ZAHIRAN – SEMBUNYI PESANAN TEKS RAHSIA

MOHAMAD ZAHIRAN BIN ZAHARI

TS. DR. NAZHATUL HAFIZAH KAMARUDIN

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

ABSTRAK

Projek ini memberi tumpuan kepada pembangunan aplikasi "Zahiran - Sembunyi Pesanan Teks Rahsia," dengan matlamat menyediakan platform penyembunyian mesej teks dalam fail imej secara senyap tanpa menjejaskan kualiti visual imej. Untuk menangani isu privasi mesej teks dalam era digital, aplikasi ini menggunakan kaedah steganografi Least Significant Bit (LSB) untuk menyembunyikan dan mengekstrak mesej teks. Dengan menggunakan Python dan perpustakaan seperti tkinter dan stegano, aplikasi ini memberi sumbangan kepada bidang keselamatan maklumat dan steganografi dengan menyediakan alat yang mudah digunakan untuk meningkatkan kesedaran dan pemahaman terhadap teknologi penyembunyian maklumat dalam kehidupan digital sehari-hari. Selain itu, kaedah implementasi LSB yang digunakan dalam projek ini diharapkan dapat menjadi panduan dan sumber pembelajaran bagi penyelidik dan pembangun yang berminat dalam bidang steganografi digital.

Kata kunci: Zahiran, “Encrypt”, “Decrypt”, “Steganography”

PENGENALAN

Dalam dunia yang dikendalikan oleh komunikasi digital dan perkongsian data, keselamatan dan kerahsiaan maklumat telah menjadi sangat penting. Projek Zahiran - Sembunyi Pesanan Teks Rahsia muncul sebagai satu usaha yang meneraju, direka untuk mengatasi cabaran kontemporari pertukaran maklumat yang selamat dan penyembunyian data sensitif. Ia mewakili gabungan kreativiti dan teknologi terkini, membolehkan pengguna untuk menyembunyikan dan mendedahkan mesej teks rahsia dalam imej dengan lancar.

Projek Zahiran - Sembunyi Pesanan Teks Rahsia merangkumi inti inovasi dan kegunaan. Ia adalah bukti kekuatan teknologi yang digunakan untuk keselamatan dan ekspresi seni. Dalam landskap di mana komunikasi digital telah menjadi norma, Projek Zahiran - Sembunyi Pesanan Teks Rahsia menawarkan perpaduan unik antara kreativiti dan kebolehan, membenarkan pengguna melindungi maklumat sensitif mereka sambil mengamalkan seni manipulasi data.

Cabaran Kontemporari: Menyelamatkan Maklumat dalam Zaman Digital

Ketika alam digital terus berkembang, begitu juga kepentingan untuk melindungi maklumat yang dikongsi di dalamnya. Di dunia di mana data dihantar, disimpan, dan dikongsi dengan mudah yang belum pernah terjadi sebelumnya, terdapat keperluan mendesak untuk alat yang melindungi data ini daripada mata-mata dan akses yang tidak dibenarkan. Keperluan ini meluas ke pelbagai domain, termasuk pengaturcaraan peribadi, profesional, dan institusi.

Projek Zahiran - Sembunyi Pesanan Teks Rahsia mengakui keperluan ini dan melangkah ke hadapan untuk menyediakan penyelesaian yang berkesan. Ia mengiktiraf kebimbangan yang semakin meningkat berkaitan dengan privasi data, keselamatan siber, dan komunikasi rahsia, dan berusaha untuk menawarkan platform yang mesra pengguna dan serbaguna untuk menangani kebimbangan ini.

Wawasan Projek Zahiran - Sembunyi Pesanan Teks Rahsia

Wawasan Projek Zahiran - Sembunyi Pesanan Teks Rahsia bersandar kepada keyakinan bahawa komunikasi digital boleh menjadi selamat dan kreatif pada masa yang sama. Ia

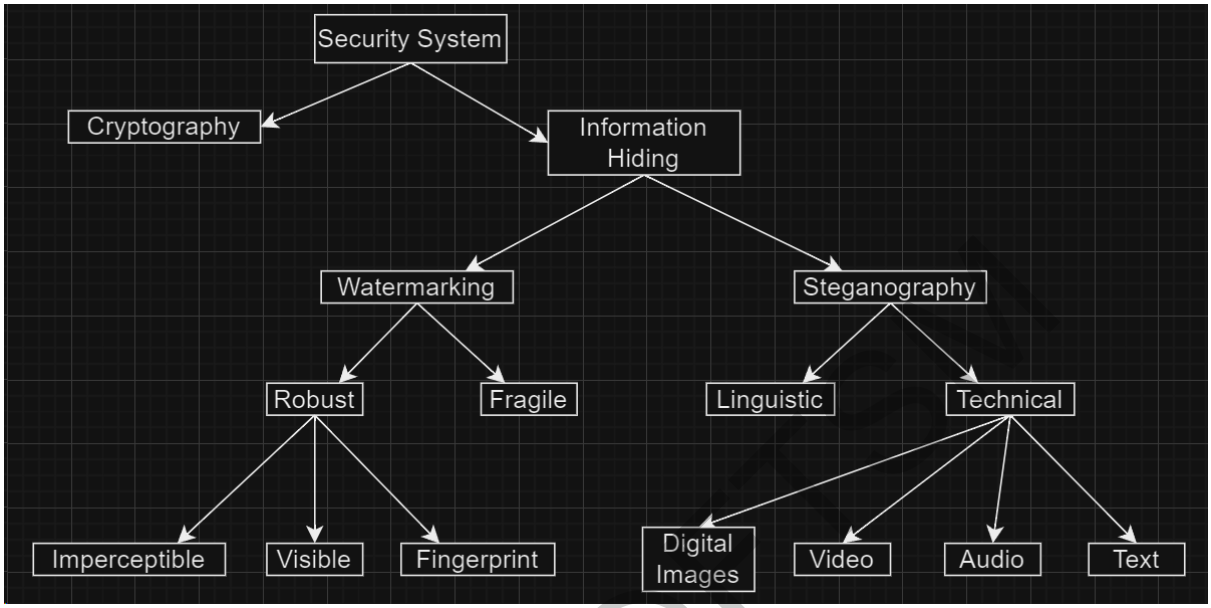
membayangkan dunia di mana individu dan organisasi boleh melindungi maklumat sensitif dalam lapisan seni. Istilah "Zahiran" sendiri diilhamkan oleh perkataan Arab "زهيران," yang membawa maksud sesuatu yang disembunyikan, mencerminkan tujuan asas projek ini.

Projek Zahiran - Sembunyi Pesanan Teks Rahsia berhasrat untuk menawarkan tempat perlindungan yang selamat bagi pengguna untuk berkomunikasi secara rahsia, dengan menggunakan kanvas imej digital sebagai medium mereka. Ia bertujuan untuk memupuk perasaan kebebasan dan keselamatan, membolehkan pengguna untuk pertukaran maklumat sensitif tanpa rasa takut dari penangkapan atau akses yang tidak dibenarkan. Wawasan ini bukan sahaja berkisar tentang keselamatan data; ia adalah tentang memberdayakan pengguna untuk menjadi seniman komunikasi selamat mereka sendiri.

Konsep steganografi pertama kali diperkenalkan dalam [1] pada tahun 1983. Steganografi yang merupakan seni menyembunyikan maklumat di dalam media yang seolah-olah tidak mencurigakan, telah menjadi aspek yang semakin penting dalam konteks keselamatan dan kerahsiaan maklumat. Steganografi menawarkan pelbagai kegunaan praktikal. Salah satu aplikasinya adalah dalam komunikasi sulit, di mana maklumat rahsia boleh disampaikan tanpa risiko menarik perhatian atau membawa ancaman daripada pihak yang berpotensi menyerang [2]. Dalam era di mana komunikasi digital melibatkan pertukaran data yang meluas dan ketidakpastian keselamatan semakin meningkat, keperluan untuk menggunakan alat dan sistem steganografi yang canggih dan berkesan semakin mendesak. Dengan kemajuan teknologi, banyak aplikasi dan sistem steganografi telah dikembangkan untuk memenuhi pelbagai keperluan pengguna.

Oleh itu, pemahaman mendalam mengenai kelebihan dan kelemahan setiap aplikasi serta algoritma yang digunakan untuk menyembunyikan maklumat menjadi kritikal. Kajian literasi ini bertujuan untuk memberikan gambaran menyeluruh mengenai pelbagai alat dan sistem steganografi yang sedia ada, merentasi berbagai jenis media seperti imej, audio, dan teks. Rajah 2.2 menunjukkan cabang-cabang berbeza dalam penyembunyian maklumat [3]. Dokumen ini berfokus pada penyembunyian maklumat melalui steganografi. Steganografi merupakan disiplin sains yang berkaitan dengan penghantaran data sulit secara rahsia dalam medium multimedia yang sesuai, seperti fail imej, audio, dan video. Pada dasarnya, steganografi melibatkan penyisipan fail, mesej, imej, atau video ke dalam fail, mesej, imej, atau video yang berkaitan. Istilah "steganografi" menggabungkan perkataan Yunani "stego,"

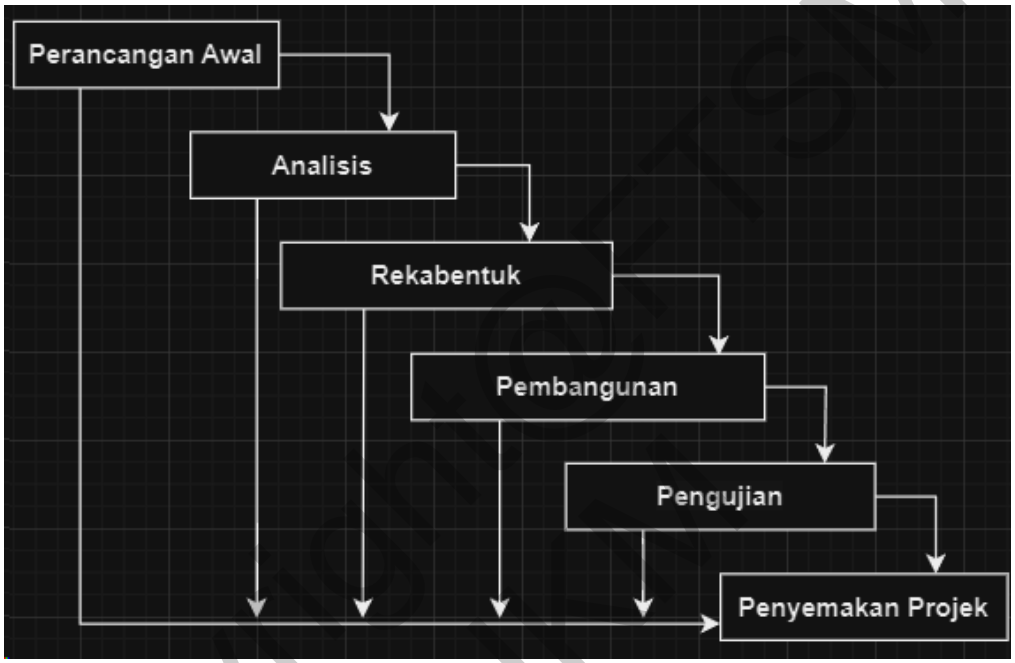
bermaksud "tutup," dan perkataan Yunani "grafia," bermaksud "penulisan," menghasilkan konsep "penulisan tertutup" [4].



Rajah 2.2 Cabang-cabang penyembunyian maklumat [1]

METODOLOGI KAJIAN

Metodologi Metodologi Projek Zahiran - Sembunyi Pesanan Teks Rahsia menggunakan metodologi *Waterfall* yang direka untuk memastikan bahawa pembangunan aplikasi ini berjalan dengan berkesan dan mencapai objektif projek secara sistematik. Berikut adalah langkah-langkah dan proses utama yang digunakan dalam metodologi Projek Zahiran - Sembunyi Pesanan Teks Rahsia:



Rajah 1.7 Model Waterfall

Fasa Perancangan Awal:

Pada fasa ini, matlamat dan objektif projek dikenalpasti dengan teliti. Ia termasuk penentuan ciri-ciri utama aplikasi, seperti keupayaan dan fungsi utama yang akan dimasukkan. Pendekatan dan teknik yang akan digunakan dalam pembangunan projek juga dirancang di sini. Selain itu, reka bentuk awal antara muka pengguna (UI) dibangunkan, menggambarkan bagaimana aplikasi akan kelihatan dan berinteraksi dengan pengguna. Aliran kerja atau proses langkah demi langkah yang akan diikuti dalam pembangunan projek disusun. Keperluan teknikal seperti perisian, perkakasan, dan alat pembangunan yang diperlukan juga dikenalpasti.

Fasa Analisis:

Fasa analisis melibatkan pengenalpastian keperluan pengguna utama dan keperluan teknikal projek. Dalam fasa ini, ciri-ciri dan fungsi yang diperlukan oleh pengguna akhir dikenal pasti,

termasuk pemilihan imej, input teks, penyembunyian data, dan pengambilan data. Keperluan teknikal dan sumber daya yang diperlukan untuk pembangunan aplikasi juga ditentukan. Setiap fungsi yang dirancang diperiksa untuk memastikan ia boleh beroperasi dengan betul dan memenuhi tujuan projek.

Fasa Rekabentuk:

Fasa rekabentuk melibatkan penciptaan pelan terperinci untuk aplikasi. Reka bentuk antara muka pengguna (UI) dihasilkan dengan mengambil kira prinsip reka bentuk yang mesra pengguna dan estetik. Antara muka yang intuitif disediakan untuk memudahkan pengguna berinteraksi dengan aplikasi. Ini memastikan aplikasi mudah difahami dan digunakan oleh pengguna.

Fasa Pembangunan:

Pada fasa pembangunan dimana pembangunan sebenar aplikasi dijalankan. Ini termasuk pengaturcaraan dan integrasi komponen teknikal seperti tkinter, tkinterdnd2, Pillow (PIL), dan stegano. Setiap bahagian aplikasi diperiksa dengan teliti untuk memastikan pelaksanaan yang cekap dan tepat. Sistem pengendalian ralat juga ditubuhkan untuk menangani kesilapan yang mungkin terjadi semasa penggunaan aplikasi.

Fasa Pengujian:

Fasa pengujian memastikan bahawa aplikasi berfungsi seperti yang diharapkan. Ujian keselamatan data dijalankan untuk memastikan teks yang disembunyikan dalam imej tidak dapat dikesan oleh pihak yang tidak sah. Pengujian fungsi dilakukan ke atas semua ciri aplikasi termasuk pemilihan imej, penyembunyian data, pengambilan data, pengendalian ralat, dan fungsionaliti reset. Penglibatan pengguna akhir dalam pengujian aplikasi membantu mendapatkan maklum balas dan mengenalpasti isu pengguna untuk membuat penambahbaikan yang diperlukan.

Penyemakan Projek:

Fasa penyemakan projek melibatkan penilaian keseluruhan projek untuk memastikan ia mencapai matlamat dan objektif yang ditetapkan. Penyemakan projek melibatkan pengesahan bahawa semua aspek telah dilaksanakan dengan betul. Potensi penambahbaikan dan perluasan aplikasi dikenal pasti untuk kegunaan masa depan, memastikan aplikasi dapat berkembang dan bertambah baik dari masa ke masa.

Model Waterfall menekankan urutan linear di mana setiap fasa mesti diselesaikan sebelum bergerak ke fasa berikutnya. Ini memastikan bahawa projek dikendalikan dengan teratur dan sistematik, meminimumkan risiko dan memastikan setiap aspek dikaji dengan teliti sebelum fasa pembangunan dan pengujian. Metodologi Projek Zahiran - Sembunyi Pesanan Teks Rahsia menekankan kepentingan keselamatan data, kreativiti, dan reka bentuk antara muka pengguna yang mesra pengguna. Ia membolehkan pembangunan aplikasi yang cekap dan berkesan, memenuhi keperluan pengguna dengan baik.

REKA BENTUK ALGORITMA

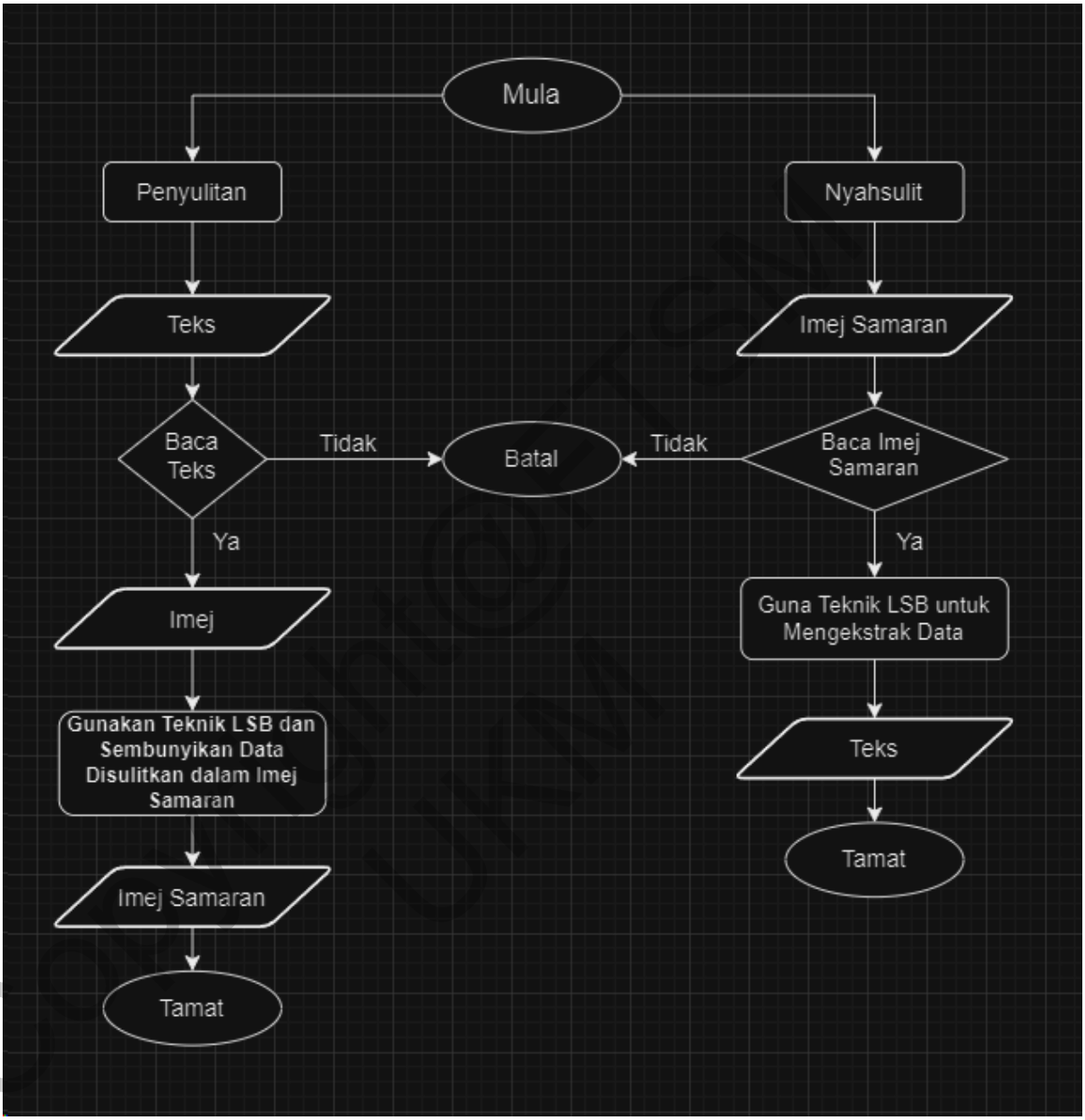
Reka bentuk algoritma menjadi teras penting dalam usaha menyusun langkah-langkah yang sistematik untuk melaksanakan teknik Least Significant Bit (LSB) dalam steganografi. Algoritma ini perlu dipelbagaikan untuk menyembunyikan dan mengeluarkan mesej tersembunyi dalam imej dengan berkesan. Pemikiran terperinci perlu diberikan kepada bagaimana setiap langkah dalam algoritma berinteraksi dengan antara muka pengguna, dan keseluruhan rekabentuknya harus memastikan kebolehgunaan yang tinggi dan kefahaman yang mudah oleh pengguna projek ini. Fokus kepada kecekapan pelaksanaan dan pengekalan keterbacaan kod juga merupakan faktor penting dalam reka bentuk algoritma untuk memastikan projek berfungsi dengan efisien dan dapat dikembangkan dengan mudah pada masa akan datang.

Contoh kod pseudo:

```
Function hide_message(image_path, message):
    Read the image from image_path
    Convert the message to binary representation
    Ensure the length of the binary message is less than or equal to the available LSBs in the image
    Iterate through each pixel in the image:
        For each color channel (e.g., R, G, B):
            Retrieve the binary representation of the current pixel channel
```

Replace the least significant bits with bits from the binary message

Save the modified image with the hidden message



Rajah 4.3: Carta Alir

Rajah 4.3 menunjukkan proses penyulitan (encryption) dan penyahsulitan (decryption) data menggunakan teknik penyembunyian data dalam imej samaran dengan teknik LSB (Least Significant Bit). Proses bermula dengan pilihan untuk penyulitan atau penyahsulitan. Jika memilih penyulitan, data teks akan dibaca. Jika teks berjaya dibaca, imej akan disediakan dan teknik LSB digunakan untuk menyembunyikan data dalam imej tersebut, menghasilkan imej samaran yang mengandungi data disulitkan. Proses ini diakhiri dengan penanda tamat.

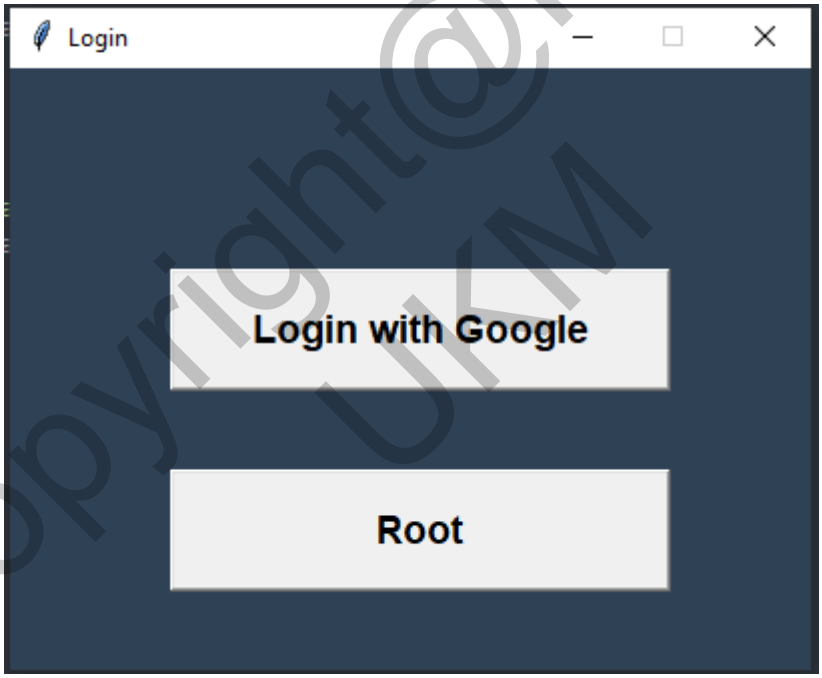
Sebaliknya, jika memilih penyahsulitan, imej samaran yang mengandungi data disulitkan akan dibaca. Jika imej samaran berjaya dibaca, teknik LSB digunakan untuk mengekstrak data dari imej tersebut, menukarnya kembali kepada bentuk teks asal. Proses ini juga diakhiri dengan penanda tamat. Jika dalam mana-mana langkah, teks atau imej samaran tidak dapat dibaca, proses akan dibatalkan.

Teknik LSB adalah teknik steganografi yang digunakan untuk menyembunyikan data dalam imej dengan mengubah bit paling kurang signifikan dalam setiap pixel imej. Teknik ini membolehkan data disembunyikan dengan cara yang sukar dikesan oleh mata kasar, menjadikan ia sesuai untuk tujuan penyulitan dan penyahsulitan data secara rahsia. Rajah ini memberi panduan jelas langkah demi langkah untuk proses penyulitan dan penyahsulitan data menggunakan imej samaran dan teknik LSB.

KEPUTUSAN DAN PERBINCANGAN

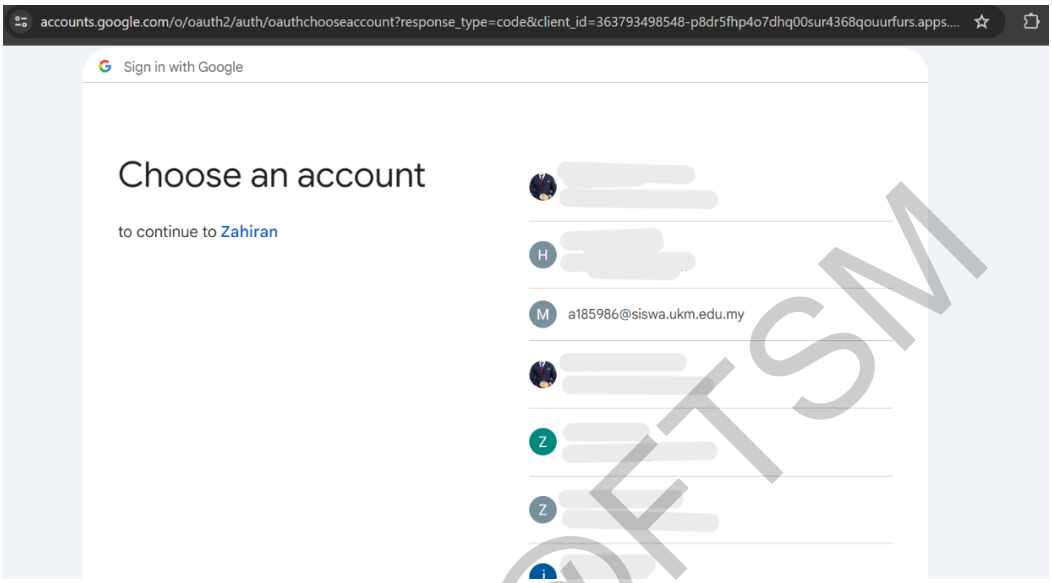
Aplikasi Zahiran – Sembunyi Pesanan Teks Rahsia telah berjaya dibangunkan dan semua dokumentasinya telah dilengkapkan. Semasa proses pembangunan, aplikasi ini dibangunkan menggunakan Python dan perpustakaan seperti tkinter dan stegano. Proses pembangunan melibatkan beberapa langkah utama seperti analisis keperluan, reka bentuk, pelaksanaan, pengujian, dan penyebaran. Proses menganalisis keperluan yang melibatkan memahami keperluan projek dan mendokumentasikan fungsi-fungsi yang diperlukan.

Apabila memasuki aplikasi, pengguna akan disambut dengan skrin Log Masuk yang memberikan pilihan sama ada log masuk melalui Google atau Root seperti mana yang di tunjukkan dalam Rajah 1.



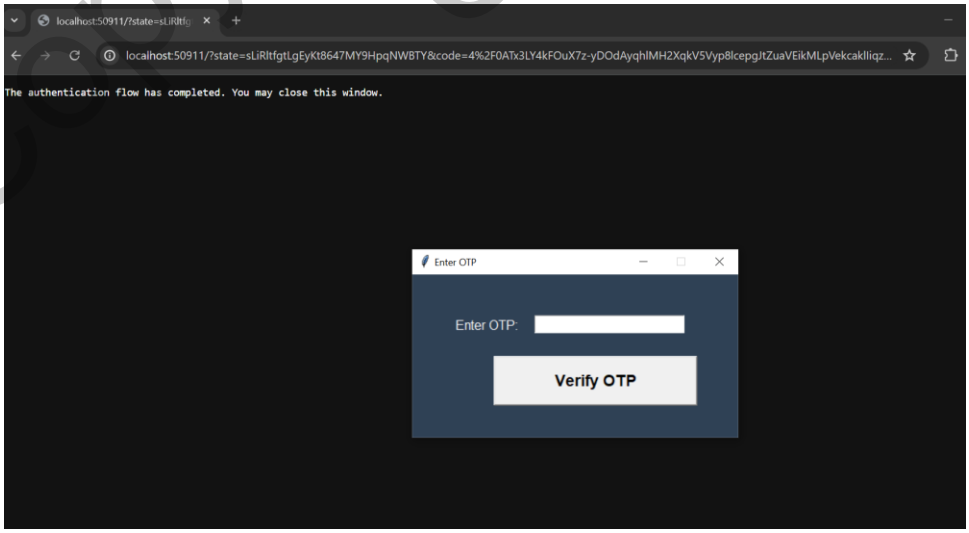
Rajah 1 Antara Muka Log Masuk

Apabila pengguna menekan butang “Login with Google”, mereka akan dipaparkan dengan muka utama google yang menwajibkan pengguna log masuk ke akaun Google terlebih dahulu seperti mana dipaparkan dalam Rajah 2.



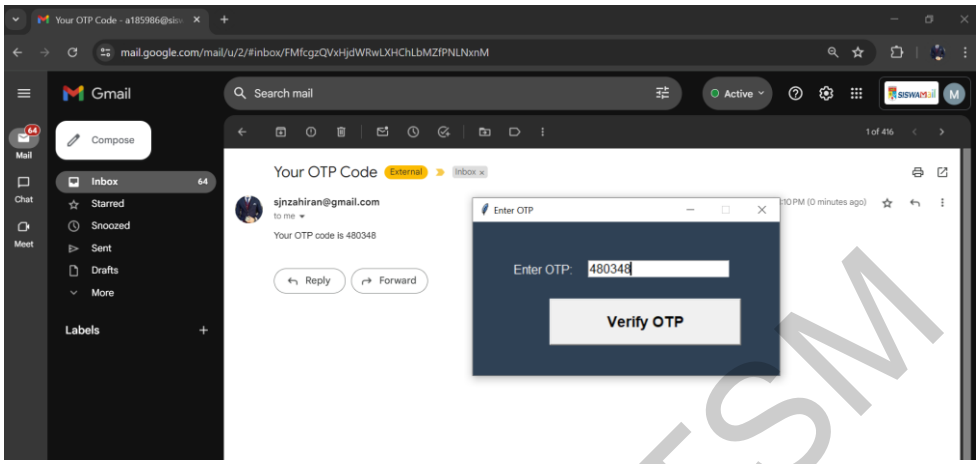
Rajah 2 Antara Muka Laman Utama Log Masuk Google

Setelah pengguna Berjaya log masuk melalui akaun google mereka, satu OTP kod akan dihantar kepada Alamat email mereke seperti mana dalam Rajah 3-5 yang menunjukkan antara muka halaman OTP bagi pengguna biasa untuk memasukkan OTP kod yang telah dihantar kepada Gmail pengguna. Rajah 3 dibawah menunjukkan kod OTP telah Berjaya dihantar ke pada akaun Google pengguna.



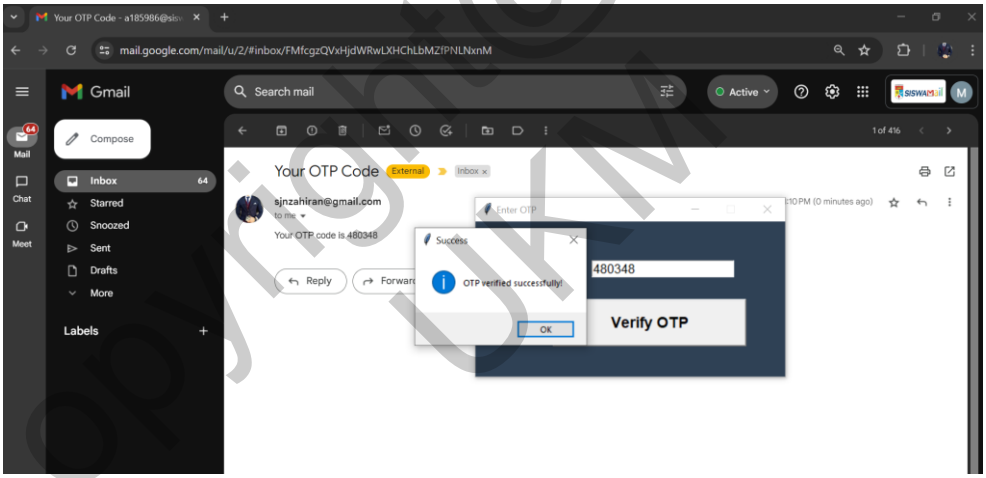
Rajah 3: Halaman OTP

Rajah 4 dibawah menunjukkan penerimaan berjaya kod OTP daripada applikasi kepada akaun Google.



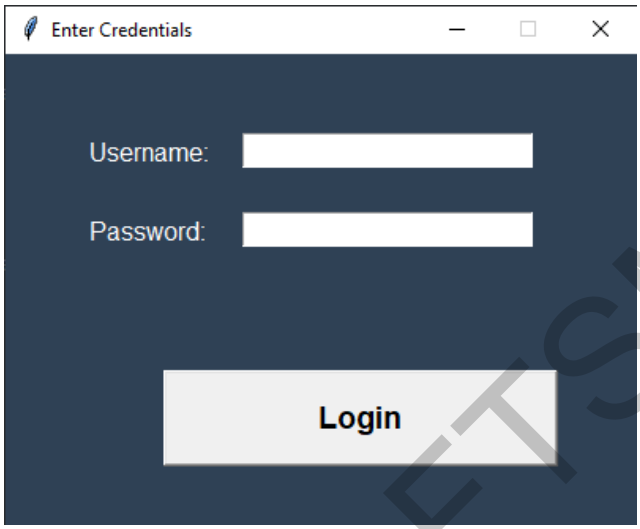
Rajah 4 : Halaman terima OTP

Rajah 5 menunjukkan kod OTP yang baru sahaja diterima oleh pengguna berjaya disahkan oleh aplikasi.



Rajah 5 : Halaman memasukkan OTP

Sekiranya pengguna menekan butang “Root” pada Rajah 1, pengguna akan dibawa ke muka depan log masuk “Root” seperti mana Rajah 6. Disini pengguna perlu memasukkan nama pengguna dan katalaluan yang sah sebelum menekan butang “Login”

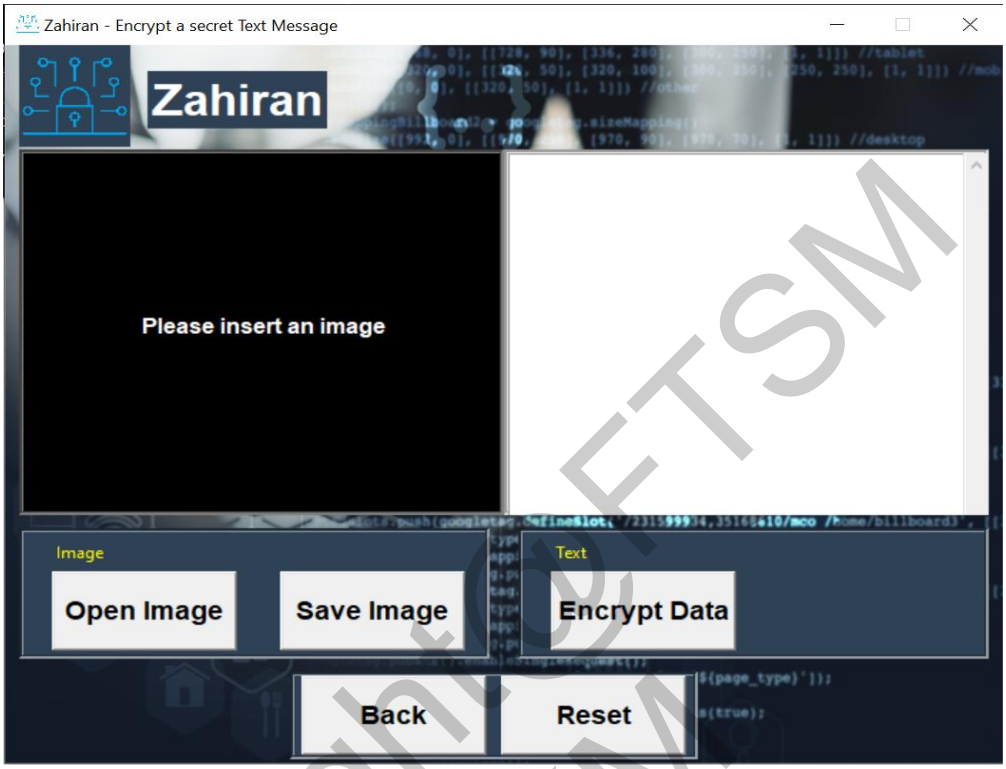


Rajah 6 Antara Muka Log masuk Root

Setelah pengguna Berjaya log masuk sama ada melalui Google atau Root, pengguna akan dibawa ke Halaman untama aplikasi yang menyediakan DUA butang iaitu “Encrypt” bagi tujuan penyulitan dan “Decrypt” bagi tujuan nyahsulit. Rajah 7 menunjukkan antara muka halaman utama bagi Aplikasi Zahiran – Sembunyi Teks Rahsia. Halaman Utama memaparkan logo dan nama aplikasi, dan butang untuk Penyulitan dan Nyahsulit.

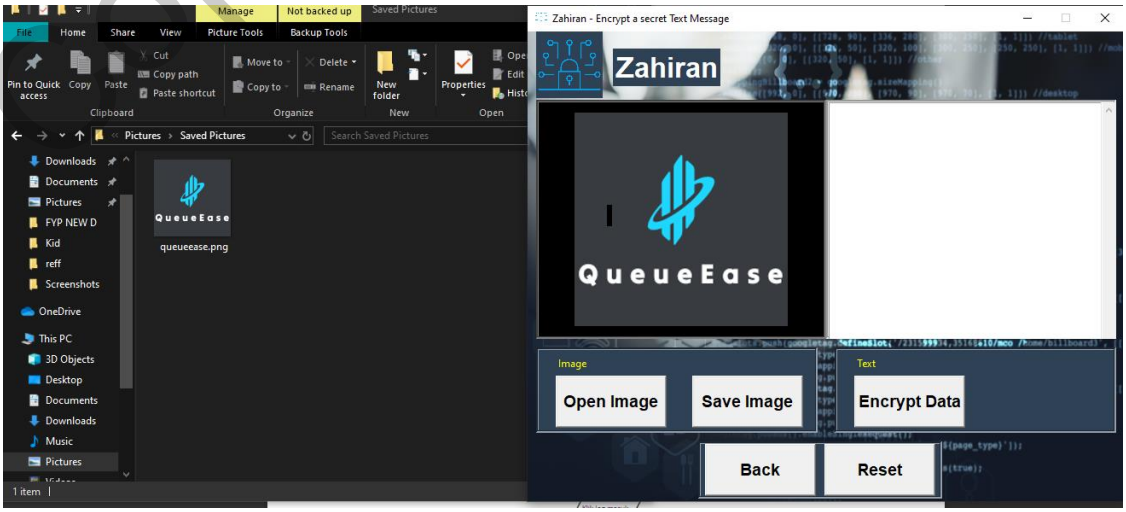
Rajah 7 : Halaman Utama Aplikasi

Rajah 8 menunjukkan antara muka halaman penyulitan bagi Aplikasi Zahiran – Sembunyi Teks Rahsia. Halaman Penyulitan memaparkan logo dan nama aplikasi, ruangan imej, ruangan teks, butang untuk memasukkan dan menyimpan imej, butang penyulitan serta butang kembali reset.



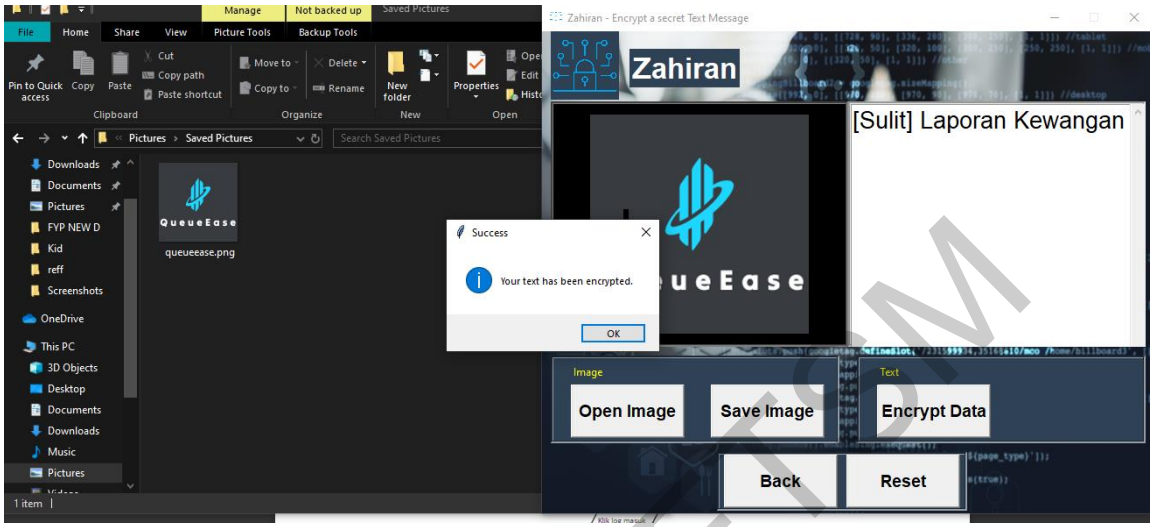
Rajah 8 : Halaman Penyulitan

Rajah 9 – 12 menunjukkan antara muka semasa pengguna memilih imej yang untuk disulitkan bersama teks. Pada Rajah 9 dibawah, pengguna telah memilih satu imej di dalam "File Explorer" mereka untuk disulitkan Bersama teks.



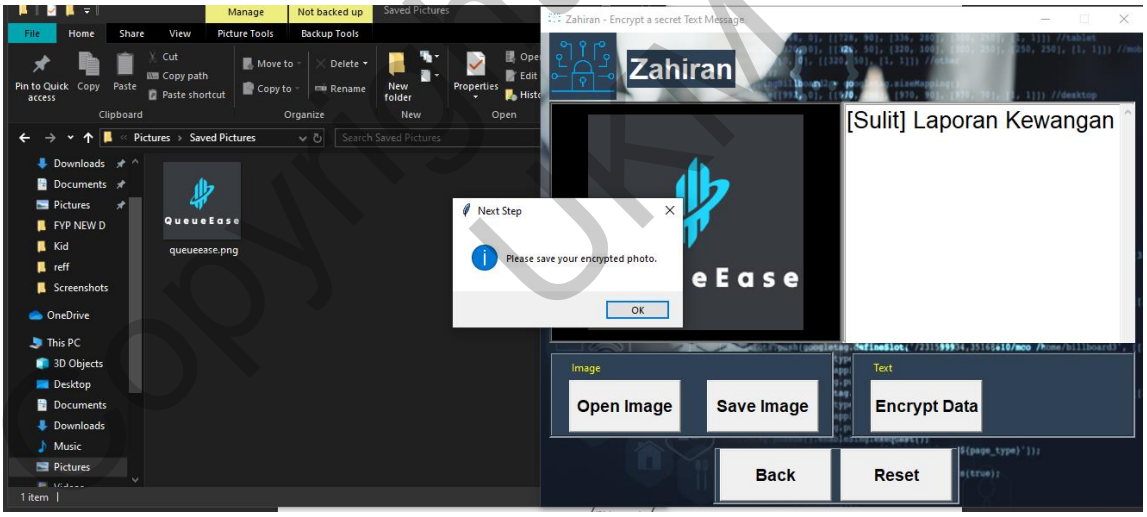
Rajah 9 : Halaman pemilihan imej untuk disulitkan

Pada Rajah 10 di bawah, pengguna telah Berjaya menyulitkan teks ke dalam imej yang telah di pilih pada Rajah 9.



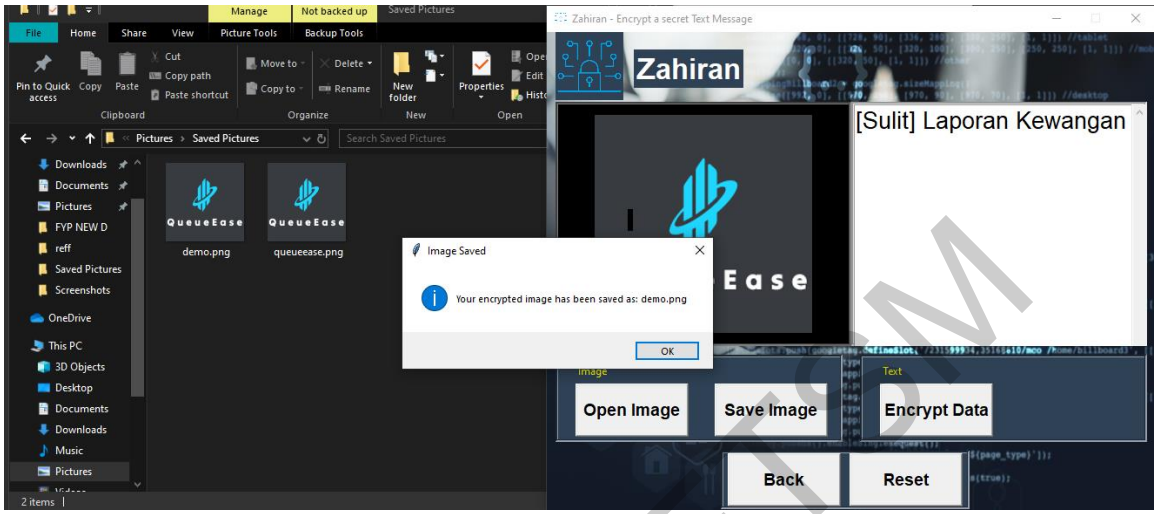
Rajah 10 : Halaman imej & teks berjaya disulitkan

Setelah pengguna menyulitkan imej dan teks tersebut, pengguna akan diminta untuk menyimpan imej Baharu yang telah disulitkan sepertimana ditunjukkan di dalam Rajah 11 di bawah.



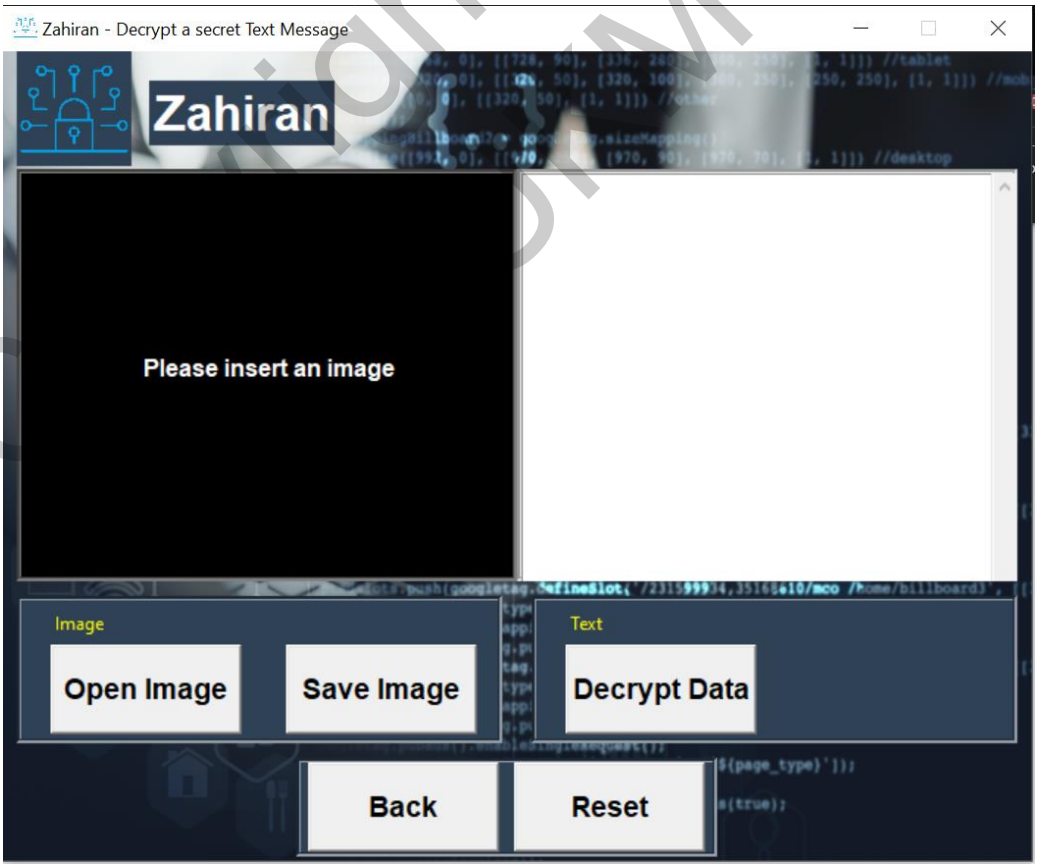
Rajah 11 : Halaman penyimpanan imej yang telah disulitkan

Rajah 12 di bawah menunjukkan pengguna berjaya menyimpan imej baharu yang telah disulitkan bersama teks dan menyimpannya sebagai “demo.png”.



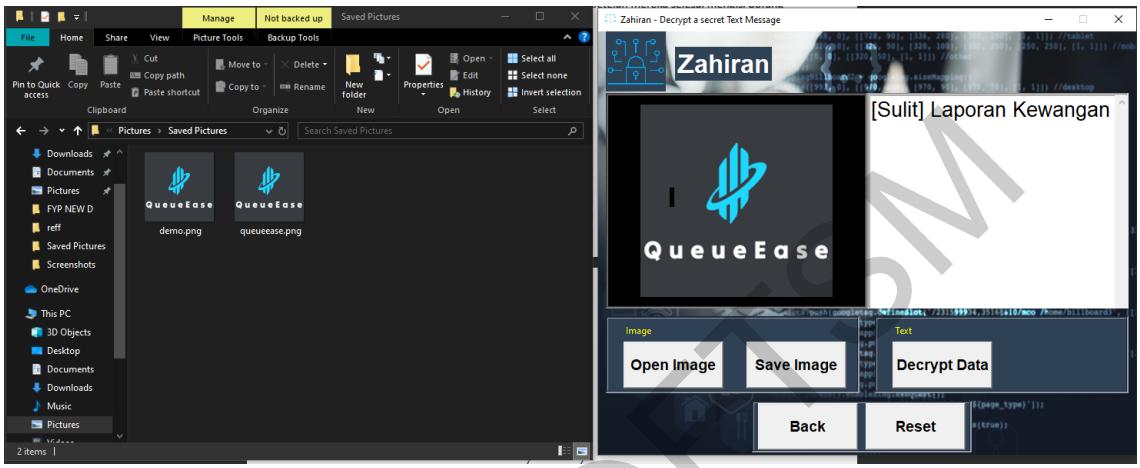
Rajah 12 : Halaman imej Berjaya disimpan

Rajah 13 menunjukkan antara muka halaman nyahsulit bagi Aplikasi Zahiran – Sembunyi Teks Rahsia. Halaman Nyahsulit memaparkan logo dan nama aplikasi, ruangan imej, ruangan teks, butang untuk memasukkan imej, butang nyahsulit serta butang kembali reset.



Rajah 13 : Halaman Nyahsulit

Rajah 14 menunjukkan antara muka apabila teks dimasukkan/dipaparkan bagi tujuan penyulitan/nyahsulit. Pengguna telah memasukkan fail imej “demo.png” dan kemudian menekan butang “Decrypt Data”. Sepertimana di tunjukkan di dalam rajah dibawah, teks yang telah disulitkan bersama imej pada awalnya berjaya di paparkan.



Rajah 14 : Halaman imej Berjaya dinyahsilutkan

Pengujian Kebolehgunaan

Pengujian aplikasi merupakan salah satu cara untuk menilai dan memastikan kelancaran penggunaan aplikasi serta memastikan bahawa perisian yang dibangunkan memenuhi ciri-ciri yang dirancang dalam pembangunan projek. Beberapa tahap pengujian, iaitu ujian komponen, ujian integrasi, dan ujian sistem, dilakukan untuk memastikan aplikasi sesuai digunakan oleh sasaran pengguna. Hasil tindak balas pengujian dikumpul dan dianalisis untuk mengenal pasti kekurangan atau kesalahan sistem, serta melakukan penambahbaikan pada aplikasi.

Pelaksanaan ujian aplikasi bermula apabila perancangan ujian telah selesai. Semua keputusan ujian direkodkan dan diperiksa dengan teliti. Ujian ini dilakukan berulangkali supaya tiada ralat berlaku pada aplikasi. Hasil pengujian menunjukkan bahwa aplikasi berfungsi sesuai dengan spesifikasi yang ditetapkan. Hasil sebenar yang diramalkan juga telah direkodkan dan berjaya dilakukan. Dibawah merupakan dapatan ujian kes guna bagi aplikasi Zahiran – Sembunyi Teks Rahsia.

ID Penguji	Hasil Jangkaan	Hasil Sebenar	Status Pengujian
T001	Pengguna Berjaya membuka applikasi	Pengguna Berjaya membuka applikasi dan antara muka halaman log masuk dipaparkan	Lulus
T002	Pengguna Berjaya log masuk melalui Google	Antara muka halaman log masuk melalui Google atau Root dipaparkan, Pengguna Berjaya dibawa kepada halaman utama akaun Google dan senarai akaun Google pengguna sedia ada terpapar	Lulus

T003	Pengguna Berjaya log masuk melalui nama pengguna dan katalaluan	Antara muka halaman log masuk melalui Google atau Root dipaparkan. Halaman nama pengguna dan katalaluan dipaparkan dan pengguna Berjaya memasukkan nama pengguna dan katalaluan. Antara muka halaman utama aplikasi dipaparkan.	Lulus
T004	Halaman Utama Bersama DUA butang “Encrypt” dan “Decrypt”	Antara muka halaman utama Bersama DUA butang “Encrypt” dan “Decrypt” terpapar dan logo dan nama aplikasi terpapar	Lulus
T005	Halaman Utama bagi aktiviti penyulitan dipaparkan	Antara muka halaman utama aktiviti penyulitan dipaparkan beserta logo aplikasi dan Butang “Open Image”, “Save Image”, “Encrypt Data”, “Back” dan Reset” terpapar dengan jelas.	Lulus

Jadual 1: Jadual Keputusan Pengujian

Berdasarkan jadual diatas, semua fungsi utama aplikasi diuji secara menyeluruh menggunakan teknik pengujian kotak putih dan hitam. Pengujian penerimaan pengguna menunjukkan bahwa aplikasi mudah digunakan dan memenuhi kebutuhan pengguna akhir. Tidak ada masalah yang tidak terduga yang ditemui selama pengujian.

Cadangan Penambahbaikan

Untuk penambahbaikan di masa hadapan, terdapat beberapa cadangan yang boleh diambil kira. Pertama, mengkaji dan mengimplementasikan teknik steganografi baru yang lebih canggih dan sesuai untuk pelbagai jenis data dan imej. Kedua, meningkatkan prestasi aplikasi dengan menstruktur semula atau meningkatkan algoritma yang digunakan untuk penyembunyian dan pengeluaran data. Ketiga, menjalankan kajian lebih mendalam mengenai keamanan aplikasi dan potensi risiko yang mungkin timbul, serta meningkatkan ketahanan aplikasi terhadap serangan luar. Keempat, meningkatkan antara muka pengguna untuk menjadikannya lebih mudah dan intuitif, serta menyediakan panduan penggunaan yang lebih komprehensif untuk pengguna tanpa latar belakang teknikal. Akhir sekali, menilai kepatuhan aplikasi terhadap undang-undang dan etika steganografi, serta mengenalpasti dan memperincikan halangan perundangan dan etika yang mungkin dihadapi oleh pengguna. Melalui penambahbaikan ini, aplikasi Zahiran - Sembunyi Pesanan Teks Rahsia dapat terus berkembang dan memberikan sumbangan yang lebih besar dalam bidang keselamatan maklumat dan steganografi.

KESIMPULAN

Secara kesimpulan Projek Zahiran - Sembunyi Pesanan Teks Rahsia bertujuan untuk membangunkan sebuah aplikasi yang membolehkan pengguna menyembunyikan mesej teks dalam imej menggunakan teknik steganografi Least Significant Bit (LSB). Projek ini direka untuk menyediakan antara muka pengguna yang intuitif dan mesra pengguna, membolehkan penyembunyian mesej dengan mudah tanpa menjejaskan kualiti imej asal. Aplikasi ini juga bertujuan meningkatkan keselamatan komunikasi dengan menggunakan kaedah penyulitan yang selamat. Dengan menggunakan bahasa pengaturcaraan Python serta perpustakaan tkinter dan stegano, aplikasi ini memberi sumbangan penting kepada bidang keselamatan maklumat dan steganografi. Ia bertujuan untuk menjadi panduan serta sumber pembelajaran bagi penyelidik dan pembangun yang berminat dalam bidang steganografi digital.

Kekuatan Sistem

Projek ini mempunyai beberapa kekuatan utama. Pertama, dari segi keselamatan data, aplikasi ini menggunakan teknik steganografi LSB yang kukuh untuk menyembunyikan mesej teks dalam imej, memastikan mesej tersebut tidak mudah dikesan oleh pihak yang tidak berkenaan. Kedua, teknik LSB yang digunakan memastikan kualiti visual imej yang disembunyikan kekal dalam tahap yang memuaskan, meminimumkan perubahan visual pada imej asal. Ketiga, antara muka pengguna yang direka dengan mesra pengguna membolehkan individu dengan latar belakang teknikal yang berbeza menggunakan aplikasi ini dengan mudah. Keempat, aplikasi ini direka untuk serasi dengan pelbagai platform, memastikan pengguna boleh mengakses dan menggunakan aplikasi ini pada pelbagai sistem operasi

Kelemahan Sistem

Terdapat beberapa kekangan yang perlu diambil kira. Pertama, aplikasi ini terhad kepada teknik steganografi LSB sahaja, yang mungkin tidak sesuai untuk semua jenis data atau imej. Kedua, projek ini perlu disiapkan dalam tempoh masa dan sumber yang terhad, yang boleh mempengaruhi kelengkapan dan kualiti hasil akhir. Ketiga, pengguna yang kurang mahir dalam teknikal mungkin menghadapi kesukaran dalam penggunaan aplikasi ini, terutamanya dalam konteks penyembunyian dan pengambilan data. Keempat, kekurangan sumber daya komputer atau prestasi yang rendah boleh mempengaruhi prestasi aplikasi ini. Selain itu, aplikasi ini terhad kepada platform yang menyokong bahasa Python dan perpustakaan khusus yang digunakan.

PENGHARGAAN

Penulis kajian ini ingin ucapkan sekalung penghargaan dan ucapan terima kasih saya ucapkan kepada penyelia projek saya, iaitu Ts. Dr. Nazhatul Hafizah di atas segala tunjuk ajar, nasihat, teguran dan dorongan serta bimbingan yang telah diberikan sepanjang proses penulisan dokumentasi Projek Zahiran– Sembunyi Pesanan Teks Rahsia. Kepakaran beliau dalam bidang teknologi sangat membantu saya menyiapkan dokumentasikan projek ini. Penghargaan ini juga dituju khas kepada semua pensyarah di Fakulti Teknologi dan Sains Maklumat (FTSM) yang telah memberi ilmu dan tunjuk ajar sepanjang pengajian saya di FTSM. Akhir sekali, ucapan terima kasih yang tidak terhingga diucapkan kepada keluarga dan teman seperjuangan saya serta sesiapa sahaja yang telah memberi semangat dan bantuan sepanjang proses penulisan dokumentasi projek tahun akhir ini dilaksanakan. Segala jasa baik kalian tidak akan di lupakan

RUJUKAN

G. J. Simmons, “The Prisoners’ Problem and the Subliminal Channel,” in Advances in Cryptology: Proceedings of CRYPTO ’83, springer, 1983, pp. 51–67.

L. Zhang, J. Wu, and N. Zhou, “Image Encryption with Discrete Fractional Cosine Transform and Chaos †,” in Proceeding of Fifth International Conference on Information Assurance and Security, 2009, pp. 61–64.

A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, “Digital image steganography: Survey and analysis of current methods,” Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.

E. E. A. Elgabar and H. A. A. Alamin, “Comparison of LSB Steganography in GIF and BMP Images,” International Journal of Soft Computing and Engineering (IJSCE), vol. 3, no. 4, pp. 79–83, 2013.

M. S. Subhedar and V. H. Mankar, “Current status and key issues in image steganography: A survey,” Computer Science Review, vol. 13–14, pp. 95–113, 2014.

D. Salomon, Coding For Data And Computer Communications. California State University: Springer, 2005.

N. F. Johnson and S. Jajodia, “Exploring Steganography: Seeing the Unseen,” Computer, vol. 31, no. 2, 1998.

M. Mishra and F. L. D. M. C. Adhikary, “An Easy yet Effective Method for Detecting Spatial Domain LSB Steganography,” International Journal of Computer Science and Business Informatics, vol. 8, no. 1, pp. 1–12, 2013.

G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, “Watermarking Digital Image and Video Data A state-of-the-art overview,” IEEE Signal Processing Magazine, vol. 17, no. 5, pp. 20–46, 2000.

S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding techniques for stegnography and digital watermarking. Artech House, Inc. Norwood, MA, USA, 2000.

P. C. Mandal, “Modern Steganographic technique : A survey,” International Journal of Computer Science & Engineering Technology (IJCSET), vol. 3, no. 9, pp. 444–448, 2012.

C. Kurak and J. McHugh, “A Cautionary Note On Image Downgrading,” in Proceeding of Computer Security Applications Conference, Eighth Annual, 1992, pp. 153–159.

F. Petitcolas, “The information hiding homepage.” [Online]. Available: http://www.petitcolas.net/steganography/image_do wngrading/.

Rouse, M. (2001). Steganography. TechTarget. [Dalam talian] https://searchsecurity.techtarget.com/definition/steganography

Tkinter: The standard Python interface to the Tk GUI toolkit. (2023). Python Software Foundation. [Dalam talian] https://docs.python.org/3/library/tkinter.html

TkinterDnD2. (2022). GitHub Repository. [Dalam talian] https://github.com/pmgagne/tkinterdnd2

The Python Imaging Library Handbook. (2007). Fredrik Lundh. [Dalam talian] https://effbot.org/imagingbook/

LSB Image Steganography. (2023). GitHub Repository. [Dalam talian] https://github.com/ragibson/LSB-Steganography

Dokumentasi Google OAuth 2.0: Google OAuth 2.0 https://developers.google.com/identity/protocols/oauth2/javascript-implicit-flow#:~:text=OAuth%202.0%20allows%20users%20to,called%20the%20implicit%20grant%20flow.

Dokumentasi Tkinter: Tkinter https://docs.python.org/id/3.6/library/tk.html

Dokumentasi PIL (Pillow): Pillow https://pillow.readthedocs.io/en/stable/

Dokumentasi Perpustakaan Stegano: Stegano https://stegano.readthedocs.io/en/latest/

Dokumentasi Perpustakaan SMTP Python: smtplib https://docs.python.org/3/library/smtplib.html

https://support.smartbear.com/readyapi/docs/functional/steps/index.html

https://www.geeksforgeeks.org/software-testing-life-cycle-stlc/

https://www.guru99.com/software-testing-life-cycle.html

https://www.theknowledgeacademy.com/blog/software-testing-life-cycle/

https://support.smartbear.com/readyapi/docs/functional/steps/index.html

https://www.geeksforgeeks.org/software-testing-life-cycle-stlc/

https://www.guru99.com/software-testing-life-cycle.html

Mohamad Zahiran Bin Zahari (A185986)
Ts. Dr. Nazhatul Hafizah Kamarudin
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia