PENGEMBANGAN WEBSITE BUILDER MENGGUNAKAN AJAX SEBAGAI KAMUFLASE MEDIA PENGIRIM PESAN RAHASIA BERBASIS IMAGE STEGANOGRAPHY

Yohanes Dwi Cahyono[1], Asep Suryanta[1] dan Eko Heri Susanto[2]

[(1)]Poltekad Kodiklatad
Jl. Raya Anggrek, Desa Pendem, Kec. Junrejo, Kota Batu, Jawa Timur 65324
[(2)]Institut Teknologi Nasional
Jl. Khp Hasan Mustopa No.23, Neglasari, Kec. Cibeunying Kaler, Kota Bandung, Jawa Barat 40124
yohanes@poltekad.ac.id, zenirakal@gmail.com, ekoheri@gmail.com

ABSTRAK

Komunikasi data di lingkungan militer sangat membutuhkan kerahasiaan, namun cara komunikasi data yang tradisional masih sering digunakan, sehingga rentan terhadap pencurian data. Diperlukan teknik yang lebih canggih untuk meningkatkan komunikasi data tersebut. Website adalah salah satu teknologi komunikasi data, namun untuk membuat sebuah website dibutuhkan teknik dan ketrampilan khusus. Peneletian ini bertujuan untuk mengembangkan website builder yang dapat digunakan untuk membangun halaman website tanpa harus memiliki ketrampilan teknis tertentu. Selain itu website dapat digunakan untuk menyisipkan pesan rahasia dalam gambar dengan teknik steganografi sebagai kamuflase, sehingga dapat meningkatkan keamanan komunikasi data. Desain website builder yang intuitif dan user friendly mempermudah operator dalam membuat halaman website dan mengintegrasikan teknik steganografi untuk menyisipkan pesan rahasia dalam gambar. Pengujian dilakukan untuk mengetahui efektivitas website builder dalam membuat halaman website sekaligus menyusupkan pesan rahasia. Hasil uji coba menunjukkan bahwa website builder sangat efektif digunakan sehingga operator hanya perlu waktu kurang dari 5 menit untuk membuat hal tersebut.

Kata Kunci: *Steganografy, Web Builder, Kamuflase Steganografy, AJAX*

PENDAHULUAN

Dalam era digital saat ini, keamanan informasi menjadi salah satu tantangan utama, terutama dalam konteks operasi militer dan komunikasi rahasia. Menjaga privasi informasi dan komunikasi data dalam operasi militer adalah kunci untuk melindungi identitas dan lokasi personel, serta informasi strategis lainnya dari pengintaian musuh [1], namun pada praktiknya cara komunikasi data yang tradisional masih sering digunakan dalam lingkungan militer, sehingga rentan terhadap pencurian data seperti misalnya pada tahun 2020, terjadi kebocoran data yang melibatkan informasi pribadi anggota TNI AD, termasuk nama, nomor induk kependudukan dan alamat. Untuk itu diperlukan teknik yang lebih modern dan canggih untuk meningkatkan keamanan komunikasi data tersebut.

Penggunaan teknik steganografi di lingkungan militer sebagai metode komunikasi data sangat relevan, karena memungkinkan menyembunyikan pesan rahasia dalam media tertentu, seperti gambar. Keberadaan teknik ini menjadi semakin penting karena memungkinkan penyisipan pesan tanpa menarik perhatian pihak lain [2].

Kelemahan teknik ini adalah adanya potensi kehilangan data, dan kualitas gambar yang rusak saat pesan disisipkan, kelemahan yang lain terkait kerentanan terhadap serangan analisis yang dilakukan oleh pihak lain, seperti serangan brute-force [3]. Selain kedua hal yang telah disebutkan, cara pengiriman gambar steganografi menjadi *issue* yang harus diselesaikan, penyebabnya karena pesan yang telah disisipkan pada gambar dapat menjadi rusak ketika ketika sarana pengirimannya tidak tepat. Untuk itu diperlukan teknik-teknik baru dalam steganografi dan cara pengirimannya agar dapat lebih meningkatkan keamanan komunikasi data rahasia.

Kelebihan teknik ini terletak pada kemampuannya untuk menyembunyikan

informasi sensitif dalam media yang umum digunakan sehari-hari, seperti gambar digital sehingga sulit terdeteksi oleh mata manusia atau alat analisis biasa, sehingga pesan rahasia dapat disembunyikan dengan efektif [4]. Selain itu, teknik steganografi gambar memiliki daya tampung yang cukup besar sehingga dimungkinkan untuk menyisipkan pesan rahasia dalam jumlah yang signifikan. Keunggulan lainnya adalah kemampuan mengenkripsi pesan sebelum disisipkan ke dalam gambar untuk meningkatkan level keamanan pesan rahasia [5].

Dari analisa kekurangan dan kelebihan pada teknik tersebut maka penelitian ini menjadi kebutuhan mendesak untuk pengembangan metode steganografi sebagai cara komunikasi data yang lebih canggih dan aman, agar semakin relevan diterapkan pada dunia militer [6]. Dalam penelitian terdahulu tentang penggunaan Transformasi Wavelet yang memecah sinyal atau gambar menjadi komponen frekuensi yang berbeda dan Algoritma Genetika dapat meningkatkan kualitas visual gambar sambil tetap menyembunyikan pesan rahasia [7]. Disamping itu, teknik kamuflase berbasis Edge juga menunjukkan potensi besar untuk menyembunyikan data dengan efektif. Metode. Steganografi Kamuflase dengan algoritma canny edge merupakan salah satu teknik baru untuk menyembunyikan data di dalam gambar, dimana data disembunyikan ke dalam piksel disisi tepi gambar. Metode ini mempertimbangkan jumlah data yang akan disisipkan sebagai faktor penting dalam pemilihan sisi tepi, semakin banyak jumlah data yang akan disisipkan, semakin besar penggunaan tepi lemah pada gambar untuk disisipkan [8]. Kelemahan utama dalam teknik ini adalah kerentanannya terhadap serangan berbasis analisis statistik yang canggih dan terus berkembang dalam mengidentifikasi pola statistik yang tidak alami pada gambar steganografi [9].

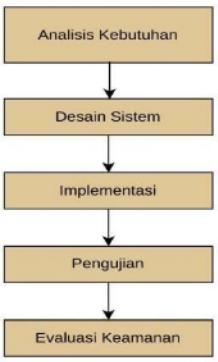
Dengan pertumbuhan teknologi web dan penggunaan internet yang semakin meluas, maka penelitian tentang steganografi berbasis web juga menjadi sangat relevan. Metode menyembunyikan pesan dalam elemen-elemen web seperti gambar dan metadata membuka peluang baru untuk komunikasi rahasia yang lebih aman. Penelitian ini tidak hanya akan memberikan kontribusi pada pengembangan teknik steganografi yang lebih efektif tetapi juga akan menjawab tantangan keamanan informasi di era digital. Gurunath dan Samanta melakukan penelitian untuk mengulas berbagai teknik yang digunakan dalam steganografi berbasis web, termasuk metode penyisipan pesan ke dalam elemen-elemen HTML, CSS, atau gambar. Bahkan pada penelitin tersebut menyebutkan jika steganografi dapat diaplikasikan pada teknologi web 2.0 maupun web 3.0 [10]. Kelemahan dari penelitian ini terletak pada pembanguan website yang memerlukan ketrampilan dan kemampuan khusus, maka pengembangan web builder menjadi aspek penting dalam dunia teknologi informasi karena dapat mendukung pembuatan website menjadi lebih mudah dan efisien [11]. A.M. Aladdin dkk dalam penelitiannya yang berjudul *The Scientific Comparison between Web-Based Site and Web-Builder* menyoroti bagaimana web builder dapat membantu pemula maupun profesional membuat situs website yang sesuai dengan kebutuhan serta mengurangi biaya dan waktu yang dibutuhkan untuk pengembangannya [12]. Penelitian ini memberikan pemahaman secara lebih baik tentang perlunya terus mengembangkan website builder agar dapat mengakomodasi kebutuhan dalam dunia digital yang terus dan semakin berkembang. Pengembangan Website Builder dengan teknik asynchron menggunakan AJAX menjadi subjek penelitian dan pengembangan yang menarik dalam beberapa tahun terakhir untuk meningkatkan responsivitas pengguna dan mempercepat interaksi antarmuka pengguna [13].

Oleh karena itu, penelitian ini difokuskan pada pengembangan website builder menggunakan AJAX yang akan dimanfaatkan sebagai sarana komunikasi data menggunakan metode steganografi gambar sebagai kamuflase pengiriman pesan rahasia untuk meningkatkan keamanan komunikasi dalam konteks militer. Selain itu penelitian ini akan memberikan implikasi yang luas bagi keamanan informasi di berbagai sektor lainnya. Dengan demikian diharapkan dapat

memberikan solusi inovatif untuk masalah keamanan informasi yang semakin kompleks di lingkungan militer.

METODE PENELITIAN

Penelitian ini dilakukan dalam beberapa tahapan penelitian yang terdiri dari tahap analisis kebutuhan, desain sistem, implementasi, pengujian, dan evaluasi keamanan.



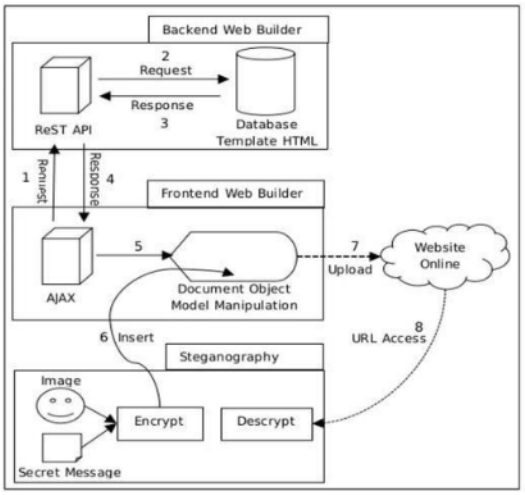
Gambar 1. *Tahapan Penelitian*

Pada tahapan analisis kebutuhan, peneliti melakukan identifikasi pengguna yang akan menggunakan website builder, yaitu operator militer. Identifikasi terkait kebutuhan fungsional juga dilakukan pada tahap ini untuk menentukan fitur terkait menyisipkan pesan rahasia dalam gambar, antarmuka pengguna yang intuitif, dan mekanisme enkripsi. Disisi lain bahwa keamanan, kecepatan, dan responsivitas sistem juga menjadi bagian non fungsional yang harus diperhatikan pada tahap ini seperti terlihat pada tabel 1.

Tabel 1. *Analisis Kebutuhan*

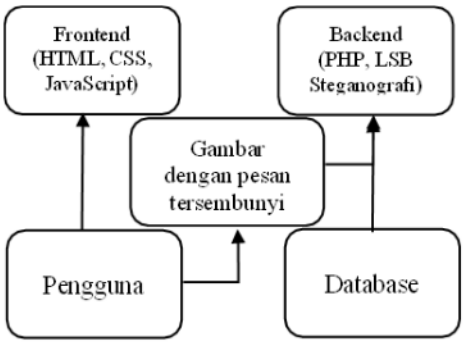
Aspek	Detail
Identifikasi pengguna	- Operator militer
Kebutuhan fungsional	- Menyisipkan pesan rahasia dalam gambar - Antarmuka pengguna yang intuitif - Mekanisme enkripsi
Kebutuhan non fungsional	- Keamanan - Kecepatan - Responsivitas sistem

Desain sistem dilakukan untuk merancang arsitektur sistem, termasuk pemilihan teknologi penggunaan AJAX untuk interaksi dinamis. Pada tahap ini peneliti membuat prototipe antarmuka pengguna yang memungkinkan operator militer untuk mengunggah gambar dan menyisipkan pesan rahasia dengan mudah. Skema desain basis data dirancang juga untuk menyimpan data steganografi dan informasi yang dibutuhkan. Desain sistem seperti ditunjukkan pada gambar.



Gambar 2. *Desain Sistem*

Desain sistem tersebut selanjutnya diimplementasikan untuk mengembangkan frontend yang berfungsi sebagai antarmuka pengguna, dengan menggunakan HTML, CSS dan JavaScript. Backend dibuat dengan mengimplementasikan logika server menggunakan bahasa pemrograman PHP yang diintegrasikan dengan teknik steganorafi LSB untuk menangani penyisipan pesan ke dalam gambar secara aman. Tahapan implementasi digambarkan dalam diagram sebagai berikut:



Gambar 3. *Diagram Implementasi*

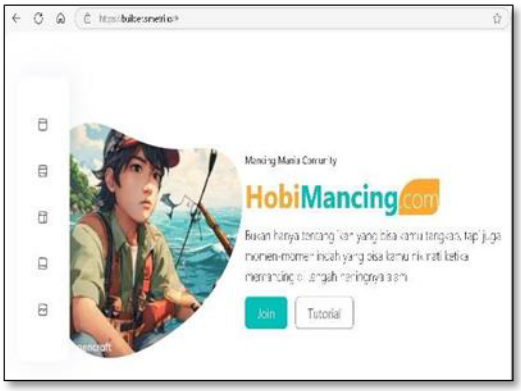
Tahapan berikutnya melakukan pengujian untuk memastikan semua fitur seperti penyisipan pesan dan pengambilan kembali data rahasia dapat bekerja dengan baik. Pengujian juga dilakukan terhadap kerentanan sistem dari serangan brute force untuk memastikan bahwa data tetap aman. Responsivitas dan kecepatan sistem saat digunakan oleh banyak pengguna juga diperhatikan dalam tahapan ini.

Tahapan terakhir dengan melakukan evaluasi keamanan dengan menganalisis risiko untuk mengidentifikasi potensi risiko keamanan yang mungkin dihadapi oleh sistem.

HASIL DAN PEMBAHASAN

Perangkat Lunak Web Builder

Dalam konteks pengembangan website builder sebagai alat komunikasi data steganografi gambar, maka web builder dikelompokkan dalam dua bagian utama perangkat lunak yaitu frontend dan backend. Frontend merupakan bagian perangkat lunak yang berinteraksi langsung dengan pengguna melalui antarmuka pengguna (UI). Pada web builder, frontend bertanggung jawab untuk memberikan pengalaman pada pengguna secara intuitif dan responsif. Ada beberapa komponen penting dalam frontend yaitu HTML yang digunakan sebagai struktur dokumen web, CSS untuk membuat desain visual dan tata letak halaman web, serta JavaScript yang membuat website menjadi lebih dinamis dan responsif. Fronend web builder dapat diakses melalui link https://builder.simetri.io/# seperti terlihat pada gambar 4 berikut ini.



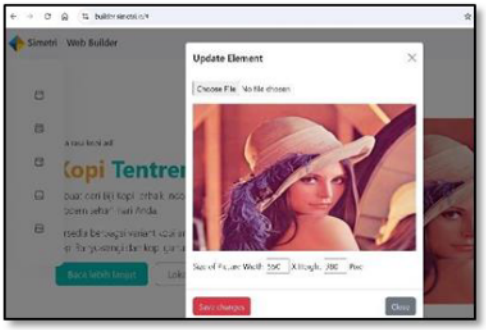
Gambar 4. *Frontend Web Builder*

Backend merupakan perangkat lunak yang bertugas melakukan interaksi dengan database dan melakukan proses logika yang lebih kompleks. Dalam konteks web builder, backend bertanggung jawab dalam mengelola data dan melakukan proses penyisipan pesan rahasia ke dalam gambar menggunakan steganografi. Beberapa komponen penting dalam backend web builder adalah Bahasa Pemrograman PHP digunakan untuk mengimplementasikan logika server selain itu terdapat Teknik Steganografi LSB yang digunakan untuk menyisipkan pesan rahasia ke dalam piksel gambar. Berikut tampilan backend pada web builder.

Gambar 5. *Backend Web Builder*

Perangkat Lunak Steganografy

Pada halaman website builder dilengkapi dengan perangkat lunak untuk upload pesan rahasia yang telah disembunyikan dalam gambar. Format gambar seperti PNG dan BMP digunakan karena memiliki struktur piksel yang memungkinkan penyisipan bit-bit tersebut tanpa mengubah kualitas visual gambar secara signifikan. Adapun tampilan aplikasi ini, terlihat seperti gambar berikut ini.



Gambar 6. *Tampilan upload stego image*

Extract Message

Perangkat lunak steganografi ini juga dilengkapi dengan fasilitas untuk mengekstrak pesan yang disembunyikan dalam gambar pada halaman website. Operator hanya perlu mengisikan alamat URL website yang mengandung pesan rahasia tersebut, kemudian melakukan proses deskripsi. Aplikasi website ini merupakan penterjemah halaman secara otomatis. Dia mampu menterjemahkan gambar-gambar dalam website yang mengandung pesan rahasia, walaupun pesan rahasia tersebut tersebar dalam beberapa gambar. Setelah dilakukan ekstrak maka semua pesan rahasianya akan dapat di baca kembali tanpa ada kerusakan. Adapun tampilan aplikasi terlihat seperti Gambar 7 berikut ini.

Gambar 7. *Tampilan Aplikasi Deskripsi*

Pengoperasian Web Builder

Berdasarkan hasil uji coba aplikasi web builder, terlihat bahwa aplikasi ini sangat membantu operator dalam membuat antar muka halaman website. Operator tidak memerlukan ketrampilan khusus untuk dapat membuat tampilan antar muka website yang profesional. Operator hanya perlu akses https://builder.simetri.io/# dari URL browser. Waktu yang dibutuhkan untuk membuat website tersebut juga sangat cepat, bahkan kurang dari 5 menit.

Gambar pada aplikasi web builder menggunakan format base64. Keuntungan penggunaan format base64 ini memudahkan operator dalam mengganti gambar pada template website dengan gambar steganografi yang mengandung pesan rahasia. Proses penyisipan gambar steganografi ke dalam halaman website tidak memerlukan keahlian teknis tentang HTML, CSS maupun JavaScript, sehingga siapapun dapat melakukannya.

Pengoperasian penyisipan gambar dengan teknik steganografi pada website builder dapat berjalan dengan baik. Berdasarkan uji coba, pesan yang disisipkan dalam gambar dapat dikirim dan diterjemahkan dengan benar melalui frontend dan backend yang dibangun menggunakan web builder.

Namun dari hasil uji coba menunjukkan, ketika gambar steganografi tersebut disimpan dalam format JPG atau JPEG, maka terjadi kesalahan pada proses penterjemahannya. Sehingga pesan rahasia yang diterjemahkan berbeda dengan pesan rahasia yang disisipkan. Kesalahan ini terjadi karena format JPG atau JPEG merupakan jenis gambar yang dikompresi menggunakan teknik lossy compression, yang menyebabkan kerusakan pada bit-bit piksel gambar. Kerusakan ini mengakibatkan bit-bit pesan rahasia yang disisipkan juga ikut rusak, sehingga pesan tidak dapat diterjemahkan dengan benar. Semakin besar kompresi yang diterapkan pada gambar, semakin banyak pula kerusakan pada pesan rahasia. Pada percobaan penyisipan pesan rahasia melalui gambar dengan format PNG atau BMP dapat berhasil dengan baik. Kedua format ini tidak menggunakan kompresi lossy, sehingga pesan rahasia yang dikirim dapat diterjemahkan dengan sempurna karena bit-bit gambar dengan format tersebut tetap utuh.

PENUTUP

Dari serangkaian uji coba, dapat disimpulkan bahwa web builder terbukti mampu mengefisienkan proses pembuatan halaman website. Ketika halaman website sudah berhasil dibuat, maka gambar-gambar yang mengandung pesan rahasia dapat disisipkan ke dalam halaman tersebut. Penelitian ini berhasil mengkamuflasekan gambar steganografi ke dalam halaman website.

Pesan rahasia yang tersembunyi pada gambar dalam website juga dapat diterjemahkan secara sempurna, jika gambar steganografi disimpan dengan format PNG atau BMP. Namun, jika gambar itu disimpan dalam format JPG atau JPEG, maka pesan

rahasia tidak dapat diterjemahkan secara sempurna karena kerusakan yang disebabkan oleh kompresi lossy.

Kelemahan penelitian ini adalah ketika pesan rahasia yang disisipkan ke dalam gambar tidak dienkripsi. Hal ini menyebabkan adanya potensi kebocoran pesan rahasia. Oleh karena itu, saran untuk penelitian selanjutnya adalah melakukan proses enkripsi terhadap pesan rahasia sebelum pesan tersebut disisipkan pada gambar.

Dengan demikian, penelitian ini memberikan kontribusi signifikan dalam pengembangan web builder yang aman dan efektif untuk komunikasi rahasia di lingkungan militer melalui gambar steganografi.

DAFTAR PUSTAKA

[1] R. Gurunath, M. F. J. Klaib, D. Samanta, and M. Z. Khan, "Social Media and Steganography: Use, Risks and Current Status," *IEEE Access*, vol. 9, pp. 153656–153665, 2021, doi: 10.1109/ACCESS.2021.3125128.

[2] S. Kaur, A. Kaur, and K. Singh, "A Survey of Image Steganography," *Int. J. Comput. Appl. Technol. Res.*, vol. 3, no. 7, pp. 479–482, 2014, doi: 10.7753/ijcatr0307.1017.

[3] R. Amirtharajan, R. Akila, and P. Deepikachowdavarapu, "A Comparative Analysis of Image Steganography," *Int. J. Comput. Appl.*, vol. 2, no. 3, pp. 41–47, 2010, doi: 10.5120/644-900.

[4] R. Din and A. J. Qasim, "Steganography analysis techniques applied to audio and image files," *Bull. Electr. Eng. Informatics*, vol. 8, no. 4, pp. 1297–1302, 2019, doi: 10.11591/eei.v8i4.1626.

[5] N. Farooq and A. Selwal, "Image steganalysis using deep learning: a systematic review and open research challenges," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 6, pp. 7761–7793, 2023, doi: 10.1007/s12652-023-04591-z.

[6] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital imasteganography: A literature survey," *Inf. Sci. (Ny).*, vol. 609, pp. 1451– 1488, 2022, doi: 10.1016/j.ins.2022.07.120.

[7] S. Agarwal, O. P. Singh, and D. Nagaria, "Analysis and comparison of wavelet transforms for denoising MRI image," *Biomed. Pharmacol. J.*, vol. 10, no. 2, pp. 831–836, 2017, doi: 10.13005/bpj/1174.

[8] A. Mohana and S. Chandra, "Message Camouflage in an Image using EDGE-Based Steganography," *Int. Res. J. Eng. Technol.*, no. March, 2022, [Online]. Available: www.irjet.net

[9] Y. Ge, T. Zhang, H. Liang, Q. Jiang, and D. Wang, "A novel technique for image steganalysis based on separable convolution and adversarial mechanism," *Electron.*, vol. 10, no. 22, pp. 1–15, 2021, doi: 10.3390/electronics10222742.

[10] Gurunath R. and D. Samanta, "A Novel Approach for Semantic Web Application in Online Education Based on Steganography," *Int. J. Web-Based Learn. Teach. Technol.*, vol. 17, no. 4, pp. 1–13, 2021, doi: 10.4018/ijwltt.285569.

[11] M. S. Arafin and Y. Jiang, "Developing a dynamic website using the online website builder Weebly for Viking Fortune Oy," p. 33, 2017.

[12] A. M. Aladdin, C. M. Rahman, and M. S. Abdulkarim, "The Scientific Comparison between Web-Based Site and Web-Builder (Open Source) Project: Functionalities, Usability, Design and Security," *Int. J. Sci. Res. Manag.*, vol. 6, no. 06, pp. 44–52, 2018, doi: 10.18535/ijsrm/v6i6.ec05.

[13] A. Ojeh, "The Future of Website Builders: Evolution in Web Design," *Sonary*, 2023, [Online]. Available: https://sonary.com/content/the- future-of-website-builders- evolution-in-web-design/