JUSTIN
Jurnal Sistem dan Teknologi Informasi
p-ISSN : 2460-3562 / e-ISSN : 2620-8989

DOI: 10.26418/justin.v11i3.66716
Vol. 11, No. 3, Juli 2023

CHESTEGA: Steganografi Menggunakan Standar PGN dalam Permainan Catur Berbasis Web

Nandhitta Aemy[1], Muhammad Al-Husaini[2]

[1]*Program Studi Sarjana Informatika Fakultas Teknik Universitas Siliwangi*
Jl. Siliwangi No. 24, Kahuripan, Kota Tasikmalaya, Jawa Barat 46115

[1]207006053@student.unsil.ac.id
[2]alhusaini@unsil.ac.id

Abstrak

Catur merupakan permainan paling popular di dunia, dimainkan oleh jutaan manusia terlepas dari berapa pun usia mereka. Saking populernya permainan ini, selama Perang Dunia II permainan catur sering digunakan sebagai media menyembunyian pesan rahasia oleh para tantara yang kemudian disebut steganografi. Para tentara tersebut mengirim pesan melalui permainan catur menggunakan sebuah notasi untuk menentukan penempatan dan analisis. Maka dapat disimpulkan bahwa Steganografi merupakan seni menyembunyikan pesan rahasia sehingga keberadaan pesan tersebut menjadi tidak dapat diketahui keberadaannya. Hal ini dianggap lebih efektif dibandingkan penyamaran pesan atau disebut juga kriptografi. Seiring berkembangnya teknologi dan informasi, notasi catur tersebut berevolusi menjadi PGN atau Portable Game Notation. PGN bukanlah satu-satunya notasi catur yang ada, tetapi PGN merupakan notasi catur resmi yang paling popular dalam pengkomputerisasian permainan catur. Pada penelitian ini akan membahas tentang Implementasi steganografi pada permainan catur yang diterapkan pada aplikasi berbasis web yang dapat melakukan enkripsi dan dekripsi pesan menggunakan algoritma LSB.

Kata kunci: Catur, Steganografi, PGN, LSB

CHESTEGA: Steganography Using the PGN Standard in Web-based Chess Games

Abstract

Chess is the most popular game in the world, played by millions of people regardless of their age. Because of its popularity, during World War II chess was often used as a medium to hide secret messages by soldiers, which was later called steganography. The soldiers sent messages through the chess game using a notation to determine placement and analysis. So it can be concluded that Steganography is the art of hiding secret messages so that the existence of the message becomes unknowable. This is considered more effective than message masking or also called cryptography. As technology and information developed, the chess notation evolved into PGN or Portable Game Notation. PGN is not the only chess notation that exists, but PGN is the most popular official chess notation in computerizing chess games. This research will discuss the implementation of steganography in chess games applied to web-based applications that can encrypt and decrypt messages using the LSB algorithm.

Keywords: Chess, Steganography, PGN, LSB

I. PENDAHULUAN

Penyembunyian informasi dan transmisi pesan rahasia telah dipraktekkan sejak zaman peradaban kuno. Teknik-teknik yang ditempuh dibidang tersebut disebut dengan Steganografi. Steganografi kini telah berkembang semakin canggih selama bertahun-tahun, terutama dengan ketersediaan media digital [1]. Tujuan dari steganografi ini sendiri bukan hanya untuk mencegah musuh mendeteksi dan mengganggu isi pesan, tetapi juga untuk menghindari timbulnya kecurigaan dalam komunikasi rahasia [2]. Steganografi melibatkan tiga langkah; menyandikan pesan, menyematkan pesan yang disandikan ke dalam sampul yang sesuai dan kemudian mengirim sampul tersebut kepada penerima. Secara teknis, langkah kedua merupakan faktor penting yang berperan sebagai pembeda diantara berbagai teknik staganografi. Pendekatan kotemporer sering dikategorikan berdasarkan jenis sampul steganografi seperti teks, gambar, audio ataupun grafik [3].

Metodelogi steganografi yang digunakan pada penelitian ini mengadopsi dari penelitian [4] adalah permainan catur atau Chestega. Chestega menyembunyikan pesan dengan 3 langkah. Pertama, menentukan parameter pengkodean, yang berarti aspek

permainan apa yang akan digunakan untuk menyimpan kode steganografi. Contoh parameter pengkodean termasuk papan catur, bidak, gerakan, dan sebagainya. Ini adalah langkah inisialisasi yang harus disepakati oleh pihak yang berkomunikasi. Kedua, Chestega mengekspresikan pesan menggunakan parameter pengkodean yang dipilih. Ketiga, dapat menyamarkan pesan dalam sampul catur.

Keuntungan utama Chestega dibandingkan pendekatan lain adalah sebagai berikut; Karena pesan tidak disembunyikan sebagai suara, dengan sampul catur, bentuk pesan tersembunyi adalah anti-distorsi. Chestega adalah pendekatan publik yang tidak bergantung pada kerahasiaan tekniknya atau membutuhkan stega-key [5]. Chestega juga tahan terhadap serangan perbandingan dengan menggunakan data yang tidak dapat dilacak atau diautentikasi. Terakhir, popularitas Catur memberikan pembenaran yang cukup untuk transmisi penutup catur di antara pihak komunikasi dan akan membantu dalam kamuflase proses komunikasi [6].

Memanfaatkan penggunaan permainan untuk menyembunyikan pesan telah dipertimbangkan oleh penelitian [7], [8]. Pada dasarnya, skrip game disarankan sebagai sampul tempat pesan disembunyikan dalam Gerakan atau komentar. Namun, pekerjaan ini memberikan opsi terbatas untuk pesan dan tidak mempertimbangkan implikasi pengkodean ada urutan gerakan maupun penggunaan data yang diautentikasi dalam hal turnamen dan permainan yang dikenal. Selain itu, pendekatan yang diusulkan rentan terhadap serangan kontras dimana ututan gerakan tidak sesuai dengan alur permainan secara logis, sebagian besar disebabkan oleh proses penyembunyian pesan. Selain itu, rentan terhadap perbandingan dan serangan lalu lintas.

II. METODOLOGI PENELITIAN

Gambar 1. Alur Metode

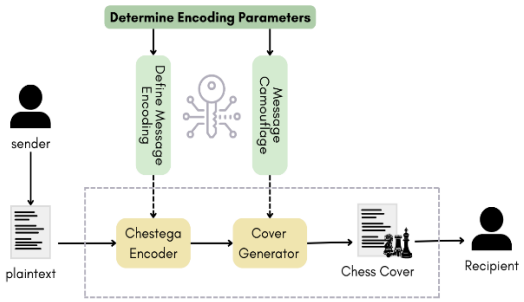
A. *Pengumpulan Data*

Langkah awal dalam metodologi adalah dengan cara melakukan study literature untuk mencari bahan objek permasalahan yang dapat digunakan sebagai acuan dalam pengembangan aplikasi yang dibuat.

B. *Perancangan*

Chestega menghindari kecurigaan dalam komunikasi rahasia dengan menyembunyikan pesan menggunakan data catur. Data catur dalam konteks ini mencakup posisi papan catur, bidak beserta warnanya, gerakan, nama turnamen, tempat dan hasil permainan. Data ini dapat dimanfaatkan untuk menyembunyikan pesan dalam skrip gerapan dalam permainan, analisis permainan, dan sebagainya. Data yang dipalsukan tidak selalu harus terlihat normal dan sah, misalnya hanya mencerminkan gerakan legal, tetapi mungkin dalam bentuk lain seperti gerakan atau posisi illegal, penggunaan gerakan illegal sering terjadi [9], [10].

Chestega terdiri dari tiga modul yang tujuan utamanya adalah untuk menentukan konfigurasi bagi pihak-pihak yang berkomunikasi menggunakan Chestega. Modul pertama menentukan parameter encoding chestega, bertujuan untuk menentukan jenis permainan yang akan digunakan untuk menanam kode steganografi. Parameter ini kemudian digunakan oleh modul kedua dan ketiga untuk menentukan encoder pesan dan skema kamuflase yang akan digunakan [4].



Gambar 2. Skema interaksi modul Chestega

1) *Determining Encoding Parameters*

Dalam modul pertama Chestega, yaitu penentuan parameter pengkodean, terdapat beberapa aspek tentang permainan catur yang menjadi pertimbangan. Aspek tersebut meliputi kotak-kotak pada papan catur, bidak-bidak, gerakan, pemain, waktu berpikir, dan sebagainya. Modul pengkodean Chestega memanfaatkan informasi ini untuk menentukan parameter yang akan digunakan dalam menyembunyikan pesan.

Proses seleksi parameter ini dipengaruhi oleh beberapa faktor, seperti ukuran pesan yang akan disandikan, gaya sampul yang digunakan, dan ketersediaan data otentik yang sesuai dengan pesan yang akan disembunyikan. Sebagai contoh, kita dapat mengasumsikan bahwa kotak-kotak persegi dengan angka yang berurutan pada papan catur dapat mewakili bidak-bidak yang akan digunakan untuk menyembunyikan bagian dari pesan. Namun, perlu diingat bahwa ukuran maksimum pesan akan dibatasi oleh jumlah bidak yang tersedia (16) dan jumlah kotak pada papan catur (64). Dengan demikian, pesan yang disandikan tidak akan melebihi 96 bit (16 bidak x 6 bit dari 64 kotak). Pesan ini kemudian dapat direpresentasikan sebagai urutan gerakan dalam permainan catur [4].

Dalam memilih parameter pengkodean, penting untuk mempertimbangkan batasan-batasan ini agar pesan dapat disandikan dengan baik dalam konteks permainan catur. Selain itu, parameter pengkodean juga dapat dipilih untuk memastikan bahwa pesan tersembunyi tidak menimbulkan kecurigaan dan terlihat sejalan dengan alur permainan yang logis.

2) *Defining Message Encoder*

Modul kedua dari Chestega adalah penentuan encoder pesan, yang bertanggung jawab untuk membuat representasi pengkodean dari pesan teks dan menyamarinya di dalam papan catur. Dalam Chestega, terdapat beberapa kendala yang perlu diperhatikan oleh

encoder pesan dalam menghasilkan kode steganografi yang akan disematkan ke dalam papan catur.

Misalnya, jika papan catur digunakan sebagai parameter encoding, encoder pesan harus memperhatikan bahwa tidak setiap kotak pada papan catur akan digunakan dan variasi nilai data harus dipertimbangkan. Sebagai contoh, gerakan bidak catur dapat menjadi salah satu parameter yang digunakan dalam metode ini. Pesan dapat disembunyikan dengan memanfaatkan nama-nama pemain, lokasi turnamen, atau teknik pembukaan (*opening techniques*) .

Berdasarkan metode pengkodean karakter, encoder pesan akan mencari data konfirmasi yang sesuai dengan nilai yang terkait dalam papan catur. Sebagai contoh, pesan akan dikodekan menjadi string biner dan kemudian dibagi menjadi kelompok-kelompok dengan jumlah bit tertentu yang telah disepakati oleh pihak yang berkomunikasi. Hal ini dilakukan untuk memastikan bahwa semua kendala pada rentang nilai kode steganografi terpenuhi [11]. Sebagai contoh, jika pengelompokan dilakukan dengan menggunakan 7-bit, maka nilai-nilai yang dihasilkan akan berada dalam rentang [0, 127] (0.000.000 - 1.111.111 dalam bentuk biner).

Berikut ini menjelaskan pengkodean pesan:

- Plaintext dari pesan tersebut adalah “informatika 2020”
- String biner bersambung dari representasi kode ASCII pesan adalah “01101001011011100110011001101111011010 00011011010110000101110100011010010110101101100001001000000011001000011000000110010001100100"
- Membagi string menjadi 7-bit masing-masing, yang ditetapkan dan disepakati oleh pihak yang berkomunikasi sehingga menghasilkan “0110100 1011011 1001100 0110111 1011010 0011011 0110110 1100001 0111010 0110100 1101011 0110000 0100100 0000110 0100011 0011001 0”
- Konversi isian pada setiap individu menjadikannya hasil decimal “52 91 76 55 90 27 54 97 58 52 107 48 36 6 35 25”

Perlu diperhatikan bahwa rentang nilai desimal yang dihasilkan dapat dengan mudah menyempit atau melebar dengan membagi string biner ke dalam kelompok kurang atau lebih dari 7 bit. Skema pengkodean ini hanya untuk ilustrasi; banyak skema alternatif yang dapat digunakan.

3) Message Camouflaging Scheme

Modul ketiga dari Chestega adalah skema kamuflase pesan, yang bertujuan untuk menyamarkan pesan dengan menyembunyikan pesan yang telah dikodekan ke dalam papan catur. Dalam Chestega, digunakan subset data yang dipilih untuk meningkatkan ketahanan terhadap serangan. Dalam praktiknya, penyerang harus mencoba semua kemungkinan subset data untuk mencari sesuatu yang relevan, dengan asumsi bahwa penyerang menduga adanya pesan tersembunyi dalam suatu subset tertentu dari dokumen yang terkait dengan papan catur [9]. Selain itu, penyerang juga harus mencoba menebak skema pengkodean yang digunakan.

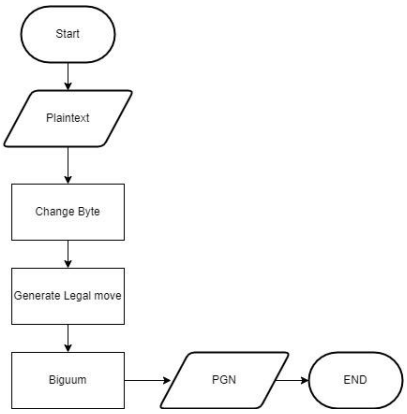
Melalui Chestega, sulit bagi musuh untuk mengidentifikasi parameter yang digunakan dalam proses penyembunyian pesan, terutama ketika tidak ada interaksi eksplisit antara pengirim dan penerima pesan. Dalam konteks Chestega, sebuah papan catur dapat fokus pada satu permainan tunggal atau mungkin melibatkan diskusi tentang beberapa permainan [12].

Dengan menggunakan papan catur sebagai wadah untuk menyembunyikan pesan, Chestega memberikan lapisan tambahan proteksi terhadap serangan dan menjaga keamanan komunikasi rahasia. Sebuah wadah (papan catur) dapat focus pada permainan tunggal atau dengan mendiskusikan beberapa permainan [13], [14]. Beberapa tema untuk berkomunikasi dengan koleksi game:

- Strategi permainan catur
- Posisi dari beberapa potongan atau penerapan konsep seperti scarifyings, mengendalikan file yang terbuka, benteng atau berlawanan kastil
- Nama-nama pemain catur, turnamen dan acara
- Tanggal dan tempat permainan, misalnya negara dan kota
- Aspek politik atau persaingan dari permainan yang dimainkan, misalnya AS vs Uni Soviet.

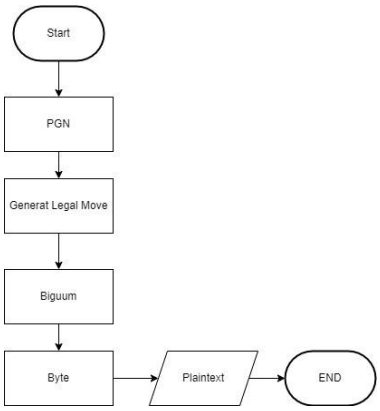
Hal yang harus diperhatikan bahwa mengidentifikasi tema dan menghasilkan teks untuk melegistimasi kemunculan game yang tidak terkait dalam cover catur dapat secara otomatis menggunakan system *Natural Language Generation* (NLG) [6]. Jenis wadah paling intuitif adalah penggunaan gambar, bila menggunakan papan catur sebagai encodingnya.

Kemudian kami menggunakan flowchart untuk mengatahui gambaran dari bagaimana sistem atau jalannya aplikasi secara terstruktur. Alur secara garis besar dapat dilihat pada gambar-gambar dibawah ini.



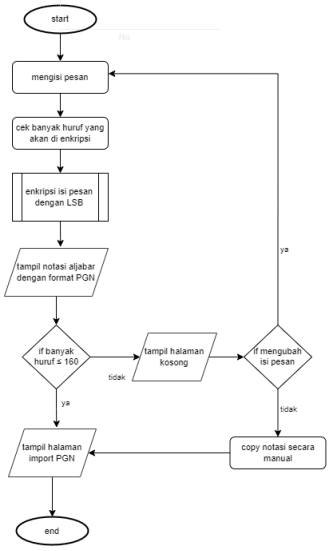
Gambar 3. *Flowchart* Proses Enkripsi Algoritma LSB

Dapat dilihat bahwa Gambar 3 tersebut menggambarkan alur dari proses enkripsi pesan menggunakan algoritma LSB.



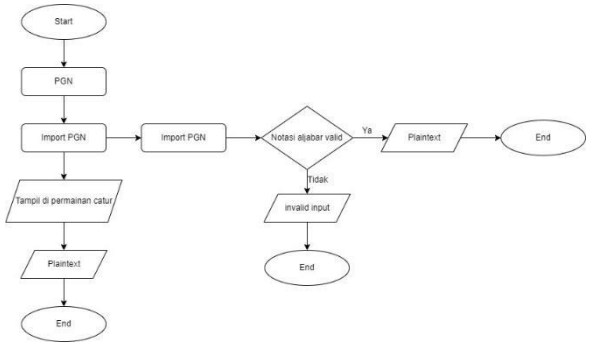
Gambar 4. *Flowchart* Proses Dekripsi Algoritma LSB

Pada Gambar 4 tersebut, menggambarkan alur dari proses dekripsi pesan menggunakan algoritma LSB.



Gambar 5. *Flowchart* Proses Enkripsi Notasi PGN

Gambar 5 merupakan alur dari proses enkripsi pesan menjadi sebuah notasi aljabar berupa PGN.



Gambar 6. *Flowchart* Proses Dekripsi Notasi PGN

Selanjutnya, Gambar 6 merupakan alur dari proses dekripsi notasi PGN menjadi sebuah plaintext.

C. Konfigurasi

Pengirim dan penerima yang berkomunikasi secara tersembunyi menggunakan chestega harus setuju pada paraturan-peraturan konfigurasi berikut:

1) Spesifikasi tertentu dari pesan yang menggunakan skema *encoding* atau *decoding* termasuk parameter yang digunakan untuk menyembunyikan pesan.
2) Gaya dan jenis *cover* catur sehingga penerima tahu apa yang harus memecahkan kode
3) Bagaimana membangun jaringan komunikasi rahasia yang memungkinkan pengirim dan penerima untuk dapat berkomunikasi, yaitu memberikan *cover* chestega kepada penerima item.

Pendekatan steganografi kontemporer dalam literature telah berfokus pada bagaimana untuk menyembunyikan pesan dan bukan pada bagaimana untuk menyamarkan pengirimannya [15]. Meskipun demikian dikatakan bahwa pengiriman cover rahasia steganografi sangat penting untuk keberhasilan steganografi. Transmisi pesan eksplisit bukan satu-satunya sarana untuk berbagi cover, web posting di forum diskusi publik dan majalah melalui layanan pos adalah cara lain yang bisa digunakan untuk berbagi cover. Singkatnya, cara penyampaian pesan tersembunyi dapat menimbulkan kecurigaan bahkan ketika menggunakan teknik steganografi yang tangguh sekalipun.

D. Implementasi

Metode terakhir ini berisikan tentang pengimplementasian dari aplikasi yang dapat dilihat pada tampilan program yang berhasil dibuat. Dimana didalamnya diterapkan beberapa aturan khusus diantaranya menghindari skakmat dan mengabaikan hasil imbang. Hal ini dilakukan karena kemungkinan ada beberapa set data yang tidak dapat dikodekan sama sekali karena skakmat, dimana tidak ada gerakan yang sah. Selain itu, langkah yang dimainkan dalam permainan ini mengabaikan aturan 50 langkah hal ini disebabkan oleh algoritma tidak tahu apa yang membuat langkah masuk akal atau tidak masuk akal. Algoritma ini hanya memainkan gerakan berdasarkan gerakan apapun yang mengkodekan data. Implementasi ini selebihnya akan dibahas pada bagian selanjutnya yaitu hasil dan pembahasan.

III. HASIL DAN PEMBAHASAN

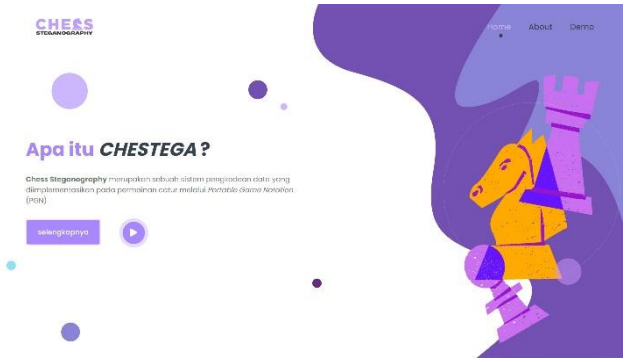
Pada bagian ini menunjukan penerapan chestega dan teknik untuk memvalidasi kelayakan dari proses penyembunyian melalui dua contoh. Dalam contoh yang pertama, kita akan melakukan enkripsi dan dekripsi pesan menggunakan papan catur sebagai wadah untuk pengkodean pesan. Contoh kedua adalah melakukan dekripsi menggunakan notasi PGN secara asal. Beberapa contoh ini juga yang menunjukkan bagaimana seorang dapat menentukan konfigurasi chesteganya. Selain itu, tujuan dari bagian ini adalah untuk menunjukkan kemampuan chestega dalam menyembunyikan data, dari pada membuat musuh sulit untuk memecahkan kode pesan.

Gambar-gambar dibawah ini merupakan tampilan web untuk user, yang dibagi menjadi 2 section tampilan yang berfungsi untuk memudahkan seorang user. Section pertama yaitu introduction atau pengenalan singkat tentang chesteg, Portable Game Notation (PGN), juga bidak catur. Dan yang kedua adalah Section demo yang menjadi inti

dari web ini dimana pengimplementasian Chestega dilakukan.

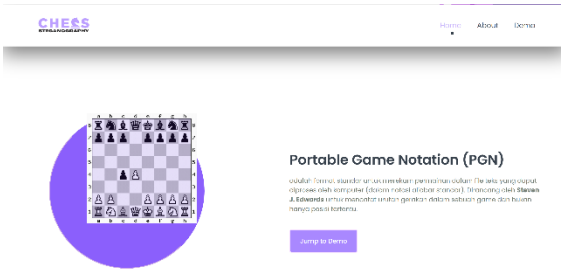
Gambar 7. UI Aplikasi *web* Chestega

Gambar 7 merupakan tampilan full-page dari aplikasi website Chestega secara menyeluruh.



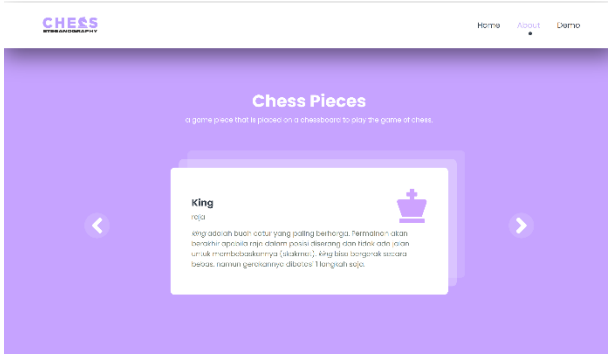
Gambar 8. UI *Section: Home* pada Web

Gambar 8 merupakan tampilan dari halaman Home yang berisikan tentang informasi singkat mengenai chestega. Kemudian, ketika user menekan tombol play, maka akan muncul pop-up yang berisikan video demo penggunaan aplikasi chestega yang berfungsi sebagai tutorial. Halaman ini disajikan dengan mengutamakan keramahan pengguna atau user-friendly, hal ini bisa dilihat dari berbagai animasi dan tema warna yang menarik, juga segala kemudahan yang tersedia pada website.



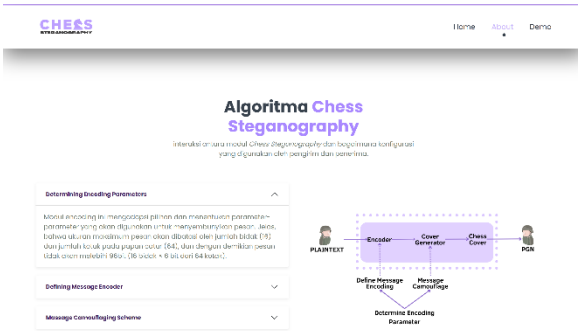
Gambar 9. UI *Section: About* (PGN) pada Web

Gambar 9 merupakan tampilan dari halaman About yang berisikan tentang informasi singkat mengenai Portable Game Notation (PGN).



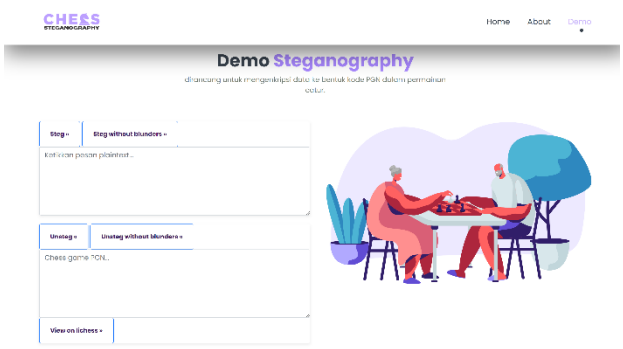
Gambar 10. UI *Section: About* (Bidak Catur)pada Web

Masih berada dihalaman About, Gambar 10 ini berisikan tentang informasi singkat mengenai bidak-bidak catur seperti King, Queen, Bishop, Knight, Rook dan Pion.



Gambar 11. UI *Section: About* (Algoritma) pada Web

Gambar 11 merupakan tampilan terakhir dari section About, berisikan tentang algoritma dan modul yang digunakan dalam perancangan aplikasi.

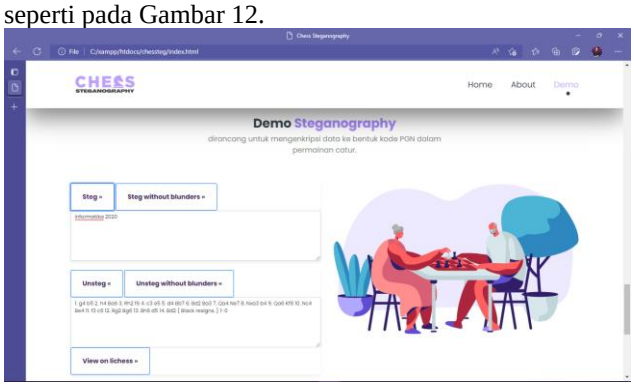


Gambar 12. UI *Section: Demo* pada Web

Gambar 12 merupakan tampilan layar untuk halaman Demo, pada halaman inilah user melakukan proses enkirpsi dan dekripsi steganografi. Tersedia 2 form dengan fungsi yang berbeda, form bagian atas merupakan form untuk menginputkan pesan, sedangkan form bagian bawah merupakan output notasi PGN yang dihasilkan.

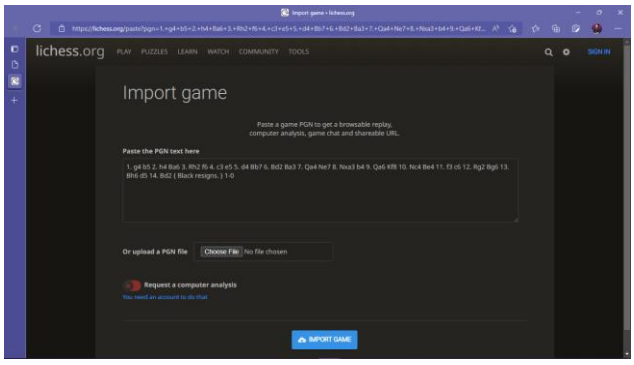
A. *Pengujian Enkripsi pada Program Aplikasi*

Pengujian pertama adalah uji coba proses enkripsi pesan ke notasi PGN. Pengujian ini dilakukan pada section demo seperti pada Gambar 12.



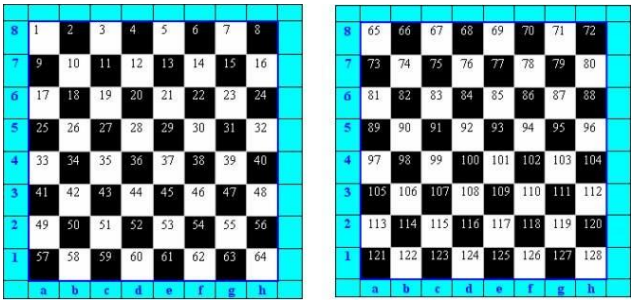
Gambar 13. Pengujian Enkripsi

Gambar 13 merupakan tampilan layar dari pengujian aplikasi steganografi. Pada form atas berisikan tentang teks yang akan dienkripsi, sedangkan form bawah merupakan hasil dari enkripsi, berupa notasi aljabar PGN. Selanjutnya untuk melihat pengimplementasian notasi tersebut pada papan catur, user hanya perlu menekan button yang bertuliskan "view on lichess", yang kemudian akan mengarahkan user ke halaman lichess.org untuk mengimport notasi aljabar seperti yang ada pada gambar 14 dibawah ini.



Gambar 14. UI *Import Game* pada web lichess.org

Secara intuitif, papan catur adalah hal yang paling dasar untuk encoding, skema pengkodean dari contoh ini mirip yang dibahas dalam bagian 3. Papan catur berukuran 8×8 persegi, yang membuat total 64 kotak seperti yang diperlihatkan pada gambar 14. Karena bidak catur memiliki dua warna hitam dan putih, sehingga pengkodean papan catur akan menjadi dua kali lipat dari yang sebelumnya 64 kotak menjadi 128 kotak.



Gambar 15. Dua sisi pada Papan Catur (B&W)

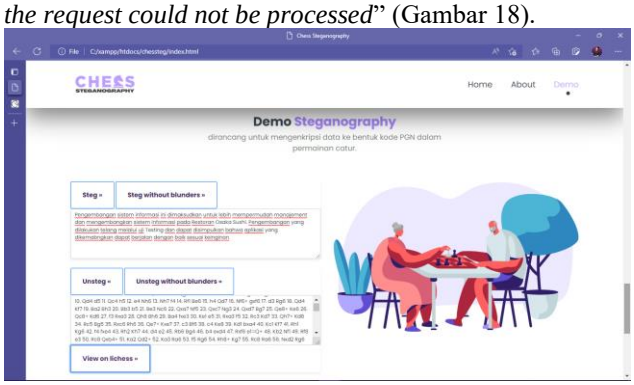
Kotak dikodekan dari 0 (dalam biner 0000000) ke 127 (dalam biner 1111111) yang dimulai pada 1 dan mengacu pada 0 dalam decimal seperti yang ditunjukan pada gambar 2, masing-masing bergerak yang diwakili oleh 7 digit biner (7-bit), mengacu pada indeks target persegi dengan potongan warna tertentu. Tujuh (7-bit) perlangkah mewakili setiap bit rate yang dinyatakan dalam chestega, setiap bit dapat berbeda dari satu implementasi yang lain. Pesan yang akan disembunyikan adalah "informatika 2020", yang akan dikodekan sebagai "52 91 76 55 90 27 54 97 58 52 107 48 36 6 35 25" bagian ini juga dijelaskan pada bagian 3. Pergerakan notasi PNG kemudian digunakan untuk menyembunyikan pesan dalam cover catur seperti pada gambar 16. Dalam cover yang digunakan untuk menyembunyikan pesan, dimulai dengan sebuah langkah yang sesuai dengan kode steganografi dalam pesan yang dikodekan.

Gambar 16. *Chess Cover* dari "informatika 2020"

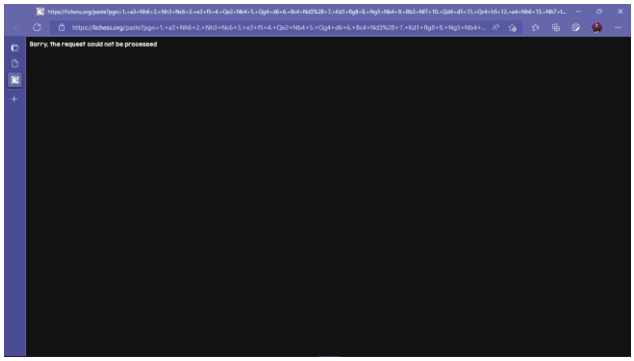
Perlu diperhatikan bahwa dalam implementasinya, link dalam permainan dapat digunakan untuk menghindari teks yang panjang dan membuatnya mudah untuk menulusuri isinya.

B. *Pengujian Enkripsi pada program aplikasi Chestega dengan kasus huruf <160*

Pengujian ini sama seperti pengujian enkripsi sebelumnya, hanya saja pada pengujian kali ini, huruf yang digunakan lebih dari 160 (Gambar 17). Dimana ketika notasi tersebut dialihkan ke halaman lichess.org, makan akan muncul tampilan layar error yang bertuliskan "*sorry, the request could not be processed*" (Gambar 18).

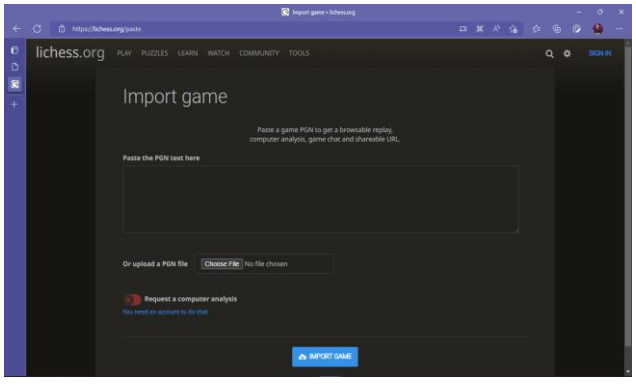


Gambar 17. Pengujian Enkripsi dengan huruf <160

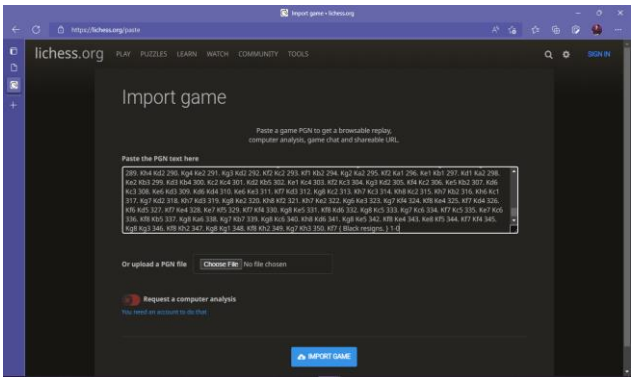


Gambar 18. Tampilan *error* pada laman lichess.org

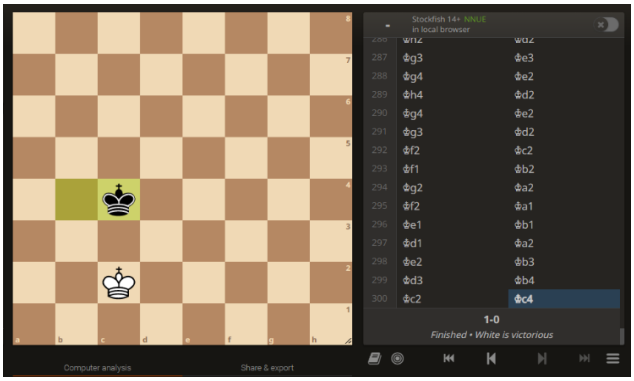
Solusi yang bisa dilakukan adalah dengan cara menyalin notasi PGN secara manual, kemudian menginputkan atau menempelkan notasi tersebut ke form yang tersedia pada laman lichess.org/paste (Gambar 19).



Gambar 19. Tampilan *import* pada laman lichess.org



Gambar 20. Tampilan *import* pada laman lichess.org (2)

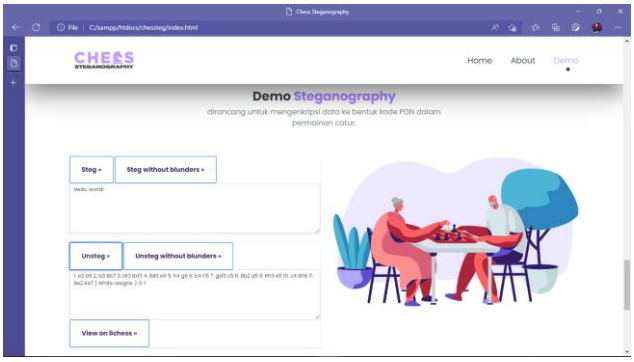


Gambar 21. *Chess Cover* dari <160 huruf

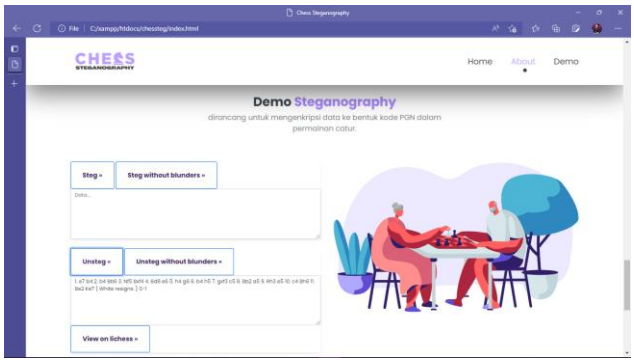
Secara teknis, proses enkripsinya sama seperti pengujian enkripsi sebelumnya, hanya saja perlu dilakukan salin dan tempel notasi PGN secara manual agar tidak terjadi error pada saat beralih ke halaman lichess.org.

C. *Pengujian Dekripsi pada program Aplikasi*

Pengujian ini dilakukan agar user dapat membaca notasi yang diterima lebih jelas. Gambar 22 merupakan tampilan dari hasil dekripsi notasi aljabar PGN, sedangkan pada Gambar 23, merupakan tampilan dari dekripsi yang gagal karena notasi yang dimasukkan salah.



Gambar 22. Tampilan hasil dekripsi notasi aljabar berhasil



Gambar 23. Tampilan hasil dekripsi notasi aljabar gagal

IV. KESIMPULAN

Dalam penelitian ini, telah diajukan metode baru steganografi yang disebut Chestega. Chestega mengusulkan penggunaan permainan populer seperti Catur sebagai sarana efektif untuk melakukan komunikasi rahasia. Pendekatan ini bertujuan untuk menghindari kecurigaan dalam komunikasi dengan menyembunyikan pesan di dalam data permainan catur. Data permainan catur yang dapat dimanfaatkan mencakup posisi papan, jenis dan posisi bidak, gerakan, nama turnamen, tempat, hasil, dan informasi mengenai pemain. Data ini digunakan untuk menyembunyikan pesan dalam skrip gerakan permainan, sesi pelatihan, analisis permainan, dan sebagainya. Pendekatan Chestega ini berbeda dari sebagian besar pendekatan kontemporer karena tidak memanfaatkan noise untuk menyisipkan pesan atau memperkenalkan noise yang dapat dideteksi. Sebaliknya, Chestega menggunakan data otentik dalam penutup yang membuatnya tahan terhadap serangan perbandingan. Chestega juga membenarkan interaksi antara pengirim dan penerima berdasarkan minat mereka dalam permainan catur, sehingga membuat analisis lalu lintas menjadi tidak efektif. Metode Chestega ini dapat diterapkan dalam berbagai jenis *cover*, seperti teks, gambar, grafik, atau audio. Selain itu, *cover* juga dapat dihasilkan secara otomatis menggunakan alat kontemporer seperti Chessmaster, yang menggunakan sistem generasi bahasa alami. Dengan demikian, Chestega juga tahan terhadap serangan profil linguistik dan statistik. Selain permainan catur, Chestega dapat diterapkan dalam permainan lain seperti teka-teki silang, domino, dan sejenisnya. Potensi penggunaan Chestega dalam konteks tersebut layak untuk diselidiki lebih lanjut di masa depan.

Akan tetapi terdapat pula kendala yang terjadi pada saat proses pengenkripsian pesan yang berjumlah lebih dari 160 kata. Hal ini disebabkan karena pesan yang terlalu panjang sehingga pada saat dilakukan pengimportan ke website lichess.org, terjadi error. Solusi yang didapatkan untuk mengatasi hal ini adalah dengan melakukan *copy* dan *paste* secara manual dari halaman demo web Chestega ke halaman web lichess.org.

DAFTAR PUSTAKA

[1] S. Rohayah, G. W. Sasmito, and O. Somantri, "Aplikasi Steganografi Untuk Penyisipan Pesan," *Jurnal Informatika Ahmad Dahlan*, vol. 9, no. 1, 2015, doi: 10.26555/jifo.v9i1.a2038.

[2] A. Desoky, *Noiseless Steganography: The Key to Covert Communications*, 1st ed. USA: Auerbach Publications, 2012.

[3] D. Edmonds and J. Eidinow, *Bobby Fischer goes to war: How a lone American star defeated the Soviet chess machine*. Harper Collins, 2005.

[4] A. Desoky and M. Younis, "Chestega: chess steganography methodology," *Security and Communication Networks*, vol. 2, no. 6, pp. 555–566, Nov. 2009, doi: https://doi.org/10.1002/sec.99.

[5] B. Lange, "Steganography using the chess PGN standard format," *Global Information Assurance Certification Paper, Technical report, SANS Institute*, 2004.

[6] D. Noever, M. Ciolino, and J. Kalin, "The Chess Transformer: Mastering Play using Generative Language Models," *CoRR*, vol. abs/2008.04057, 2020, [Online]. Available: https://arxiv.org/abs/2008.04057

[7] J. C. Hernandez-Castro, I. Blasco-Lopez, J. M. Estevez-Tapiador, and A. Ribagorda-Garnacho, "Steganography in games: A general methodology and its application to the game of Go," *Comput Secur*, vol. 25, no. 1, pp. 64–71, 2006, doi: https://doi.org/10.1016/j.cose.2005.12.001.

[8] Shalu and Y. Sharma, "A Review on Game based Steganography," in *2019 International Conference on Intelligent Sustainable Systems (ICISS)*, 2019, pp. 286–290. doi: 10.1109/ISS1.2019.8908097.

[9] A. Bansal and V. Kumar, "Steganography Technique Inspired by Rook," *International Journal of Information Security and Privacy (IJISP)*, vol. 15, no. 2, pp. 53–67, 2021, [Online]. Available: https://EconPapers.repec.org/RePEc:igg:jisp00:v:15:y:2021:i:2:p:53-67

[10] A. Bansal, "Steganography Technique using Chess Puzzle & Block Mapping," *vivekanand journal of research*, vol. 6, pp. 52–71, Jun. 2017.

[11] D. Neeta, K. Snehal, and D. Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits," in *2006 1st International Conference on Digital Information Management*, 2007, pp. 173–178. doi: 10.1109/ICDIM.2007.369349.

[12] D. J. Barnes, "pgn-extract: A Portable Game Notation (PGN) Manipulator for Chess Games." University of Kent, 2014. [Online]. Available: https://kar.kent.ac.uk/45760/

[13] A. Arya, S. Soni, and] M-Tech Scholar Student, "Performance Evaluation of Secrete Image Steganography Techniques Using Least Significant Bit (LSB) Method," *International Journal of Computer Science Trends and Technology (IJCST)*, vol. 6, [Online]. Available: www.ijcstjournal.org

[14] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," in *2014 International Conference on Computer Communication and Informatics*, 2014, pp. 1–4. doi: 10.1109/ICCCI.2014.6921751.

[15] A. Desoky, "Comprehensive Linguistic Steganography Survey," *Int. J. Inf. Comput. Secur.*,

vol. 4, no. 2, pp. 164–197, Aug. 2010, doi: 10.1504/IJICS.2010.034816.