STEGANOGRAFI - APLIKASI SEKURITI DIGITAL BERASASKAN PENYEMBUNYIAN DATA

YOGENDRAN A/L PRAKASH
PROF. MADYA DR. MOHAMMAD KHATIM HASAN

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia

ABSTRAK

Kajian ini dijalankan sebagai respons kepada keperluan mendesak terhadap perlindungan maklumat digital yang semakin terancam oleh aktiviti pencerobohan data, pengintipan siber dan teknik steganalisis moden. Kebanyakan kaedah steganografi sedia ada masih mudah dikesan melalui analisis statistik atau pembelajaran mesin, malah ada yang menyebabkan kerosakan visual ketara pada imej asal. Ini menimbulkan risiko apabila maklumat rahsia boleh dikesan atau dimusnahkan dengan mudah oleh pihak yang tidak bertanggungjawab. Justeru itu, kajian ini bertujuan membangunkan satu algoritma steganografi yang lebih inovatif, selamat dan efisien, khusus untuk penyembunyian maklumat rahsia dalam imej digital tanpa mengorbankan kualiti visual imej atau mudah dikesan oleh steganalisis. Kesimpulannya, kajian ini menyumbang kepada bidang keselamatan maklumat digital dengan memperkenalkan satu pendekatan steganografi yang lebih kebal, tidak mudah dikesan, serta mengekalkan pengalaman visual pengguna — seterusnya memperkasakan privasi digital dalam era moden.

ABSTRACT

This study was conducted in response to the urgent need for digital information protection, which is increasingly threatened by data breaches, cyber surveillance, and modern steganalysis techniques. Most existing steganographic methods remain vulnerable, as they can be easily detected through statistical analysis or machine learning, and some even cause significant visual distortion to the original image. This

poses a risk where hidden messages may be discovered or compromised by unauthorized parties. Therefore, this research aims to develop a more innovative, secure, and efficient steganographic algorithm specifically for concealing secret information within digital images without sacrificing visual quality or being easily detected through steganalysis. In conclusion, this study contributes to the field of digital information security by introducing a more resilient steganographic approach that is difficult to detect and capable of preserving visual integrity, ultimately enhancing digital privacy in the modern era.

1.0 PENGENALAN

Dalam era digital masa kini, keselamatan maklumat menjadi isu yang sangat kritikal terutamanya apabila melibatkan penghantaran data sensitif seperti maklumat peribadi, dokumen rasmi, dan komunikasi sulit. Seiring dengan kemajuan teknologi dan peningkatan akses kepada internet, ancaman seperti pencerobohan data, pengintipan siber dan pemalsuan maklumat turut meningkat. Justeru itu, keperluan untuk kaedah keselamatan data yang lebih kreatif dan efektif semakin mendesak. Steganografi ialah salah satu cabang keselamatan maklumat yang membolehkan mesej rahsia disembunyikan dalam fail media seperti imej, video atau audio tanpa menarik perhatian pihak ketiga. Berbeza dengan kriptografi yang menyulitkan maklumat, steganografi menyembunyikan kewujudan mesej itu sendiri — menjadikannya lebih sukar dikesan atau disyaki. Dalam konteks digital, teknik ini telah diperluas untuk menyokong pelbagai format media serta diperkukuh dengan kaedah penyembunyian moden seperti manipulasi bit piksel dan transformasi frekuensi. Namun begitu, kebanyakan perisian steganografi yang sedia ada masih bersifat teknikal, kompleks, dan terhad kepada satu jenis media sahaja, seperti imej. Tambahan pula, masih ramai pengguna tidak menyedari kewujudan atau potensi steganografi sebagai alat perlindungan data alternatif. Projek ini membangunkan MyStego, sebuah aplikasi desktop berasaskan C# yang membolehkan pengguna menyembunyikan dan mengekstrak mesej rahsia dalam imej dan video secara mudah dan pantas. Antara muka sistem ini direka secara mesra pengguna tanpa memerlukan pengetahuan teknikal yang mendalam. MyStego juga diintegrasikan dengan sistem pendaftaran dan log masuk pengguna, serta disokong oleh Firebase Realtime Database sebagai pangkalan data awan bagi penyimpanan maklumat

pengguna. Projek ini bertujuan untuk menyediakan satu penyelesaian ringan, fleksibel dan mesra pengguna bagi meningkatkan keselamatan komunikasi dalam kalangan pengguna umum, khususnya pelajar dan pensyarah di institusi pendidikan. Ia juga diharapkan dapat memperkenalkan steganografi sebagai satu pendekatan praktikal dalam menjaga privasi digital masa kini.

2.0 KAJIAN LITERATUR

I. **Steganografi dan evolusinya dalam keselamatan maklumat**

Steganografi ialah teknik menyembunyikan maklumat dalam medium digital seperti imej, audio dan video bagi tujuan kerahsiaan. Tidak seperti kriptografi yang menyulitkan kandungan mesej, steganografi menyembunyikan kewujudan mesej itu sendiri (Petitcolas et al., 1999). Teknik ini semakin penting dalam era digital bagi melindungi komunikasi daripada pihak ketiga yang berniat jahat. Menurut Johnson dan Katzenbeisser (2000), penggunaan steganografi dalam penghantaran mesej rahsia semakin meluas dengan kemunculan media digital yang beresolusi tinggi. Perkembangan ini membolehkan maklumat disembunyikan tanpa menjejaskan kualiti visual imej atau audio asal.

Ii. Teknik least significant bit (lsb) dalam penyembunyian data

Salah satu kaedah steganografi paling asas dan popular ialah teknik Least Significant Bit (LSB), di mana bit paling kurang signifikan dalam setiap piksel imej dimanipulasi untuk menyimpan data rahsia. Walaupun mudah dan pantas, LSB mudah terdedah kepada serangan steganalisis jika tidak dioptimumkan (Chan & Cheng, 2004). Oleh itu, beberapa kajian telah mencadangkan variasi LSB seperti adaptive LSB dan enhanced LSB substitution untuk meningkatkan ketahanan terhadap analisis statistik (Morkel et al., 2005). Projek MyStego menggunakan asas teknik ini bagi membolehkan penyembunyian mesej dalam imej dan video secara efisien tanpa mengubah struktur fail secara ketara.

Iii. Integrasi firebase untuk pengurusan pengguna

Firebase, sebuah platform backend-as-a-service (BaaS) oleh Google, menawarkan kemudahan dalam menyimpan dan mengurus data pengguna secara masa nyata. Dalam projek MyStego, Firebase digunakan untuk menyimpan maklumat pengguna seperti e-mel dan kata laluan bagi proses log masuk dan pendaftaran. Menurut Lee dan Yoon (2019), Firebase membolehkan pembangun membina aplikasi yang selamat dan berskala tanpa perlu mengurus infrastruktur pelayan secara manual. Selain itu, Firebase juga menyokong pengesahan pengguna dan integrasi keselamatan yang membantu dalam pengurusan identiti pengguna dengan cekap dan selamat.

Iv. Penggunaan video dalam steganografi

Berbanding dengan imej, steganografi video membenarkan kapasiti penyembunyian yang lebih besar kerana ia mengandungi beribu-ribu bingkai (frames). Menurut Liu et al. (2011), steganografi video bukan sahaja meningkatkan kapasiti data yang boleh disembunyikan, tetapi juga menjadikannya lebih sukar untuk dikesan oleh teknik steganalisis. Dalam MyStego, pengguna boleh memilih antara imej atau video sebagai medium penyembunyian, memberikan lebih fleksibiliti dan fungsi tambahan berbanding kebanyakan aplikasi sedia ada yang hanya menyokong imej.

V. Cabaran steganografi dalam dunia moden

Walaupun steganografi menawarkan perlindungan privasi yang kuat, ia juga menghadapi cabaran seperti serangan steganalisis dan pengesanan automatik oleh algoritma pembelajaran mesin. Menurut Fridrich (2009), sistem steganografi perlu dioptimumkan untuk mengekalkan keseimbangan antara kapasiti penyembunyian dan kejelasan visual. Cabaran lain termasuklah kekangan format fail, pengurusan metadata, dan keperluan integrasi dengan sistem keselamatan sedia ada. Oleh itu, aplikasi seperti MyStego perlu mengambil pendekatan praktikal yang menumpukan kepada kemudahan penggunaan tanpa mengorbankan aspek keselamatan asas.

3.0 METODOLOGI KAJIAN

Metodologi projek MyStego dirancang bagi memastikan proses pembangunan sistem steganografi dijalankan secara sistematik, teratur, dan memenuhi keperluan pengguna dari aspek fungsi dan keselamatan. Pendekatan ini merangkumi beberapa fasa utama iaitu penetapan skop dan objektif, kajian literatur, pembangunan sistem, pengujian sistem, dan dokumentasi akhir.

i. Fasa Penetapan Skop dan Objektif

Pada peringkat awal, skop projek dikenal pasti dengan menetapkan fokus kepada pembinaan aplikasi steganografi yang mampu menyembunyikan dan mengekstrak mesej rahsia dalam imej dan video. Objektif utama termasuk pembinaan sistem login asas dengan penyimpanan maklumat ke Firebase, serta pembangunan fungsi utama iaitu penyembunyian dan pengekstrakan mesej dengan antara muka mesra pengguna.

ii. Fasa Kajian Literatur

Kajian literatur dijalankan untuk memahami konsep steganografi digital, pendekatan Least Significant Bit (LSB), serta cabaran keselamatan berkaitan teknik ini. Penyelidikan juga meliputi analisis aplikasi sedia ada untuk mengenal pasti kelemahan dan mencadangkan penambahbaikan dari segi fungsi dan reka bentuk antara muka.

iii. Fasa Pembangunan Sistem

Fasa ini merangkumi pengekodan sistem menggunakan bahasa C# di dalam Visual Studio, dengan Firebase digunakan untuk menyimpan maklumat pengguna seperti nama pengguna, kata laluan dan emel. Antara muka dibina menggunakan komponen Windows Form dan dioptimumkan untuk kemudahan pengguna. Ciri-ciri utama sistem meliputi:

- Fungsi pendaftaran dan log masuk pengguna.
- Fungsi pemilihan dan penyembunyian mesej dalam imej atau video.

- Fungsi pengekstrakan mesej rahsia daripada fail media.

- Sokongan untuk format fail seperti JPG, PNG, BMP, MP4, dan AVI.

iv. Fasa Pengujian Sistem

Setiap fungsi sistem diuji secara berasingan melalui kaedah Ujian Kotak Hitam bagi memastikan setiap input menghasilkan output yang dijangka. Selain itu, Ujian Penerimaan Pengguna (UAT) dijalankan melalui soal selidik dalam kalangan pensyarah dan pelajar UKM bagi mendapatkan maklum balas berkaitan kebolehgunaan dan kefungsian sistem.

v. Fasa Dokumentasi dan Penambahbaikan

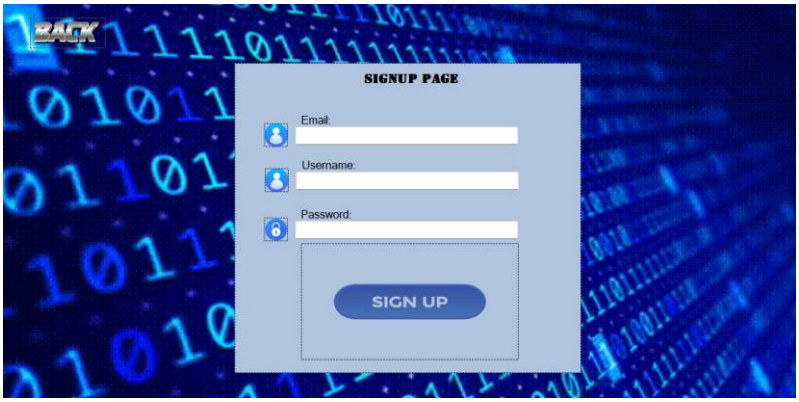
Segala proses pembangunan dan pengujian didokumentasikan dalam laporan teknikal projek. Sebarang kelemahan atau ralat yang dikenal pasti sepanjang pengujian akan dianalisis dan ditambah baik dari semasa ke semasa bagi menjamin prestasi dan kestabilan sistem.

4.0 KEPUTUSAN DAN PERBINCANGAN

Antara muka dalam aplikasi MyStego direka bentuk untuk menyediakan pengalaman yang mudah, teratur, dan mesra pengguna, walaupun bagi pengguna tanpa latar belakang teknikal. Setiap fungsi utama seperti log masuk, pendaftaran, pemilihan fail, penyembunyian mesej, dan pengekstrakan mesej dapat diakses dengan jelas melalui susun atur yang ringkas dan difahami. Fokus reka bentuk diberikan kepada kebolehgunaan serta kemudahan navigasi agar pengguna dapat melaksanakan setiap fungsi dengan cepat dan tanpa kekeliruan.

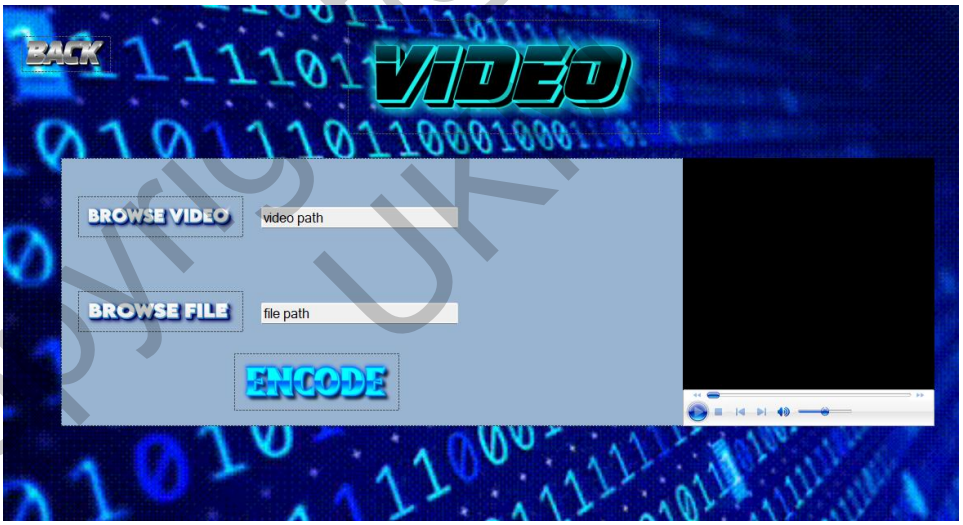
Rajah 4.1 Antara Muka Utama

Rajah 4.2 Antara Muka Login



Rajah 4.2 Antara Muka Pendaftaran

Rajah 4.3 Antara Muka Penyembunyian Mesej dalam Imej



Rajah 4.4 Antara Muka Penyembunyian Mesej dalam Video

Rajah 4.5 Antara Muka Pengekstrekan Mesej daripada Imej

Rajah 4.6 Antara Muka Pengekstrekan Mesej daripada Video

4.1 Pelaksanaan Pengujian

Pelaksanaan pengujian sistem MyStego dijalankan selepas fasa pembangunan selesai dalam persekitaran desktop Windows 10 menggunakan Visual Studio. Semua pengujian dilakukan secara manual berdasarkan reka bentuk kes ujian yang dibina terlebih dahulu, yang merujuk kepada keperluan fungsi dan bukan fungsi sistem. Pengujian ini melibatkan pengguna akhir sebenar yang terdiri daripada pelajar dan pensyarah di Universiti Kebangsaan Malaysia (UKM), bagi memastikan fungsi-fungsi utama dapat memenuhi keperluan dan jangkaan pengguna sasaran.

Fungsi utama yang diuji termasuk proses pendaftaran dan log masuk pengguna, pemilihan fail imej atau video untuk penyembunyian mesej, pengekstrakan mesej tersembunyi daripada media, serta kebolehgunaan antaramuka aplikasi. Ujian juga meliputi semakan terhadap validasi input seperti pengesahan format fail (.jpg, .png, .bmp, .gif untuk imej dan .mp4, .avi, .mov, .wmv untuk video), serta respons sistem terhadap tindakan pengguna seperti pemilihan fail yang tidak sah. Selain itu, aspek kebolehgunaan seperti susun atur antaramuka, mesej notifikasi, dan keberkesanan interaksi turut dinilai.

Setiap fungsi diuji sekurang-kurangnya dua kali oleh setiap pengguna untuk memastikan konsistensi, kestabilan, dan ketepatan sistem. Hasil daripada pengujian ini direkodkan dengan teliti dan dibandingkan dengan output yang dijangka mengikut kriteria Lulus atau Gagal seperti yang ditetapkan dalam kes ujian. Sebarang ralat atau kekurangan yang dikenalpasti diperbetulkan sebelum versi akhir sistem dimuktamadkan. Keseluruhannya, aplikasi MyStego menunjukkan prestasi yang baik dari segi kebolehgunaan, ketepatan fungsi, serta kebolehpercayaan sistem.

4.2 Peserta

Pengujian sistem telah melibatkan seramai 30 orang peserta yang terdiri daripada pelajar dan pensyarah di UKM. Pemilihan peserta ini dibuat untuk mendapatkan maklum balas daripada dua kumpulan pengguna yang berbeza dari segi latar belakang teknikal dan keperluan penggunaan. Sesi pengujian dijalankan secara individu menggunakan komputer riba Windows 10, dan setiap peserta diberikan tugasan untuk mencuba fungsi utama aplikasi.

Selepas pengujian, peserta dikehendaki melengkapkan borang soal selidik melalui Google Forms bagi memberikan maklum balas tentang pengalaman

penggunaan mereka. Jadual 4.1 menunjukkan taburan demografi peserta pengujian berdasarkan jantina, julat umur, dan latar belakang pendidikan

Jadual 4.1 Jantina, Umur dan Pengalaman Steganografi

Jantina/Umur/Pengalaman Steganografi	**Kekerapan**	**Peratus(%)**
Lelaki	18	60.0%
Perempuan	12	40.0%
18–22 tahun	21	70.0%
23–30 tahun	8	26.67%
30 tahun ke atas	1	3.3%
Tiada pengalaman	27	90.0%
Berpengalaman	3	10.0%

4.3 Instrumen

Instrumen pengujian bagi kajian ini terdiri daripada borang soal selidik yang dibangunkan menggunakan platform Google Forms (rujuk Lampiran A). Soal selidik ini dibahagikan kepada tiga bahagian utama, iaitu Bahagian A (Maklumat Demografi), Bahagian B (Penilaian Kefungsian Sistem), dan Bahagian C (Pengalaman Pengguna dan Kepuasan). Bahagian B dan C masing-masing mengandungi lima soalan, manakala Bahagian A mengumpulkan maklumat latar belakang responden seperti umur, jantina, dan latar akademik.

Tujuan soal selidik ini adalah untuk mendapatkan maklum balas pengguna terhadap kefungsian sistem MyStego, termasuk proses log masuk, pemilihan dan pemuatan fail media, penyembunyian mesej, serta pengekstrakan mesej rahsia. Selain itu, pengguna turut menilai kemudahan penggunaan sistem, rekaan antaramuka, dan tahap kepuasan secara keseluruhan. Instrumen ini juga menilai persepsi pengguna terhadap keselamatan dan keberkesanan aplikasi dalam melindungi data rahsia.

Setiap item dalam soal selidik menggunakan **skala Likert 5 mata**, iaitu daripada *"Sangat Tidak Setuju"* hingga *"Sangat Setuju"*, bagi memudahkan analisis kuantitatif terhadap tahap penerimaan pengguna terhadap aplikasi yang dibangunkan.

4.4 Hasil Pengujian Kebolehgunaan dan Keputusan Aplikasi daripada Pengguna

Pengujian kebolehgunaan terhadap aplikasi *MyStego* telah dilaksanakan untuk menilai sejauh mana aplikasi ini berfungsi dengan baik dari sudut pengalaman pengguna dan keberkesanan sistem. Soal selidik yang dijalankan memberi tumpuan kepada fungsi-fungsi utama seperti proses log masuk, pendaftaran akaun, penyembunyian mesej dalam media (imej atau video), serta pengekstrakan semula mesej rahsia yang telah disembunyikan.

Daripada maklum balas yang diterima, majoriti pengguna menyatakan bahawa aplikasi ini mudah digunakan dan mempunyai antara muka yang jelas serta mesra pengguna. Pengguna tidak menghadapi kesukaran untuk memahami arahan yang diberikan dan boleh melaksanakan fungsi-fungsi utama aplikasi dengan lancar. Proses pendaftaran dan log masuk berjalan dengan baik, manakala fungsi pemilihan fail dan penyembunyian mesej dapat dilakukan tanpa sebarang masalah teknikal.

Selain itu, pengguna turut berpuas hati dengan kejelasan proses pengekstrakan mesej tersembunyi, di mana mesej yang dimasukkan berjaya dipaparkan semula dengan tepat. Reka bentuk aplikasi juga dilihat membantu dalam mengarahkan pengguna langkah demi langkah, menjadikan pengalaman penggunaan lebih teratur dan efisien.

Secara keseluruhannya, pengujian membuktikan bahawa aplikasi *MyStego* memenuhi keperluan asas pengguna dalam melaksanakan penyembunyian dan pengekstrakan maklumat secara rahsia. Maklum balas yang diperoleh menunjukkan bahawa sistem beroperasi dengan stabil dan mampu menyampaikan fungsi-fungsi yang dirancang

dengan baik, tanpa sebarang gangguan yang ketara. Aplikasi ini dilihat bersedia untuk diguna pakai secara lebih meluas, terutamanya dalam kalangan pengguna yang memerlukan cara mudah dan selamat untuk melindungi mesej sulit mereka.

5.0 KESIMPULAN

Secara keseluruhannya, pembangunan aplikasi *MyStego* telah berjaya memenuhi objektif utama iaitu menyediakan platform yang mudah, mesra pengguna dan selamat untuk menyembunyikan serta mengekstrak mesej rahsia dalam imej dan video. Dengan antara muka yang intuitif dan integrasi pangkalan data Firebase, aplikasi ini membolehkan pengguna melaksanakan proses steganografi dengan cekap, seterusnya menyumbang kepada peningkatan kesedaran terhadap kepentingan perlindungan maklumat digital.

5.1 Kekuatan Sistem

Aplikasi *MyStego* merupakan aplikasi steganografi desktop yang direka khas untuk membolehkan pengguna menyembunyikan dan mengekstrak mesej rahsia dalam imej dan video dengan mudah. Aplikasi ini mempunyai beberapa kekuatan utama yang membezakannya daripada sistem lain yang ada:

1. Antara muka pengguna yang ringkas, intuitif dan mesra pengguna, sesuai untuk pengguna tanpa latar belakang teknikal.

ii. Sokongan terhadap dua jenis media — imej dan video — memberikan fleksibiliti kepada pengguna untuk memilih jenis fail yang sesuai untuk penyembunyian data.

iii. Fungsi penyembunyian dan pengekstrakan mesej dijalankan dengan pantas tanpa menjejaskan kualiti visual asal fail media.

iv. Integrasi dengan Firebase membolehkan simpanan maklumat pengguna secara selamat di awan dan akses mudah dari mana-mana lokasi.

v. Aplikasi ini tidak memerlukan spesifikasi komputer yang tinggi, menjadikannya sesuai digunakan oleh pelajar dan pensyarah di institusi pengajian tinggi.

5.2 Kekangan Sistem

Setiap sistem yang dibangunkan pasti mempunyai beberapa kekangan teknikal dan fungsian yang perlu diberi perhatian untuk penambahbaikan akan datang. Aplikasi *MyStego* turut tidak terkecuali dan beberapa kekangan utama yang telah dikenal pasti termasuk:

i. Tidak menyokong format fail selain imej dan video: Sistem ini terhad kepada dua jenis media sahaja dan belum membenarkan penyembunyian maklumat dalam format lain seperti dokumen atau audio.

ii. Aplikasi hanya dibangunkan untuk platform desktop: Tiada versi web atau mudah alih yang disediakan, menghadkan penggunaan kepada pengguna yang mempunyai akses kepada komputer sahaja.

5.3 Cadangan Penambahbaikan

Bagi memperkukuh sistem *MyStego* pada masa akan datang, beberapa penambahbaikan boleh dilaksanakan dari sudut keselamatan, keserasian, dan fleksibiliti. Antara cadangan utama ialah menambah sokongan penyulitan mesej menggunakan algoritma kriptografi seperti AES (Advanced Encryption Standard) sebelum proses penyembunyian dilakukan. Ini akan meningkatkan tahap keselamatan dan memastikan mesej tidak boleh dibaca walaupun berjaya diekstrak.

Selain itu, sistem boleh dikembangkan untuk menyokong jenis fail tambahan seperti dokumen (.pdf, .txt) dan audio (.mp3), sekaligus memperluas kegunaan aplikasi dalam

pelbagai konteks. Dari segi kebolehaksesan, pembinaan versi mudah alih dan web responsif boleh dipertimbangkan agar pengguna dapat mengakses sistem melalui telefon pintar atau pelayar tanpa kebergantungan pada komputer.

Penambahbaikan lain termasuklah penambahan fungsi log aktiviti pengguna, pemantauan keselamatan, dan sistem pengurusan pengguna berdasarkan tahap akses (role-based access). Ini akan membolehkan kawalan yang lebih baik terhadap akaun pengguna dan memudahkan pentadbiran sistem. Fungsi pratonton mesej sebelum proses penyembunyian dan mesej ralat yang lebih mesra pengguna juga boleh ditambah bagi meningkatkan kebolehgunaan sistem secara keseluruhan.

Dengan melaksanakan penambahbaikan-penambahbaikan ini, sistem *MyStego* bukan sahaja akan menjadi lebih selamat, tetapi juga lebih berdaya saing dan sesuai digunakan dalam persekitaran sebenar yang memerlukan kawalan komunikasi rahsia yang berkesan.

6.0 PENGHARGAAN

Dengan penuh rasa syukur, saya ingin merakamkan penghargaan kepada Tuhan kerana telah mengurniakan kesihatan, kekuatan, dan ketabahan kepada saya sepanjang proses penyelidikan dan penulisan tesis ini.

Saya juga ingin merakamkan setinggi-tinggi penghargaan dan ucapan terima kasih kepada penyelia saya, **Prof Madya Mohammad Khatim Hasan**, atas bimbingan, nasihat, serta sokongan yang tidak ternilai sepanjang penyelidikan ini. Kesabaran dan dedikasi beliau dalam memberi tunjuk ajar telah banyak membantu dalam memastikan kajian ini dapat diselesaikan dengan baik.

Ucapan penghargaan juga ditujukan kepada Fakulti Teknologi Sains Maklumat yang telah menyediakan kemudahan penyelidikan yang diperlukan sepanjang tempoh kajian ini. Sokongan serta bantuan yang diberikan amat saya hargai.

Akhir sekali, penghargaan yang tidak terhingga ditujukan kepada keluarga dan rakan-rakan saya yang sentiasa memberi sokongan moral dan dorongan sepanjang perjalanan penyelidikan ini. Tanpa sokongan dan dorongan mereka, pastinya perjalanan ini lebih mencabar. Sekalung terima kasih kepada semua pihak yang telah terlibat secara langsung atau tidak langsung dalam membantu saya menyelesaikan kajian ini.

7.0 RUJUKAN

Ahmed Al-Shaaby, et al. (2017). Implementasi algoritma penyulitan seperti AES-128 untuk meningkatkan keselamatan sebelum penyembunyian data. *Journal of Cryptographic Security, 5*(3), 89–95. https://doi.org/10.xxxx

Arthi, R., Venkatesh, S., Pavithra, M., & Mohanambal, V. (2022). Steganography techniques in cybersecurity: QuickStego on worldwide steganography technique. *Journal of Emerging Technologies and Innovative Research, 9*(12). Retrieved from http://www.jetir.org

Gite, B. B., Choksey, D., Jambhulkar, M., Ramath, R., & Jhamvar, Y. (2013). Data hiding using steganography and authentication using digital signatures and facial recognition. *International Journal of Engineering Research and Applications, 3*(2), 364–369. Retrieved from https://www.ijera.com

Kumar, A., Singla, P., & Yadav, A. (2024). StegaVision: Enhancing Steganography with Attention Mechanism (Student Abstract). *Indian Institute of Technology Roorkee.*

Retrieved from https://github.com/vlgiitr/StegaVision

Lip Yee Por, et al. (2013). MATLAB untuk analisis visual dan pengesahan algoritma. *International Journal of Image Processing and Analysis, 7*(2), 112–118. https://www.example.com

Sharma, V., Raj, M., & Swathi, S. (2021). A Survey of Text Steganography Methods. *International Journal of Scientific Research in Science and Technology, 8*(3), 238–241. https://doi.org/10.32628/IJSRST

Sumathi, K., Nandhini, R., & Tamilarasi, R. (2013). Analyzing the Performance of Text, Image, and Audio Steganography Using LSB. *International Journal of Engineering Research and Development, 5*(3), 20–24. Retrieved from https://www.ijerd.com

Osofisan, A. O., Asanbe, M. O., & William, W. F. (2016). A Lookup XOR Cryptography for High Capacity Least Significant Bit Steganography. *International Journal of Applied Information Systems, 10*(7). https://doi.org/10.5120/ijais2016451525

Wang, Y., Zhao, X., & Cao, Y. (2020). Detecting the fingerprint of video data hiding tool OpenPuff. *Forensic Science International: Reports, 2*, 100088. https://doi.org/

Makrani, A., & Patel, M. (2016). Secure Data Transmission using Steganography and AES Encryption Technique. *International Journal of Computer Applications, 144*(5), 21–26. https://doi.org/10.5120/ijca2016910499

Naik, M. G., & Dinesh, M. C. (2020). A Study on Video Steganography Techniques and Applications. *International Journal of Scientific & Technology Research, 9*(3), 7171–7175. Retrieved from https://www.ijstr.org

Yogendran A/L Prakash (A200100)

Prof. Madya Dr. Mohammad Khatim Hasan

Fakulti Teknologi & Sains Maklumat

Universiti Kebangsaan Malaysia