SISTEM PERLINDUNGAN DATA MENGGUNAKAN KAEDAH STEGANOGRAFI IMEJ (DATASHIELD UKM)

MUHAMMAD NURAIMAN BIN JOHARI
DR AZANA HAFIZAH BINTI MOHD AMAN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Projek DataShield UKM ini bertujuan membangunkan aplikasi web steganografi khusus untuk warga UKM, yang membolehkan pengguna menyembunyikan data teks dalam imej dan mengekstrak semula teks daripada imej semula menggunakan teknik *Least Significant Bit* (LSB). Pada era teknologi kini, banyak berlakunya peningkatan ancaman keselamatan digital yang semakin merisaukan seperti pencerobohan data, penggodaman*, Man-in-the-Middle* (MITM*) Attack* dan banyak lagi. Ketiadaan platform mesra pengguna juga adalah salah satu masalah yang dihadapi bagi melindungi maklumat rahsia tanpa menimbulkan kecurigaan. Dengan itu sistem aplikasi web DataShield UKM ini dapat membantu melindungi data-data penting yang ingin di kongsikan. Projek aplikasi web ini akan menyediakan alat yang membolehkan pengguna menyembunyikan dan mengekstrak data secara selamat melalui imej digital yang kelihatan normal. Projek ini mempunyai objektif utama untuk membangunkan sistem yang mudah digunakan, selamat, dan efektif dalam melindungi maklumat. Sistem ini membolehkan pengguna memuat naik imej dalam pelbagai bentuk format seperti JPEG, PNG, JPG dan GIF. Kaedah penyembunyian mesej teks dengan menggunakan teknik LSB yang digabungkan dengan penyulitan keselamatan tinggi menggunakan AES-GCM dan penjanaan kunci melalui PBKDF2. Hanya pengguna dengan kata laluan yang betul dapat mengekstrak semula mesej yang disembunyikan. Antaramuka sistem direka secara mesra pengguna, lengkap dengan paparan pratonton imej, mesej kejayaan dan fungsi muat turun imej terbenam. DataShield UKM menawarkan satu penyelesaian efektif dan mudah diakses bagi melindungi keselamatan maklumat digital di kalangan komuniti UKM mahupun di peringkat luar.

PENGENALAN

Dalam era digital yang semakin pesat berkembang di negara Malaysia ini. Ancaman terhadap privasi data semakin meningkat termasuklah pencerobohan data, penggodaman dan kecurian maklumat. Berdasarkan data yang direkodkan Jabatan Siasatan Jenayah Komersial (JSJK), Bukit Aman, Polis Diraja Malaysia (PDRM) sejak 2019 hingga bulan Ogos menunjukan trend jenayah dalam talian semakin meningkat secara ketara tahun demi tahun (Datuk Seri Ramli Mohamed Yoosuf 2024). Salah satu kaedah yang boleh digunakan untuk melindungi data ialah kaedah steganografi, iaitu teknik menyembunyikan maklumat dalam fail media seperti imej, video atau audio. Berbeza dengan kaedah kriptografi yang mengubah data asli kepada data yang disulitkan, sebaliknya steganografi menyembunyikan kewujudan data tersebut, menjadikannya sukar dikesan oleh pihak yang tidak dibenarkan. Projek ini telah berjaya dilaksanakan melalui pembangunan aplikasi web DataShield UKM, yang menyokong format imej seperti JPEG, PNG, JPG dan GIF, serta membolehkan proses pembenaman dan pengekstrakan mesej dilakukan dengan selamat melalui integrasi penyulitan AES-GCM dan PBKDF2. Antaramuka sistem juga direka dengan paparan pratonton imej, pengesahan input, fungsi muat turun stego-imej serta pemberitahuan kejayaan yang memberikan pengalaman mesra pengguna. Sistem ini sekali gus membuktikan bahawa steganografi boleh diintegrasikan dalam aplikasi web moden untuk meningkatkan keselamatan maklumat dalam kalangan pengguna di Malaysia.

METODOLOGI KAJIAN

Metodologi kajian ini merangkumi pendekatan sistematik dalam pembangunan sistem DataShield UKM. Projek ini dibangunkan menggunakan Model Pembangunan Secara *Incremental Development* yang membolehkan sistem dibina secara berfasa, bermula dari asas fungsi utama hingga ke integrasi keseluruhan antara muka dan sistem penyulitan. Model ini dipilih kerana ia menyediakan kerangka yang fleksibel dan membolehkan penambahbaikan sistem secara berperingkat, sesuai dengan keperluan projek yang melibatkan pelbagai fungsi seperti pembenaman data, pengekstrakan data menggunakan kata kunci, dan pemprosesan imej.

Fasa Perancangan

Fasa perancangan merupakan peringkat awal yang penting dalam pembangunan projek DataShield UKM. Dalam fasa ini, permasalahan dan objektif projek dikenal pasti dengan jelas, diikuti dengan penetapan skop dan sasaran projek secara terperinci. Selain itu, jadual pelaksanaan turut dirancang bagi memastikan kelancaran projek, merangkumi tempoh masa untuk setiap fasa seperti perancangan, analisis, pelaksanaan, penilaian dan penyerahan. Keseluruhannya, fasa ini bertujuan memastikan projek dapat dijalankan secara tersusun dan mencapai matlamat yang telah ditetapkan.

Fasa Analisis

Fasa ini melibatkan pengumpulan keperluan sistem melalui kajian sastera, analisis sistem sedia ada, serta pemerhatian terhadap isu keselamatan data digital yang semakin membimbangkan. Tumpuan diberikan kepada keperluan pengguna khusus untuk komuniti UKM. dan juga umum dalam pelbagai sektor seperti pendidikan, perbankan, komunikasi peribadi dan organisasi yang memerlukan kaedah penghantaran maklumat secara rahsia tanpa menimbulkan kecurigaan. Fokus utama dalam fasa ini adalah untuk membangunkan sebuah platform yang mampu menyembunyikan data teks ke dalam imej digital dengan cara yang selamat, tidak mudah dikesan, dan pada masa yang sama, mudah digunakan oleh pengguna tanpa memerlukan pengetahuan teknikal yang mendalam. Ciri-ciri seperti penyulitan kata laluan, sokongan pelbagai format imej, dan keupayaan untuk mengekstrak semula data dengan tepat turut dikenal pasti sebagai

keperluan penting bagi memastikan kebolehgunaan dan keberkesanan sistem yang dibangunkan.

Fasa Reka Bentuk

Dalam fasa ini, reka bentuk sistem dijalankan melibatkan pembangunan antaramuka pengguna bahagian hadapan *(frontend)* menggunakan HTML, CSS dan Bootstrap, manakala logik sistem turut dikendalikan menggunakan JavaScript. Reka bentuk antara muka disusun agar mudah digunakan, responsif, dan menarik untuk memberikan pengalaman pengguna yang optimum.

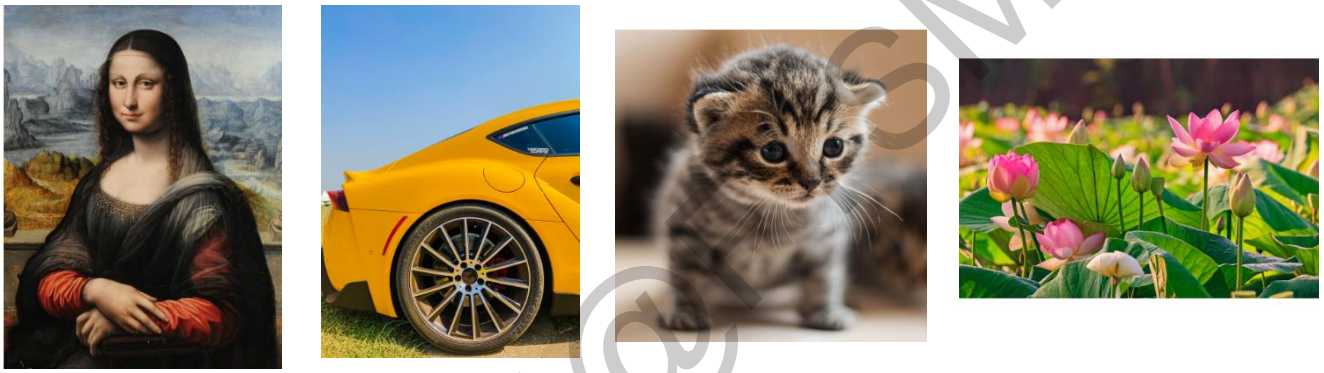
Fasa Pembangunan

Pembangunan aplikasi merangkumi dua komponen utama: pembenaman *(embedding)* dan pengekstrakan *(extraction).* Fungsi utama melibatkan proses menyembunyikan mesej ke dalam imej menggunakan teknik Least Significant Bit (LSB) serta penyulitan data melalui algoritma AES-GCM dan penjanaan kunci menggunakan PBKDF2. Bagi menjamin kebolehpercayaan sistem, satu reka bentuk pengesahan input yang menyeluruh telah dibangunkan, termasuk paparan mesej ralat sekiranya pengguna tidak memuat naik imej, tidak memasukkan mesej, atau gagal menyediakan kata laluan.

Fasa Pengujian

Asas pengujian sistem DataShield UKM ditetapkan berdasarkan dokumen keperluan yang merangkumi keperluan fungsian dan bukan fungsian yang telah dibangunkan dalam fasa analisis dan reka bentuk sistem. Pengujian juga disandarkan kepada algoritma yang digunakan dalam sistem, iaitu algoritma *Least Significant Bit* (LSB) Jenis pengujian yang dilaksanakan dalam projek ini merupakan pengujian fungsian yang menggunakan pendekatan Kotak Hitam *(Black Box Testing),* ia menfokuskan kepada tahap pengujian sistem secara keseluruhan. Pengujian tidak berfungsi juga dijalankan dengan menggunakan pengujian prestasi, di mana fokusnya bertujuan untuk memastikan sistem dapat berfungsi dengan efisien tanpa menyebabkan gangguan yang ketara terhadap kualiti imej menggunakan kaedah PSNR *(Peak Signal-to-Noise Ratio)* dan MSE *(Mean Squared Error)* , serta mematuhi keperluan masa pemprosesan yang ditetapkan.

PSNR adalah ukuran yang digunakan untuk menilai kualiti imej yang diubah selepas proses pembenaman mesej. Kaedah ini bertujuan untuk memastikan bahawa prestasi sistem dalam menyembunyikan mesej dalam imej tidak menyebabkan penurunan kualiti imej yang ketara, ianya penting untuk sistem web steganografi yang memerlukan imej stego kelihatan hampir sama dengan imej asal.



Rajah 1 Imej Yang Digunakan Untuk Pengujian

Selain itu, empat imej dalam format PNG yang berukuran 512x512 akan digunakan, contoh imej tersebut seperti di rajah 1. Ukuran 512x512 piksel dipilih kerana ia memberikan keseimbangan antara ketepatan ujian dan keperluan pemprosesan, di mana imej ini cukup besar untuk menampung mesej yang akan disembunyikan, tetapi masih relevan untuk ujian dalam sistem steganografi. Keempat-empat imej ini mewakili pelbagai jenis kandungan visual yang akan diuji dalam keadaan yang berbeza, memastikan pengujian berjalan dengan lancar dan menyeluruh.

$$PSNR = 10\log_{10}(\frac{MAX^2}{MSE}) \quad \ldots(1.1)$$

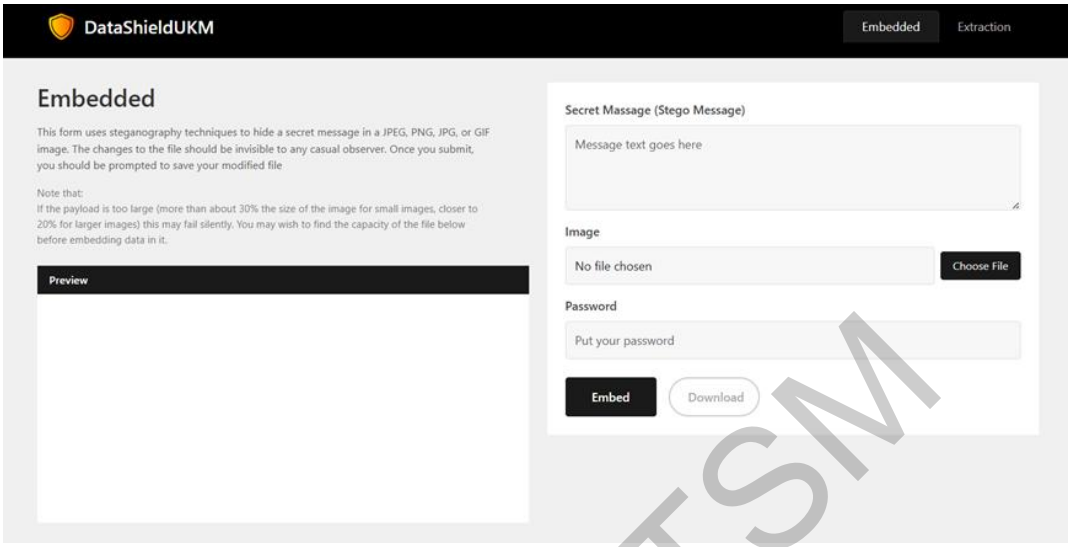
$$MSE = \frac{1}{mn}\sum\frac{m-1}{i=0}\sum\frac{n-1}{j=0}[I(i,j) - K(i,j)]^2 \quad \ldots(1.2)$$

Bagi setiap imej, keputusan PSNR akan dicatatkan untuk ketiga-tiga kapasiti mesej yang diuji. Hasil ujian ini memberi gambaran tentang bagaimana setiap kapasiti mesej mempengaruhi kualiti imej selepas proses pembenaman. Imej dengan kapasiti mesej yang lebih besar, seperti 2,500 bit, mungkin menunjukkan penurunan dalam nilai PSNR berbanding imej yang menggunakan kapasiti mesej lebih kecil, seperti 1,240 bit, kerana lebih banyak data disembunyikan, yang boleh menyebabkan perubahan yang lebih besar pada imej.

KEPUTUSAN DAN PERBINCANGAN

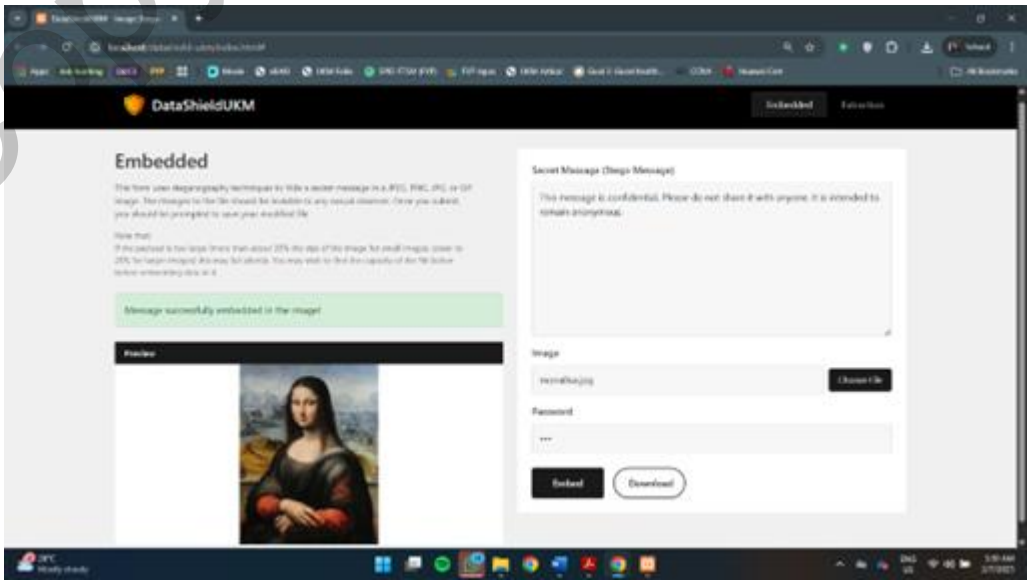
Sistem DataShield UKM ini telah berjaya mencapai objektif utamanya iaitu untuk menyediakan platform yang selamat dan efisien bagi penyembunyian mesej rahsia dalam imej. Pengujian dilakukan dari aspek fungsian dan prestasi, yang melibatkan penggunaan teknik steganografi *Least Significant Bit* (LSB). Sistem menunjukkan keupayaan untuk menjalankan proses pembenaman dan pengekstrakan mesej dengan berkesan, sambil mengekalkan kualiti imej yang tinggi berdasarkan nilai PSNR yang diukur selepas penyembunyian mesej. Proses penyulitan juga dijalankan dengan baik, memastikan kerahsiaan mesej terpelihara. Keseluruhan ujian membuktikan bahawa DataShield UKM mampu memenuhi keperluan keselamatan yang telah ditetapkan.

Apabila pengguna mengakses sistem DataShield UKM, mereka akan disambut dengan halaman utama yang memaparkan modul Pembenaman *(Embedded).* Modul ini merupakan komponen utama yang membolehkan pengguna menyembunyikan mesej rahsia ke dalam imej digital menggunakan teknik steganografi secara mesra pengguna dan selamat. Paparan ini direka dengan susun atur yang teratur serta mudah difahami bagi memastikan pengguna dapat menggunakan sistem ini tanpa kekeliruan, walaupun tanpa pengetahuan teknikal yang mendalam.



Rajah 2 Antara Muka Modul Pembenaman *(Embedded)*

Di bahagian kanan halaman, pengguna disediakan dengan borang untuk memasukkan mesej rahsia yang ingin disembunyikan seperti dalam rajah 2. Pengguna perlu memilih fail imej yang sesuai dalam format JPEG, PNG, JPG atau GIF, serta menetapkan kata laluan bagi proses penyulitan mesej tersebut. Kata laluan ini penting kerana ia akan digunakan untuk menyulitkan mesej dan hanya dengan kata laluan yang betul sahaja mesej dapat diekstrak semula. Seterusnya, terdapat dua butang utama iaitu butang *"Embed"* untuk memulakan proses pembenaman, dan *"Download"* untuk memuat turun imej yang telah dimasukkan mesej.

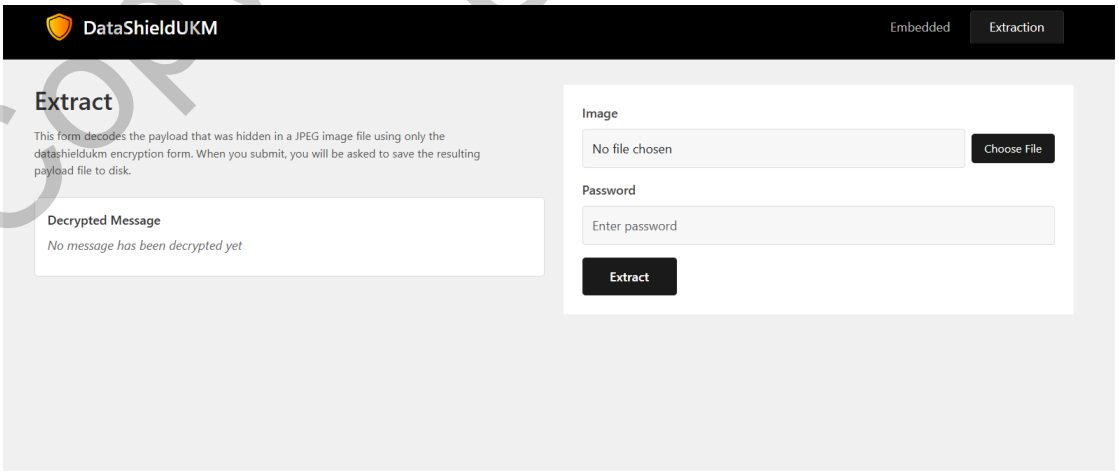


Rajah 3 Antara Muka Modul Pembenaman Berjaya Dibenamkan

Sementara itu, di sebelah kiri halaman, sistem akan memaparkan pratonton imej setelah proses pembenaman berjaya dilakukan seperti dalam rajah 3. Imej tersebut kelihatan seperti biasa tanpa sebarang perubahan visual, namun mengandungi mesej rahsia yang telah disulitkan. Sekiranya proses berjaya, pengguna akan diberikan makluman berbentuk mesej kejayaan berwarna hijau di atas pratonton, bagi memaklumkan bahawa mesej telah berjaya disembunyikan.

Selain itu, sistem ini turut memaparkan nota peringatan penting yang mengingatkan pengguna bahawa kapasiti mesej yang boleh disembunyikan adalah bergantung kepada saiz imej yang digunakan. Bagi imej bersaiz kecil, had selamat adalah sekitar 30% daripada saiz asal imej, manakala bagi imej yang lebih besar, had yang disarankan adalah sekitar 20%. Langkah ini penting bagi mengelakkan berlakunya kegagalan pembenaman sekiranya mesej terlalu panjang.

Halaman "*Extraction*" ini adalah paparan yang membolehkan pengguna mengekstrak mesej tersembunyi daripada imej yang telah diubahsuai. Borang pada halaman ini menyediakan fungsi untuk memuat naik imej yang mengandungi mesej rahsia yang disembunyikan, dan pengguna perlu memasukkan kata laluan yang betul untuk mengekstrak mesej tersebut seperti di paparan rajah 4 di bawah.



Rajah 4 Antara Muka Bagi Modul Pengekstrakan *(Extraction)*

Sistem ini akan memaparkan mesej ralat sekiranya pengguna memasukkan kata laluan yang tidak sah semasa proses pengekstrakan mesej. Seperti yang ditunjukkan dalam Rajah 4, sistem memaparkan notifikasi bertulis “Incorrect password. Please try again with the correct password.” apabila percubaan untuk menyahsulit mesej menggunakan kata laluan yang salah dilakukan. Dalam keadaan ini, proses pengekstrakan tidak diteruskan dan tiada mesej yang dipaparkan di ruangan “Decrypted Message” kepada pengguna.

Keadaan ini membuktikan bahawa sistem mempunyai mekanisme keselamatan asas yang efektif untuk mencegah akses tidak sah terhadap maklumat sulit yang tersembunyi dalam imej. Mekanisme ini amat penting dalam menjamin kerahsiaan dan integriti maklumat yang disembunyikan menggunakan teknik steganografi, serta memperkukuh kepercayaan pengguna terhadap sistem DataShield UKM dalam pengurusan data rahsia.

Pengujian Fungsian

Teknik pengujian fungsian bagi sistem DataShield UKM menggunakan pendekatan Kotak Hitam *(Black Box Testing)* yang berfokus kepada pemeriksaan output sistem berdasarkan input tertentu tanpa perlu mengetahui secara mendalam struktur dalaman atau kod sumber aplikasi. Kaedah ini amat sesuai bagi sistem seperti DataShield UKM yang melibatkan dua fungsi utama iaitu proses pembenaman (embedding) dan pengekstrakan (extraction) mesej sulit ke dalam dan daripada imej digital.

Berdasarkan jadual 1 keputusan pengujian fungsian, sistem *DataShield UKM* telah menjalani 14 kes ujian menggunakan kaedah *Black Box Testing* yang memfokuskan kepada pengujian input dan output tanpa melihat kod dalaman. Ujian meliputi pelbagai aspek termasuk pembenaman mesej ringkas, mesej kosong, dan mesej panjang yang melebihi kapasiti imej. Hasil ujian menunjukkan sistem mampu menyembunyikan mesej dengan jayanya (TC01), memaparkan ralat apabila mesej kosong dimasukkan (TC02), dan menghalang proses jika mesej terlalu panjang (TC03).

Selain itu, pengujian terhadap pelbagai format imej seperti PNG, JPEG, GIF, TIFF, dan HEIF (TC04 hingga TC10) menunjukkan sistem menyokong kebanyakan format popular, manakala sesetengah format seperti TIFF dan HEIF tidak memaparkan pratonton, tetapi sistem tetap memberikan tindak balas yang bersesuaian. Dari segi keselamatan, sistem berjaya mengesan kata laluan yang salah dan memaparkan ralat (TC011), serta menghalang pengekstrakan apabila tiada imej stego dimuat naik (TC012).

Sistem juga menunjukkan antara muka pengguna yang responsif (TC013) dan boleh berfungsi dengan baik dalam pelayar web seperti Chrome, Edge, dan Mozilla Firefox (TCP150). Kesemua keputusan pengujian menunjukkan status "Lulus", yang membuktikan sistem berfungsi dengan baik, stabil, dan memenuhi keperluan fungsi yang ditetapkan.

Jadual 1 Keputusan Kaedah Yang Dicadangkan Bagi Pengujian Fungsian

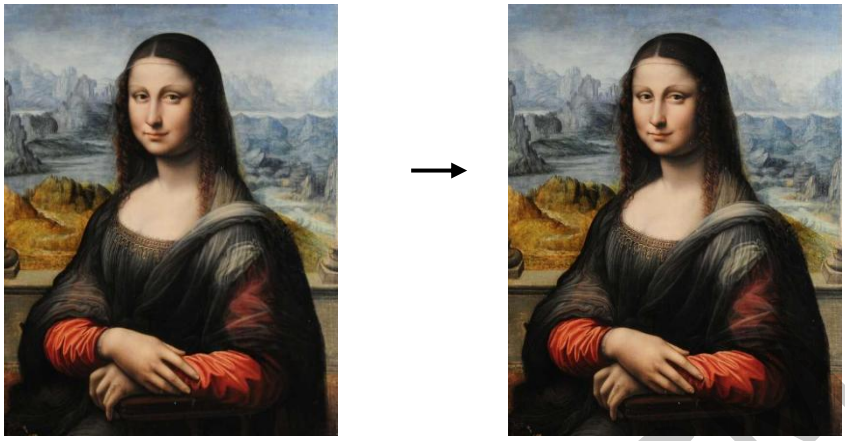
ID Ujian	Fungsi Diuji	Input	Kata Kunci	Jangkaan Output	Status Pengujian
TC01	Pembenaman mesej ringkas	Imej JPG + "Hello UKM"	ukm123	Imej baru mengandungi mesej tersembunyi tanpa perubahan visual	Lulus
TC02	Pembenaman mesej kosong	Imej JPEG + "" (tiada mesej)	ukm123	Paparan ralat atau mesej tidak disimpan	Lulus
TC03	Pembenaman mesej panjang	Imej JPEG + mesej > kapasiti imej	ukm123	Mesej tidak dapat di ekstrak	Lulus
TC04	Pembenaman format imej PNG	Imej PNG + "test"	ukm123	Proses pembenaman berjaya	Lulus
TC05	Pembenaman format imej JPG	Imej JPG + "test"	ukm123	Proses pembenaman berjaya	Lulus
TC06	Pembenaman format imej PDF	Imej PDF + "test"	ukm123	Paparan pratonton tidak dipaparkan	Lulus
TC07	Pembenaman format imej TIFF	Imej TIFF + "test"	ukm123	Paparan pratonton tidak dipaparkan	Lulus
TC08	Pembenaman format imej GIF	Imej GIF + "test"	ukm123	Proses pembenaman berjaya	Lulus
TC09	Pembenaman format imej HEIF	Imej HEIF + "test"	ukm123	Paparan pratonton tidak dipaparkan	Lulus
TC10	Pembenaman format imej JPEG	Imej JPEG + "test"	ukm123	Proses pembenaman berjaya	Lulus
TC011.	Pengekstrakan dengan kata kunci salah	Imej stego JPG	salah123	Paparan ralat “ kata laluan tidak tepat sila guna kan kata laluan yang betul”	Lulus
TC012	Pengekstrakan tanpa imej	Tiada imej dimuat naik	-	Paparan ralat “silat muat naik imej”	Lulus
TC013	UI mesra pengguna	Akses dan klik semua fungsi pada antara muka web	-	Fungsi responsif	Lulus
TCP15	Ujian web di pelbagai platform enjin carian	Sistem web akan dibuka dipelbagaii enjin carian Chrome, Edge, and Mozila Firefox	-	Sistem web berfungsi dengan baik	Lulus

Pengujian Bukan Fungsian

Jadual 2 Keputusan Kaedah Yang Dicadangkan Bagi Pengujian Tidak Berfungsi

Jenis Imej berwarna (512x512)	**Kapasiti 1,240 (bit)**	**Kapasiti 2,000 (bit)**	**Kapasiti 2,500 (bit)**
	PSNR	**PSNR**	**PSNR**
Monalisa	76.55	77.04	76.22
Kereta	76.59	77.03	76.42
Kucing	76.64	77.21	76.34
Bunga	76.49	77.33	76.27

Berdasarkan keputusan ujian PSNR yang ditunjukkan dalam jadual 2, terdapat kaedah yang boleh digunakan untuk melakukan pengujian terhadap kualiti imej stego. PSNR *(Peak Signal-to-Noise Ratio)* ialah ukuran kuantitatif yang digunakan untuk menilai kualiti pemampatan atau perubahan dalam imej digital, di mana nilai PSNR yang lebih tinggi menunjukkan bahawa perbezaan antara imej asal dan imej yang diubahsuai adalah kecil. Secara umumnya, nilai PSNR 30 dB ke atas dianggap baik, manakala antara 20–30 dB masih boleh diterima tetapi menunjukkan terdapat perubahan yang ketara. Jika nilai PSNR kurang dari 20 dB, ini menunjukkan kualiti imej telah merosot dengan teruk. Berdasarkan dari hasil pengujian yang telah dijalankan kebanyakan imej yang telah diubah suai mempunyai nilai PSNR lebih dari 70 dB, jika hasil ujian menunjukkan PSNR berada dalam lingkungan lebih 30 dB *(Wikipedia contributors, 2025)*. Ini bermaksud kualiti imej stego masih tinggi dan tidak banyak berubah dari imej asal, menunjukkan kualiti imej tersebut tidak berubah.



Imej Penutupan Asal Imej Penutupan Stego

Rajah 5 Perbandingan Imej Penutupan

Rajah 5 menunjukan imej penutupan asal dan stego yang telah dibandingkan untuk melihat kualiti imej tersebut sebelum dan selepas proses pembenaman. Formula yang digunakan untuk mengira PSNR adalah seperti berikut:

Cadangan Penambahbaikan

Untuk penambahbaikan sistem di masa hadapan, beberapa aspek boleh diperbaiki. Pertama, mekanisme pengesahan kapasiti imej perlu ditingkatkan dengan menambah amaran apabila mesej yang dimasukkan melebihi kapasiti imej yang boleh disembunyikan. Ini akan mengelakkan masalah yang timbul apabila sistem tidak dapat menampung mesej yang terlalu besar. Kedua, keseragaman antara peranti boleh diperbaiki dengan menggunakan reka bentuk antaramuka yang lebih responsif, yang dapat menyesuaikan elemen-elemen UI dengan pelbagai saiz skrin peranti. Tambahan pula, algoritma penyulitan boleh diperbaiki dengan meningkatkan kecekapan pemprosesan, terutamanya apabila mengendalikan mesej yang lebih besar.

Di samping itu, sistem boleh diperkembangkan dengan menambah modul pelaporan yang lebih komprehensif, yang membolehkan pengguna melihat hasil ujian, kualiti imej stego, dan statistik berkaitan penyembunyian mesej. Ini akan memberi pengguna lebih banyak kawalan dan maklumat mengenai proses yang sedang dijalankan.

KESIMPULAN

Sepanjang proses pembangunan sistem DataShield UKM, sistem ini telah berjaya mencapai objektif utamanya iaitu untuk menyediakan platform yang selamat dan efisien bagi penyembunyian mesej rahsia dalam imej. Pengujian dilakukan dari aspek fungsian dan prestasi, yang melibatkan penggunaan teknik steganografi *Least Significant Bit* (LSB). Sistem menunjukkan keupayaan untuk menjalankan proses pembenaman dan pengekstrakan mesej dengan berkesan, sambil mengekalkan kualiti imej yang tinggi berdasarkan nilai PSNR yang diukur selepas penyembunyian mesej. Proses penyulitan juga dijalankan dengan baik, memastikan kerahsiaan mesej terpelihara. Keseluruhan ujian membuktikan bahawa DataShield UKM mampu memenuhi keperluan keselamatan yang telah ditetapkan.

Kekuatan Sistem

Kekuatan utama sistem DataShield UKM adalah keupayaan untuk menyembunyikan mesej dalam imej tanpa menyebabkan penurunan yang ketara pada kualiti imej. Sistem juga mempunyai antaramuka pengguna yang mesra pengguna, yang memudahkan interaksi pengguna tanpa perlu mempunyai pengetahuan teknikal yang mendalam. Penyulitan dan steganografi yang digunakan memberi tahap keselamatan yang tinggi, memastikan mesej yang disembunyikan tidak mudah dikesan.

Kelemahan Sistem

Antara salah satu kelemahan sistem ini yang lain ialah sistem mungkin masih meneruskan proses penyembunyian walaupun data sebenar tidak dapat ditanam sepenuhnya ke dalam imej. Fenomena ini dikenali sebagai kegagalan secara senyap (*silent failure)*, di mana pengguna tidak menerima sebarang makluman bahawa proses telah gagal. Berdasarkan pemerhatian, imej bersaiz kecil hanya mampu menampung mesej sehingga 30% daripada saiz asal imej, manakala bagi imej yang lebih besar, had selamat adalah sekitar 20%. Sekiranya had ini dilepasi, mesej yang ditanam mungkin tidak dapat diekstrak semula dengan sempurna, sekali gus menjejaskan kebolehpercayaan sistem dalam memastikan kerahsiaan data terjamin.

RUJUKAN

AES-GCM Encryption and Decryption Examples using Web Crypto (subtle.crypto) JavaScript API. (n.d.). Gist. https://gist.github.com/themikefuller/aca9491f960cbb8d94cdd7236698f0cd

Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. Applied Sciences, 13(21), 11771.

Al-Harbi, O. A., Alahmadi, W. E., & Aljahdali, A. O. (2020). Security analysis of DNA based steganography techniques. SN Applied Sciences, 2(2). https://doi.org/10.1007/s42452-019-1930-1

Bachrach, M., & Shih, F. Y. (2017). Survey of image steganography and steganalysis.Multimedia Security: Watermarking, Steganography, and Forensics, 201-214.

Balagyozyan, L.A. & Hakobyan, Robert. (2021). Steganography in Frames of Graphical Animation. E3S Web of Conferences. 266. 09006. 10.1051/e3sconf/202126609006.

Bedi, P., & Dua, A. (2020). Network Steganography using the Overflow Field of Timestamp Option in an IPv4 Packet. Procedia Computer Science, 171, 1810–1818. https://doi-org.eresourcesptsl.ukm.remotexs.co/10.1016/j.procs.2020.04.194

Datuk Wilson Ugak Kumbong . "4,174 Kes Keselamatan Siber Dari Januari-Ogos 2024." Portal Berita, 2024, berita.rtm.gov.my/nasional/senarai-berita-nasional/senarai-artikel/4-174-kes-keselamatan-siber-dari-januari-ogos-2024. Accessed 30 Oct. 2024.

Fazzani, H. (2024, August 20). *Implementing AES-GCM encryption in JavaScript*. Haikel Fazzani. https://www.haikel-fazzani.eu.org/blog/post/javascript-cryptography-aes-gcm

Gini. "What Is Least Significant Bit Algorithm in Information Security?" Www.tutorialspoint.com, 11 Mar. 2022, www.tutorialspoint.com/what-is-least-significant-bit-algorithm-in-information-security.

Hameed, R. S., Hasan, F. F., & Abdulbaqi, A. S. (2024). Adaptive Image Steganography Domain: A review of the recent works. Lecture Notes in Networks and Systems, 1–14. https://doi.org/10.1007/978-981-97-6318-4_1

Hattim, M. & Taha, Z. 2019. Secure and hidden text using aes cryptography and lsb steganography. Journal of Engineering Science and Technology 14(3): 1434–1450.

Hiyam Nadhim Khalid, Azana Hafizah Mohd Aman, A. H. M. A., & Hasimi Sallehuddin, H. S. (2021). Image Steganography: The method of hiding information (1st ed., Vol. 1). Penerbit Universiti Kebangsaan Malaysia.

Huang, Chiung-Wei & Chou, Changmin & Chiu, Yu-Che & Chang, cy. (2018). Embedded FPGA Design for Optimal Pixel Adjustment Process of Image Steganography. Mathematical Problems in Engineering. 2018. 1-8. 10.1155/2018/5216029.

Hussain, M., Wahab, A. W. A., Idris, Y. I. Bin, Ho, A. T. S. & Jung, K. H. 2018. Image steganography in spatial domain: A survey. Signal Processing: Image Communication 65(December 2017): 46–66. doi:10.1016/j.image.2018.03.012

Ismail, M. (2024, March 18). *Secure your data: AES-GCM encryption & Decryption for JavaScript, TypeScript, Java, and Python .* DEV Community. https://dev.to/ihssmaheel/shielding-your-data-aes-gcm-encryption-decryption-for-javascript-typescript-java-and-python-1cpm

K, P., & Jaitly, V. (2023). Securing medical images using compression techniques with encryption and image steganography. Securing Medical Images Using Compression Techniques With Encryption and Image Steganography, 1–7. https://doi.org/10.1109/conit59222.2023.10205855

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299–326. https://doi-org.eresourcesptsl.ukm.remotexs.co/10.1016/j.neucom.2018.06.075

Kaur, R., & Mahajan, M. (2016). Random Pattern based sequential bit (RaP-SeB) Steganography with Cryptography for Video Embedding. International Journal of Modern Education and Computer Science, 8(9), 51–59. https://doi.org/10.5815/ijmecs.2016.09.07

Kumar, R., & Singh, H. (2019). Recent trends in text steganography with experimental study. Springer International Publishing. https://doi-org.eresourcesptsl.ukm.remotexs.co/10.1007/978-3-030-22277-2_34

Latifah Arifin. “Trend Jenayah Dalam Talian Meningkat Secara Ketara Tahun Demi Tahun - JSJK Bukit Aman.” Berita Harian, 5 Sept. 2024, www.bharian.com.my/berita/nasional/2024/09/1294533/trend-jenayah-dalam-talian-meningkat-secara-ketara-tahun-demi-tahun.

Liao, X., Yu, Y., Li, B., Li, Z., & Qin, Z. (2020). A New Payload Partition Strategy in Color Image Steganography. IEEE Transactions on Circuits and Systems for Video Technology, 30(3), 685-696.

Metallurgical. (n.d.). *LSB-steganography-javascript/lsb-steganography.js at master · metallurgical/LSB-steganography-javascript*. GitHub.

Pandey, J., Joshi, K., Jangra, M., & Sain, M. (2019, May 1). Pixel Indicator Steganography Technique with Enhanced Capacity for RGB Images. IEEE Xplore.

Rachael, O., Misra, S., Ahuja, R., Adewumi, A., Ayeni, F. & Mmaskeliunas, R. 2020. Image Steganography and Steganalysis Based on Least Significant Bit (LSB). Lecture Notes in Electrical Engineering 605(September): 1100–1111. doi:10.1007/978-3-030-30577-2_97

Rana Sami Hameed, Forat Falih Hasan, Azmi Shawkat Abdulbaqi, "Adaptive Image Steganography Domain: A Review of the Recent Works", Proceedings of Fifth Doctoral Symposium on Computational Intelligence, vol.1095, pp.1, 2024.

Roy, S., & Kapoor, V. (2020). High Data Rate Audio Steganography (Vol. 1059). Springer. https://doi-org.eresourcesptsl.ukm.remotexs.co/10.1007/978-981-15-0324-5_43

Shanthakumari, R., & Malliga, S. (2020). Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. Multimedia Tools and Applications, 79(5-6), 3975-3991.

Taha, Mustafa & Hashim, Mohammed & Khalid, Hiyam & Aman, Azana. (2021). A Steganography Embedding Method Based on Psingle / Pdouble and Huffman Coding. 10.1109/CRC50527.2021.9392522.

Taha, Mustafa & Mahdi, Qasim & Sabah, Mustafa & Shafry, Mohd & Rahim, Mohd & Hashim, Mohammed & Mardziah, Aina & Ahmad, Binti. (2018). Categorization of spatial domain techniques in image steganography: A revisit. Journal of Advanced Research in Dynamical and Control Systems. 10. 13.

Web Cyb. (2024, August 27). *2. Creating a Simple Password Manager with JavaScript | Encryption & Decryption* [Video]. YouTube. https://www.youtube.com/watch?v=UnYN5HyPMSI

Younus, Z. S., & Hussain, M. K. (2019). Image steganography using exploiting modification direction for compressed encrypted data. Journal of King Saud University - Computer and Information Sciences.

Zhao, X., Yang, C., & Liu, F. (2021a). On the Sharing-Based Model of Steganography. In Lecture notes in computer science (pp. 94–105)

Muhammad Nuraiman Bin Johari (A200136)
Dr. Azana Hafizah Binti Mohd Aman
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia