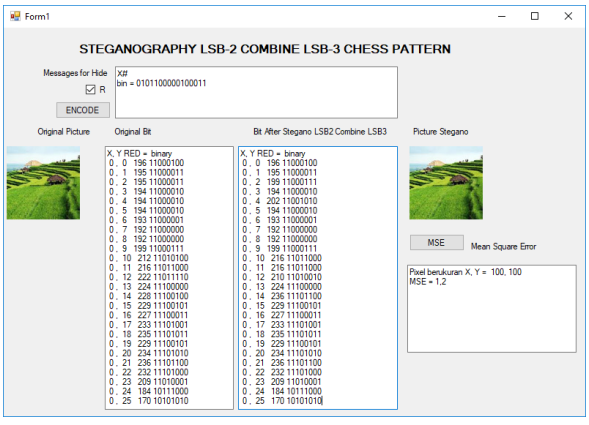
Nilai Pixel Citra Asli	Biner Citra	Kombinasi LSB-2 & LSB-3	Nilai Pixel Citra Baru
84	01010100	0101**01**00	84
78	01001110	01001110	78
101	01100101	0110**00**01	**97**
95	01011111	01011111	95
87	01010111	0101**11**11	**95**
98	01100010	01100010	98
99	01100011	0110**10**11	**107**
100	01100100	01100100	100

Dari tabel diatas dapat dilihat bahwa terdapat beberapa nilai pixel citra yang mengalami perubahan. Perubahan nilai pixel citra setelah penyisipan pesan, sedikit banyaknya akan mempengaruhi warna sebuah citra

.

IV. HASIL DAN PEMBAHASAN

Berikut ini hasil dari penyisipan pesan yang terdiri dari perbandingan gambar asli, gambar hasil penyisipan *(stego image)* dan nilai MSE :



Gambar 3. Proses Penyisipan Pesan dengan Kombinasi Steganografi LSB-2 dan LSB-2

V. KESIMPULAN

Dari penelitian ini dapat disimpulkan, bahwa :

1. Kombinasi LSB-2 dan LSB-3 mempunyai keunikan, dimana dalam setiap kali penyisipan pesan, bit pesan akan di ambil 2 bit sekaligus, dan kemudian akan disisipkan ke dalam bit pixel citra pada 2 bit yang berurutan, yaitu pada urutan bit ke -5 dan ke-6
2. Nilai MSE yang diperoleh pada gambar hasil penyisipan sebesar 1,2 %. Nilai MSE ini menunjukkan tidak terlihat adanya perubahan nilai warna yang significant dari citra hasil penyisipan terhadap citra asli

REFERENSI

[1] N. Khairina, "Perbandingan Steganografi Least Significant Bit (LSB) dengan Penyisipan Menurut Koordinat Parabola dan Koordinat Linear dalam Pengamanan Pesan Teks Pada File Bitmap", SENARAI. Medan : Universitas Sumatera Utara, 2014.

[2] T. Zebua, "Penerapan Metode LSB-2 untuk Menyembunyikan Ciphertext pada Citra Digital". Pelita Informatika Budi Darma", Vol. X No. 3, 2015.

[3] M. Emam M, A. Abdekmgeid A, & F. A. Omara, "Image Steganography Method Based on LSB Technique", "International Journal of Computer Application". 2015.

[4] E.S Wijaya & Y.Prayudi, "Konsep Hidden Message Menggunakan Teknik Steganografi Dynamic Cell Spreading", "Media Informatika", Vol. 2 No.1, 2004.

[5] J.Jiao, C.Huang, H.Lin, & G.Zhang, " A Chinese Chessboard Calibration Method in Chess-Playing Robot by Machine Vision Sensing", IOP Conf.Series: Journal of Phyisics : 1026, 2018.

[6] N.Khairina, "Analisis Steganografi Metode Two Sided Side Match", "Journal of Computer Engineering, System and Science (CESS)", Vol.1 No.2. 2016.