

# Implementasi Enkripsi Polialfabet dengan Metode LSB Steganografi dalam QR Code untuk Keamanan Tiket Konser

## *Implementation of Polyalphabetic Encryption with the LSB Steganography Method in QR Codes for Concert Ticket Security*

Adrian Fadhali Wiratama<sup>1</sup>, Nur Pratama<sup>2</sup>, Dean Adriansyah Asy'ari<sup>3</sup>

<sup>1</sup>Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa

<sup>2</sup>Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa

<sup>3</sup>Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa

<sup>1</sup>rianwiratama80@gmail.com, <sup>2</sup>nurpratama001@gmail.com\*, <sup>3</sup>deanadriansyah09@gmail.com\*

### **Abstract**

*Information security is very important. This journal discusses methods for protecting information on concert tickets by applying polyalphabetic encryption and LSB steganography techniques in QR codes. Polyalphabetic encryption is used to increase data security on concert tickets, while LSB steganography aims to hide more information in QR codes without reducing their visual clarity. Algorithm development, implementation, and performance evaluation of security solutions are discussed in this research. Experimental results show that this method successfully improves good and reliable security for verifying the authenticity of concert tickets, providing a higher level of security for real use. Therefore, it is hoped that the results of this research will increase public confidence in the security of QR Code-based concert tickets.*

**Keywords:** *Polyalphabet, Steganography, Cryptography, LSB, QR Code*

### **Abstrak**

Keamanan informasi sangat penting. Jurnal ini membahas metode untuk melindungi informasi pada tiket konser dengan menerapkan enkripsi polialfabet dan teknik steganografi LSB dalam kode QR. Enkripsi polialfabet digunakan untuk meningkatkan keamanan data pada tiket konser, sementara steganografi LSB bertujuan untuk menyembunyikan lebih banyak informasi dalam kode QR tanpa mengurangi kejelasan visualnya. Pengembangan algoritma, implementasi, dan evaluasi kinerja solusi keamanan dibahas dalam penelitian ini. Hasil eksperimen menunjukkan bahwa metode ini berhasil meningkatkan keamanan yang baik dan dapat diandalkan untuk memverifikasi keaslian tiket konser, memberikan tingkat keamanan yang lebih tinggi untuk penggunaan nyata. Oleh karena itu, diharapkan bahwa hasil penelitian ini akan meningkatkan kepercayaan masyarakat terhadap keamanan tiket konser berbasis QR Code.

**Kata kunci:** Polialfabet, Steganografi, Kriptografi, LSB, QR Code

### **Pendahuluan**

#### **Latar Belakang**

Konteks evolusi hiburan global terus berubah, dan penyelenggaraan konser, yang pada dasarnya merupakan perpaduan seni, teknologi, dan dinamika kompleks, memunculkan pertanyaan mendalam terkait dengan perlunya merespons tantangan keamanan dan integritas tiket dalam lingkup perubahan paradigma ini[1]. Di era yang diwarnai oleh penetrasi teknologi informasi yang menyeluruh dalam kehidupan sehari-hari, menjadi suatu keniscayaan untuk menanggapi ancaman manipulasi dan pemalsuan tiket konser, yang tidak hanya dapat mengakibatkan kerugian finansial bagi penyelenggara acara tetapi juga memunculkan ketidakpastian dan ketidaknyamanan bagi pengunjung[2].

Pentingnya membangun lapisan keamanan yang tangguh dan terukur dalam konteks tiket konser menjadi jelas, dan sebagai respons terhadap dinamika ini, penelitian dan inovasi terus berperan sebagai pilar penting dalam menciptakan solusi yang tidak hanya efektif tetapi juga adaptif terhadap perkembangan teknologi dan metode keamanan[3]. Dalam kaitannya dengan perlindungan data tiket, pendekatan yang melibatkan aspek enkripsi dan steganografi muncul sebagai jawaban terhadap panggilan tuntutan zaman[4].

Enkripsi polialfabet, sebagai suatu bentuk enkripsi yang menggunakan beberapa alfabet atau sandi, menawarkan perspektif keamanan yang jauh lebih kompleks dibandingkan dengan metode konvensional[5]. Terdapat kebutuhan mendesak untuk mengintegrasikan kekuatan enkripsi polialfabet dengan praktik steganografi yang cerdas, khususnya melalui metode Least Significant Bit (LSB), dalam QR Code, yang telah menjadi pilihan utama untuk tiket konser digital karena keterbacaan, kepraktisan, dan efisiensinya[6].

Steganografi LSB dalam QR Code memberikan kemampuan untuk menyisipkan informasi tambahan tanpa mengurangi kualitas visual atau fungsional QR Code[7]. Melalui penelitian ini, upaya untuk merangkai keunggulan kedua metode tersebut—enkripsi polialfabet dan steganografi LSB—dalam suatu solusi yang terintegrasi menjadi suatu eksplorasi konseptual yang mengajukan pernyataan nyata dalam mendukung keamanan tiket konser[8].

Dengan demikian, penelitian ini menggagas implementasi solusi ini sebagai langkah progresif dalam membangun sistem keamanan yang holistik dan adaptif untuk tiket konser[9]. Diharapkan bahwa hasil penelitian ini tidak hanya menjadi terobosan dalam melawan potensi pemalsuan tiket tetapi juga merangsang pertumbuhan dan inovasi dalam industri hiburan, membawa dampak positif bagi semua pemangku kepentingan, dari penyelenggara hingga pengunjung konser, melalui penyediaan pengalaman konser yang tak terlupakan dan aman[10].

### **Tinjauan Litelatur**

Tantangan keamanan tiket dalam domain konser telah menjadi fokus penelitian yang signifikan dalam beberapa tahun terakhir[11]. Dengan peningkatan risiko manipulasi dan pemalsuan tiket, para peneliti semakin tertarik untuk mencari solusi inovatif yang mampu memberikan perlindungan yang lebih kuat dan lebih canggih[12]. Sejumlah penelitian sebelumnya telah mengeksplorasi konsep enkripsi polialfabet sebagai metode keamanan yang efektif, menghadirkan lapisan kompleksitas melalui penggunaan beberapa alfabet atau sandi[13].

Pentingnya steganografi sebagai pendekatan penyembunyian informasi tambahan tanpa mengurangi kualitas media penyimpanan telah diperkuat oleh kemunculan metode Least Significant Bit (LSB)[14]. Penyisipan informasi dalam bit-bit paling tidak signifikan dari media, khususnya QR Code, telah menjadi subyek penelitian yang intensif[15]. QR Code, sebagai bentuk representasi visual dari data, menjadi target penelitian dalam konteks tiket konser digital, di mana keamanan dan keterbacaan sangat penting[16].

Beberapa penelitian terdahulu telah mendemonstrasikan keberhasilan integrasi antara enkripsi dan steganografi dalam konteks keamanan data, meskipun belum banyak penelitian yang secara spesifik memusatkan perhatian pada aplikasi kedua teknik ini dalam QR Code tiket konser[17]. Oleh karena itu, penelitian ini berusaha untuk menjembatani kesenjangan pengetahuan ini dan menyajikan kontribusi baru melalui implementasi enkripsi polialfabet dan metode steganografi LSB dalam QR Code, sebagai solusi komprehensif untuk meningkatkan keamanan tiket konser[18]-[23].

Dengan menyatukan konsep-konsep yang telah dijelajahi dalam literatur, penelitian ini diarahkan untuk memberikan pemahaman yang lebih dalam tentang kekuatan dan kelemahan kombinasi enkripsi

polialfabet dan steganografi LSB dalam melindungi integritas dan keabsahan tiket konser[24]. Diharapkan bahwa hasil penelitian ini dapat memberikan kontribusi signifikan terhadap literatur dan menjadi landasan untuk penelitian lebih lanjut dalam bidang keamanan informasi dan teknologi tiket konser[25].

### **Alasan Penelitian**

Penelitian ini dilakukan sebagai respons terhadap permasalahan serius dalam domain konser, yakni adanya potensi tiket palsu atau manipulasi data tiket dalam konteks kemajuan teknologi yang semakin pesat. Dalam lingkungan di mana tiket konser rentan terhadap risiko manipulasi dan pemalsuan, diperlukan solusi yang modern dan efektif untuk meningkatkan tingkat keamanan.

Pemilihan fokus penelitian pada enkripsi polialfabet bertujuan untuk menciptakan lapisan keamanan yang lebih tinggi dan kompleks dalam melawan potensi serangan terhadap integritas data tiket konser. Konsep ini dapat dibayangkan sebagai penggunaan beberapa kunci gembok untuk melindungi data tiket.

Selain itu, steganografi dipilih untuk dimanfaatkan karena metodenya memungkinkan penyisipan informasi tambahan dalam QR Code tanpa merusak tampilan visual atau fungsionalitas dasar QR Code itu sendiri.

Penelitian ini menggabungkan kedua konsep tersebut, yaitu enkripsi polialfabet dan steganografi, dengan tujuan menciptakan solusi yang komprehensif dan andal. Sasarannya sederhana, yakni melindungi tiket konser dari potensi pemalsuan dan memberikan tingkat keamanan tambahan untuk pengunjung dan penyelenggara acara. Harapannya, melalui penelitian ini, dapat tercipta suasana konser yang lebih aman dan nyaman bagi seluruh pihak terlibat.

### **Tujuan Penelitian**

Penelitian ini bertujuan untuk mengembangkan suatu sistem keamanan tiket konser yang efektif dan canggih dengan mengintegrasikan enkripsi polialfabet dan metode LSB steganografi dalam QR Code. Adapun tujuan khususnya meliputi:

**Meningkatkan Keamanan Tiket Konser:** Menyusun solusi keamanan yang mampu mengatasi risiko manipulasi dan pemalsuan tiket konser, sehingga meningkatkan tingkat kepercayaan baik dari pihak penyelenggara acara maupun pengunjung.

**Melindungi Integritas Data Tiket:** Mengimplementasikan enkripsi polialfabet sebagai langkah perlindungan utama untuk memastikan keutuhan dan keabsahan data tiket konser dari upaya manipulasi atau penyusupan.

**Meminimalkan Risiko Pemalsuan:** Menggunakan steganografi LSB dalam QR Code untuk menyisipkan informasi tambahan secara rahasia, sehingga merumitkan proses pemalsuan tiket dan memberikan lapisan keamanan tambahan.

**Meningkatkan Efisiensi Distribusi Tiket Digital:** Memastikan bahwa implementasi keamanan ini tidak merugikan proses distribusi tiket konser digital, melainkan meningkatkan efisiensi dan kepraktisan bagi pengguna.

**Menjadi Rujukan Inovatif:** Menyajikan kontribusi baru dalam literatur terkait keamanan tiket konser dengan menggabungkan konsep enkripsi polialfabet dan steganografi LSB dalam konteks QR Code, sehingga dapat menjadi acuan bagi penelitian selanjutnya di bidang ini.

## **Metode Penelitian**

### **Desain Penelitian**

Tujuan penelitian ini adalah untuk membuat aplikasi yang menggunakan kombinasi algoritma kriptografi Polyalphabet Cipher dan steganografi LSB (Least Significant Bit). Tujuan penelitian ini adalah untuk meningkatkan keamanan data teks yang ada di kode QR Tiket Konser.

### **Penerapan Program**

Beberapa pedoman digunakan untuk memungkinkan implementasi teknik Least Significant Bit (LSB), seperti Cipher Monoalphabetic yang berfungsi sebagai dasar untuk mengubah algoritma Cipher Polyalphabet, dan tabel ASCII 8 bit yang berfungsi sebagai dasar untuk mengonversi huruf ke dalam bilangan biner.

Polyalphabet Cipher dibuat pertama kali oleh Leon Battista pada tahun 1568. Metode ini adalah evolusi dari metode substitusi monoalphabetic. Sesuai dengan namanya, algoritma cipher polyalphabet menggunakan berbagai kunci untuk mengenkripsi kumpulan karakter atau string.

Salah satu metode steganografi paling sederhana untuk menyisipkan pesan pada media gambar adalah Least Significant Bit (LSB). Metode ini memasukkan informasi pada bit terakhir (8 bit) setiap piksel, yang berarti bahwa bit terakhir dari setiap piksel akan diubah, misalnya jika pesan rahasia adalah 01000001. Pendekatan LSB embedding dapat diterapkan pada berbagai format tipe data dan dapat digunakan untuk berbagai tujuan keamanan multimedia. Oleh karena itu, hingga saat ini, LSB masih merupakan metode steganografi yang populer.

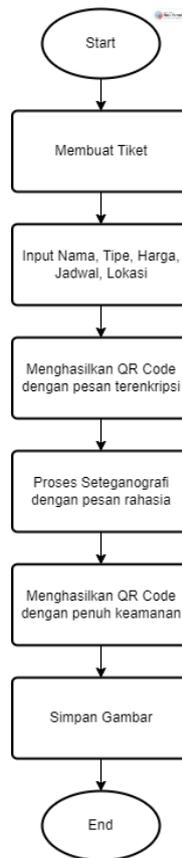
### **Rancangan Kegiatan**

Untuk memulai penelitian ini, literatur yang berkaitan dengan algoritma kriptografi Polyalphabet Cipher dan steganografi LSB akan diperiksa secara menyeluruh. Tujuan dari tahap awal ini adalah untuk mendapatkan pemahaman yang menyeluruh tentang kemajuan terbaru dan cara kedua algoritma tersebut digunakan dalam konteks keamanan data.

Setelah mendapatkan dasar teoritis yang kokoh, langkah berikutnya adalah membuat model sistem yang mengintegrasikan algoritma steganografi LSB dan kriptografi Polyalphabet Cipher. Tahap ini memerlukan perancangan model yang dapat berfungsi secara efektif dengan kedua algoritma tersebut, sehingga menghasilkan tingkat keamanan terbaik untuk data teks yang ada di kode QR Tiket Konser.

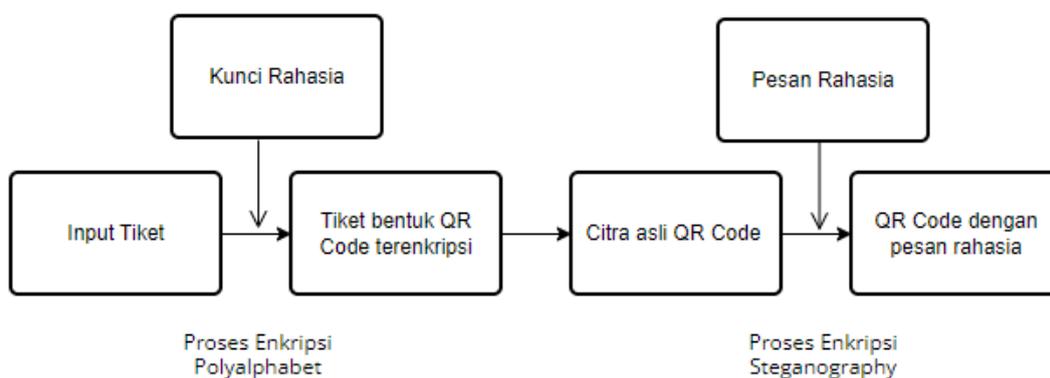
Tahap berikutnya adalah melakukan implementasi model sistem yang telah dirancang. Langkah ini akan mewujudkan model sistem secara nyata, yang akan memudahkan proses enkripsi dan dekripsi data teks dengan menggunakan kombinasi algoritma kriptografi dan steganografi.

Evaluasi keberhasilan dan tingkat keamanan metode yang digunakan adalah tahap terakhir dalam desain kegiatan ini. Pengujian menyeluruh akan mencakup elemen seperti enkripsi dan dekripsi serta analisis kemungkinan kelemahan. Hasilnya akan dianalisis secara menyeluruh untuk memberikan gambaran yang jelas tentang seberapa efektif teknik yang digunakan.



Gambar 1 Tahap Rancangan

Metode Polyalphabet Cipher digunakan untuk penyandian dan penyisipan pesan teks, yang kemudian dikombinasikan dengan Metode Steganografi LSB untuk enkripsi sistem ini. Gambar 1 menunjukkan bagaimana proses ini diterapkan pada data gambar yang termasuk dalam QR Code Tiket Konser.



Gambar 2 Penyandian

Proses enkripsi dan steganografi menggunakan elemen seperti kunci, foto asli, teks rahasia, dan teks terenkripsi. Proses dimulai dengan memilih foto asli dan menulis teks rahasia menggunakan algoritme

Polyalphabet. Kemudian, teknik steganografi digunakan untuk menyimpan dan memasukkan teks terenkripsi ke dalam foto asli. Proses ini berguna dalam banyak situasi, terutama dalam hal keamanan, privasi, dan penyimpanan data rahasia.

### Ruang Lingkup atau Objek Penelitian

Untuk mencapai tujuan utama, yaitu menciptakan aplikasi yang menggunakan kombinasi algoritma steganografi LSB dan kriptografi Polyalphabet Cipher untuk meningkatkan keamanan data teks dalam kode QR Tiket Konser.

### Tempat Penelitian

Lokasi penelitian mencakup lingkungan akademik dan pusat penelitian yang memiliki fasilitas yang tepat untuk melakukan penelitian ini, seperti laboratorium komputer dan akses internet.

### Teknik Pengumpulan Data

Data dikumpulkan menggunakan algoritma steganografi LSB dan kriptografi Polyalphabet Cipher untuk mengamankan dan menyembunyikan informasi pada data teks.

### Teknik Analisis Penelitian

Analisis penelitian mencakup evaluasi keberhasilan dan tingkat keamanan prosedur. Selain itu, hasil dibandingkan dengan pendekatan lain yang relevan. Peneliti menggunakan pendekatan interdisipliner untuk membuat aplikasi yang menggabungkan algoritma steganografi LSB dan kriptografi Polyalphabet Cipher. Harapannya, penelitian ini akan memberikan kontribusi positif untuk meningkatkan keamanan data teks dalam kode QR Tiket Konser.

### Variabel Pengujian

#### Mean Square Error (MSE)

MSE adalah metrik analisis kuantitatif yang digunakan untuk mengevaluasi kualitas citra yang dihasilkan dan keunggulan metode yang digunakan. B1 dan B2 berfungsi sebagai representasi matriks citra dalam matriks citra berukuran  $m \times n$ . Secara sederhana, Mean Square Error (MSE) adalah ukuran rata-rata dari selisih kuadrat antara sinyal piksel gambar hasil pemrosesan dan sinyal asli. Nilai MSE yang lebih rendah menunjukkan tingkat kesalahan yang lebih rendah dan kualitas gambar yang lebih baik. Nilai MSE adalah nol. Gambar menggambarkan rumus MSE.

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} [f(i, j) - g(i, j)]^2$$

Gambar 3 Rumus MSE

#### Peak Signal to Noise Ratio (PSNR)

Peak Signal-to-Noise Ratio (PSNR) adalah metrik kualitas citra yang mengukur seberapa dekat gambar yang dihasilkan oleh suatu sistem dengan gambar aslinya. Nilai PSNR yang tinggi menunjukkan kualitas gambar yang lebih baik. Rumus yang ditunjukkan di sini digunakan untuk menghitung PSNR.

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

Gambar 4 Rumus PSNR

## Hasil dan Pembahasan

Aplikasi yang dikembangkan berdasarkan algoritma Polyalphabet yang dikombinasikan dengan steganografi gambar menggunakan teknik LSB untuk keamanan teks dalam kode QR Tiket Konser harus mengikuti prosedur berikut:

### Inisialisasi Algoritma Polyalphabet

Pertama, algoritma Vigenere dimulai dengan menetapkan kunci kriptografi, yang akan digunakan untuk melindungi teks data.

### Enkripsi Data Teks

Algoritma Polyalphabet digunakan untuk mengenkripsi data teks yang akan ditukar atau disimpan. Dalam proses ini, kunci digunakan sebagai kunci enkripsi untuk menjaga keamanan konten teks. Suatu kunci digunakan untuk mengubah informasi pada gambar awal menjadi bentuk terenkripsi, dan proses dekripsi berhasil mengembalikan teks ke bentuk aslinya. Kunci yang tepat sangat penting untuk memastikan proses dekripsi berhasil. Data teks yang sudah dienkripsi dimasukkan ke dalam gambar dengan menggunakan steganografi LSB. Teknik ini menggunakan setiap piksel gambar untuk menyimpan data. sebagian dari teks data.

### Pemilihan Gambar Penyimpanan

Penetapan gambar sebagai media penyimpanan data hasil enkripsi menjelaskan proses di mana kode QR secara tidak sengaja dibuat sebagai tempat untuk menyimpan teks yang telah dienkripsi. Dalam hal ini, gambar tidak hanya berfungsi sebagai media penyimpanan tetapi juga berfungsi sebagai cara aman untuk menyembunyikan informasi yang telah dienkripsi.

### Steganografi dengan Teknik LSB

Ini menunjukkan bahwa diskusi akan melibatkan evaluasi menyeluruh dari komponen penting yang membentuk karakteristik citra. Nama file, dimensi citra (lebar x tinggi), dan ukuran file dalam kilobita (KB) adalah komponen yang paling penting dalam analisis ini. Dianggap penting untuk memahami bagaimana gambar mempengaruhi kualitas visual, kapasitas penyimpanan, dan tujuan penggunaan. Untuk menyimpan bit data teks yang telah dienkripsi, metode LSB (Least Significant Bit) steganografi menggunakan bit paling tidak signifikan pada setiap piksel gambar. Proses ini memungkinkan data disembunyikan tanpa mengurangi kualitas visual gambar.

Tabel 1 Citra Asli

Citra Asli	Ukuran Citra(Pixel)	Ukuran Citra
	200*200	18.7 kb

memberikan gambaran menyeluruh tentang ciri-ciri gambar, termasuk rincian seperti nama, dimensi, dan ukuran file. Data ini sangat penting untuk mengevaluasi pengaruh gambar terhadap kapasitas penyimpanan dan kualitas visual, seperti yang ditunjukkan dalam tabel 1.

Tabel 2 Citra Terenkripsi

Citra Terenkripsi	MSE	PSNR
	0.0	361.20199909921956

Kami melakukan analisis dan menemukan informasi tentang hasil kinerja proses enkripsi, yang mencakup nama file, teks terenkripsi, dan penilaian numerik seperti MSE dan PSNR. Penilaian ini bermanfaat untuk mengukur kemampuan enkripsi untuk mempertahankan kualitas gambar dan kemampuan gambar terenkripsi untuk menunjukkan gambar asli. Terbukti bahwa nilai MSE dan PSNR relatif rendah untuk setiap gambar, menunjukkan bahwa proses steganograp Di mana teks disimpan dalam gambar yang telah dipilih

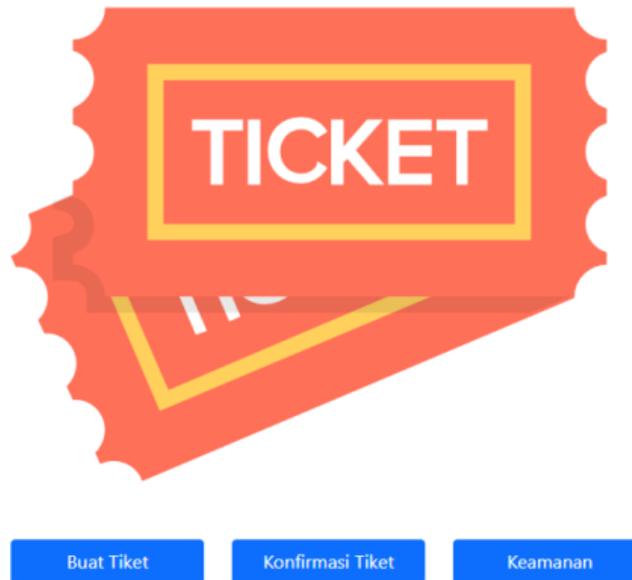
#### Simpan Gambar Termodifikasi ke dalam Galeri

Setelah data teks disematkan, gambar yang telah diubah disimpan dalam Galeri sebagai representasi visual dari informasi tersembunyi yang dapat diambil kembali melalui proses dekripsi yang tepat.

## Desain Antarmuka

Antarmuka berfungsi untuk memudahkan interaksi antara sistem dan pengguna. Gambar 6 menunjukkan antarmuka yang dirancang untuk menerapkan kriptografi menggunakan kombinasi Cipher Polyalphabet dan metode steganografi LSB pada Kode QR. Antarmuka ini ditunjukkan dalam program aplikasi.

### Sistem Tiket Konser



Gambar 5 Menu Utama

### Keamanan QR Code

Upload Image:

 No file chosen

Pesan:

Submit

Back

Gambar 6 Keamanan QR Code

## Pembuatan Tiket Konser

Nama Awal:	Nama Tengah:	Nama Akhir:
<input type="text"/>	<input type="text"/>	<input type="text"/>
Tipe Konser:		
<input type="text"/>		
Harga Konser:		
<input type="text"/>		
Jadwal Konser:		
<input type="text"/>		
Lokasi Konser:		
<input type="text"/>		
<input type="button" value="Buat QR Code"/>		

Gambar 7 Pembuatan Tiket Konser

### Kesimpulan

Terbukti bahwa kombinasi algoritma Polyalphabet Cipher dan steganografi LSB meningkatkan keamanan data teks dalam kode QR tiket konser. Penelitian ini memberikan kontribusi positif untuk pengembangan strategi keamanan data teks dalam konteks keamanan seperti QR Code tiket konser karena pendekatan metodologi yang diusulkan efektif dalam menjaga kerahasiaan dan keamanan data teks yang disimpan di dalam kode QR tiket konser. Disarankan untuk menguji teknik ini pada berbagai jenis file dan ukuran data untuk mengevaluasi kehandalan dalam konteks yang lebih luas untuk penelitian mendatang.

### Ucapan Terima Kasih

Kami sangat berterima kasih atas undangan Anda untuk mempresentasikan jurnal kami di Seminar Nasional Sains dan Teknologi Ketiga di Universitas Pelita Bangsa. Kami sangat berterima kasih atas kesempatan ini untuk berbagi hasil penelitian kami tentang peningkatan keamanan data teks dalam kode QR tiket konser dengan menggunakan algoritma Polyalphabet Cipher dan steganografi LSB. Kami berharap penelitian ini akan memberikan kontribusi positif untuk pengembangan strategi untuk meningkatkan keamanan data teks dalam kode QR tiket konser. Saya ingin mengucapkan terima kasih atas kesempatan ini.

## Daftar Rujukan

- [1] Merliana, Ni Putu Eka. "Pemanfaatan Teknologi Kriptografi dalam mengatasi kejahatan Cyber." *Satya Dharma: Jurnal Ilmu Hukum* 3, no. 2 (2020): 23-40. <https://ejournal.iahntp.ac.id/index.php/satya-dharma/article/view/678>
- [2] Afsari, Melani, Dadang Iskandar Mulyana, Alfiani Damaiyanti, and Naini Sa'adah. "Implementasi Mode Operasi Kombinasi Cipher Block Chaining dan Metode LSB-1 Pada Pengamanan Data text: indonesia." *Jurnal Pendidikan Sains dan Komputer* 2, no. 01 (2022): 70-82. <http://teknois.stikombinaniaga.ac.id/index.php/JBS/article/view/87>
- [3] Abdillah, Muhammad Oemar, Ogie Ariansah Pane, and Farhan Rusdy Asyhary Lubis. "Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB)." *Jurnal Sains dan Teknologi (JSIT)* 3, no. 1 (2023): 40-46. <http://www.jurnal.minartis.com/index.php/jsit/article/view/482>
- [4] GIRSANG, NARDIANTI DEWI. "PERANCANGAN SISTEM INFORMASI ABSENSI KARYAWAN DENGAN QR CODE BERBASIS WEB PADA PT. SALIM IVOMAS PRATAMA Tbk." *Circle Archive* 1, no. 1 (2023). <http://circle-archive.com/index.php/carc/article/view/2>
- [5] Abdillah, Muhammad Oemar, Ogie Ariansah Pane, and Farhan Rusdy Asyhary Lubis. "Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB)." *Jurnal Sains dan Teknologi (JSIT)* 3, no. 1 (2023): 40-46. <http://jurnaldigit.org/index.php/digit/article/view/78>
- [6] NISAK, CHOIROTON. "PENGARUH CITRA MEREK, KEAMANAN DAN KEMUDAHAN TERHADAP KEPUTUSAN PEMBELIAN TIKET PESAWAT PADA TIKET. COM." PhD diss., Universitas Mercu Buana Jakarta, 2022. <https://repository.mercubuana.ac.id/71173/>
- [7] Prabowo, Muhammad Jerry, and Riki Wanto. "Implementasi Steganografi Berbasis Mobile Menyembunyikan Pesan Gambar Dan Suara." *Jurnal Merdeka Informatika* 1, no. 1 (2023): 33-36. <https://jurnal.atmosferdigital.com/index.php/jmi/article/view/22>
- [8] xSyahril, Muhammad, and Hendra Jaya. "Aplikasi steganografi pengamanan data nasabah di Standard Chartered Bank menggunakan metode Least Significant Bit dan RC4." In *Seminar Nasional Sains dan Teknologi Informasi (SENSASI)*, vol. 2, no. 1. 2019. <https://jurnal.atmosferdigital.com/index.php/jmi/article/view/22>
- [9] Wiranata, Ade Davy, and Rima Tamara Aldisa. "Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA." *Jurnal JTik (Jurnal Teknologi Informasi dan Komunikasi)* 5, no. 3 (2021): 277-281. <https://scholar.archive.org/work/el44wbhe2zejvbn6mxo5tj6w4/access/wayback/http://journal.lembagakita.org/index.php/jtik/article/download/219/pdf>
- [10] Aulia, Shabila Fitri, and Siti Sauda. "IMPLEMENTASI ALGORITMA STEGANOGRAFI FIRST OF FILE DAN END OF FILE UNTUK PENYISIPAN TEXT DALAM GAMBAR." *Jurnal Nasional Ilmu Komputer* 1, no. 2 (2020): 93-104. <http://journal.jis-institute.org/index.php/jnik/article/view/156>
- [11] Musri, Tengku, and Awang Pradana. "PERANCANGAN ENKRIPSI KEAMANAN DATA MENGGUNAKAN METODE LEAST SIGNIFICANT BIT DENGAN TEKNIK MODIFIKASI RANDOM DATA ENCRYPT ALGORITHM UNTUK AUDIO STEGANOGRAPHY." *Elektrika Borneo* 6, no. 2 (2020): 48-53. <http://180.250.193.171/index.php/elektrika/article/view/1649>
- [12] Ramadhani, A. Muh, and Tasrif Hasanuddin. "Modifikasi Least Significant Bits pada Gambar sebagai Data Hiding Steganography." *Indonesian Journal of Data and Science* 2, no. 2 (2021): 91-102. <https://www.jurnal.yoctobrain.org/index.php/ijodas/article/view/48>
- [13] Gustiawan, Andre, Jusuf Wahyudi, and Eko Suryana. "Perancangan Aplikasi Steganografi Pada Citra Digital Menggunakan Metode Pixel Value Differencing." *JUKI: Jurnal Komputer dan Informatika* 5, no. 1 (2023): 151-163. <https://ioinformatic.org/index.php/JUKI/article/view/213>

- [14]Hasugian, Penda Sudarto. "Analisa Metode Least Significant Bit Dalam Penyisipan Pesan Terenkripsi Terhadap Citra Digital: Analysis of the Least Significant Bit Method in Inserting Encrypted Messages against Digital Images." *Journal Of Computer Networks, Architecture and High Performance Computing* 1, no. 1 (2019): 21-25. <https://jurnal.itscience.org/index.php/CNAPC/article/view/45>
- [15]Dewi, Novita Permata, David JM Sembiring, Raheliya BR Ginting, and Meiliyani BR Ginting. "Pengamanan Data dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma Luc Serta Steganografi Chaotic Lsb." *Jurnal Syntax Admiration* 3, no. 2 (2022): 341-361. <https://www.jurnalsyntaxadmiration.com/index.php/jurnal/article/view/389>
- [16]Setiawan, Nanda, and Lili Tanti. "Kerahasiaan Teks Yang Disisipkan Ke Dalam Gambar Menggunakan Metode Porta Dan LSB." *Information Technology and Cyber Crime (ITCC)* 1, no. 1 (2022): 52-58. <http://download.garuda.kemdikbud.go.id/article.php?article=3328402&val=29177&title=Kerahasiaan%20Teks%20Yang%20Disisipkan%20Ke%20Dalam%20Gambar%20Menggunakan%20Metode%20Porta%20Dan%20LSB>
- [17]Agustini, Siti, and Muchamad Kurniawan. "Peningkatan Keamanan Teks Menggunakan Kriptografi Dan Steganografi." *Scan: Jurnal Teknologi Informasi dan Komunikasi* 14, no. 3 (2019): 33-38. <http://www.ejournal.upnjatim.ac.id/index.php/scan/article/view/1685>
- [18]Tarigan, Ranga Satya, and Guruh Dwiatma. "ANALISA STEGANOGRAFI DENGAN METODE BPCS (Bit-Plane Complexity Segmentation) DAN LSB (Least Significant Bit) PADA PENGOLAHAN CITRA." (2022). <https://osf.io/948ps/download>
- [19]Nasution, Yusuf Ramadhan, Mhd Furqan, and Meri Sinaga. "Implementasi Steganografi Menggunakan Metode Spread Spectrum Dalam Pengamanan Data Teks Pada Citra Digital." *J-SAKTI (Jurnal Sains Komputer dan Informatika)* 4, no. 2 (2020): 351-358. <http://tunasbangsa.ac.id/ejurnal/index.php/jsakti/article/view/226>
- [20]Handayani, Tri, Tri Yuliati, and Siti Patimah. "Implementasi Steganografi Dengan Metode End Of File (EOF) Untuk Menyisipkan Pesan Teks Pada Gambar." *Jurnal Fasilkom* 11, no. 3 (2021): 143-149. <https://ejurnal.umri.ac.id/index.php/JIK/article/view/3124>
- [21]Nugroho, Catur. "Steganografi Pada Pengiriman Teks Pesan Gambar dengan Metode Least Significant Bit & Steghide." *Jurnal Ilmu Siber (JIS)* 1, no. 4 (2022): 113-116. <https://jurnal.unsia.ac.id/index.php/jis/article/view/373>
- [22]Prahmana, I. Gusti. "IMPLEMENTASI ALGORITMA OTP DAN STEGANOGRAFI EOF DALAM PENYISIPAN PESAN TEKS PADA CITRA." *JTIK (Jurnal Teknik Informatika Kaputama)* 6, no. 2 (2022): 457-465. <https://jurnal-backup.kaputama.ac.id/index.php/JTIK/article/view/850>
- [23]Sephiana, Nuke, Muhlis Tahir, Shinta Dwi Wulandari, Faizal Reza Rahmansyah, Rofikoh Nabila Nuvitasari, and Ray Albian Prakasa. "Analisis Perbandingan Algoritma Monoalphabetic Cipher dan Polyalphabetic Substitution Cipher pada Sistem keamanan Data." *Explore IT: Jurnal Keilmuan dan Aplikasi Teknik Informatika* 15, no. 1 (2023): 16-21. <https://jurnal.yudharta.ac.id/v2/index.php/EXPLORE-IT/article/view/3823>
- [24]Putri, Rahmawati Awwaliyah, Kiswara Agung Santoso, and Ahmad Kamsyakawuni. "Pengkodean Polyalphabetic dengan Modifikasi Algoritma ElGamal-Caesar Cipher." In *PRISMA, Prosiding Seminar Nasional Matematika*, vol. 4, pp. 540-547. 2021. <https://journal.unnes.ac.id/sju/index.php/prisma/article/view/45022>
- [25]Sephiana, Nuke, Muhlis Tahir, Shinta Dwi Wulandari, Faizal Reza Rahmansyah, Rofikoh Nabila Nuvitasari, and Ray Albian Prakasa. "Analisis Perbandingan Algoritma Monoalphabetic Cipher dan Polyalphabetic Substitution Cipher pada Sistem keamanan Data." *Explore IT: Jurnal Keilmuan dan Aplikasi Teknik Informatika* 15, no. 1 (2023): 16-21. <https://jurnal.yudharta.ac.id/v2/index.php/EXPLORE-IT/article/view/3823>