BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Teknologi penyembunyian informasi (*information hiding*) adalah teknologi yang menjadi solusi untuk dapat mengamankan konten multimedia yang memiliki nilai jual tinggi. Salah satu jenis dari teknologi adalah steganografi, suatu teknik seni mengirimkan pesan atau informasi rahasia dalam suatu konten multimedia ke tujuan [1]. Dengan menggunakan teknik steganografi, pesan rahasia dapat dikirimkan kepada orang yang berhak menerima tanpa diketahui oleh publik.

Steganografi memiliki tujuan utama untuk menyisipkan pesan rahasia pada media (citra, audio, video dan pesan) yang memiliki kinerja, antara lain memberikan kualitas/imperseptibilitas/invisibilitas yang tinggi pada citra/audio-stego, menyediakan kapasitas yang besar pada pesan rahasia yang disisipkan pada media penampung, dan mampu mempertahankan informasi rahasia dari berbagai serangan.

Steganografi saat telah mengalami banyak perkembangan. Variasi metode yang dilakukan untuk meningkatkan kemampuan kerja penyembunyian informasi menghasilkan kemajuan yang cukup signifikan pada dunia penelitian. Beberapa tahun terakhir, steganografi mulai dikembangkan bersama dengan teknologi kuantum. Teknologi kuantum adalah teknologi yang mampu memberikan kecepatan sinyal dan kapasitas kanal yang tinggi. Pada tahun 2019, Google mengklaim teknologi kuantum dapat melakukan tugas/komputasi dalam 200 detik. Sementara pada teknologi klasikal, tugas/komputasi yang sama membutuhkan waktu 10.000 tahun [2]. Hal menjadikan teknologi kuantum sebagai teknologi yang harus dikuasai agar bisa mengantisipasi kemungkinan serangan baru menggunakan teknologi kuantum di masa depan.

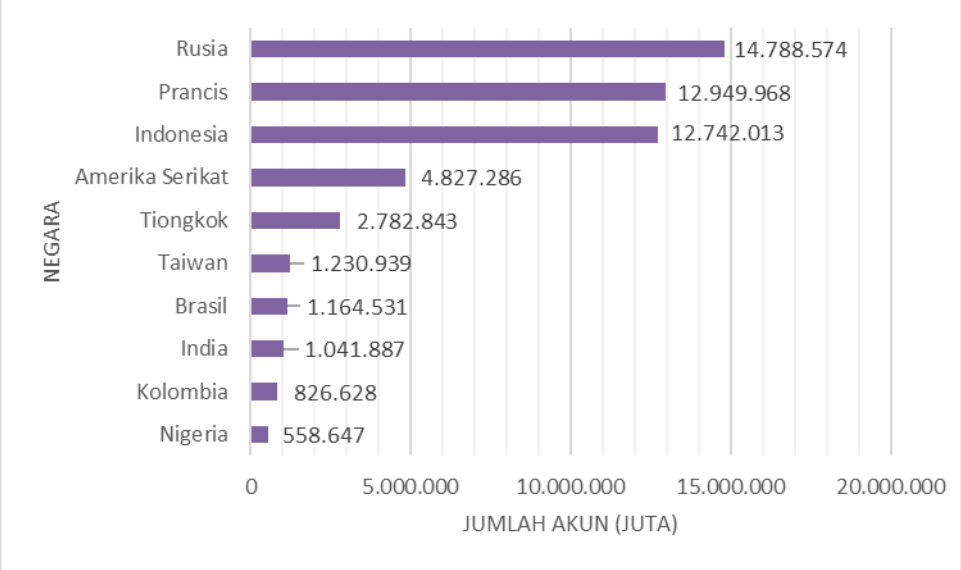
Rentannya keamanan konten multimedia disertai rendahnya pengetahuan masyarakat tentang teknologi steganografi menjadikan salah satu alasan utama masih tingginya angka pencurian data di Indonesia. Selain itu, kurangnya media demonstrasi steganografi kuantum yang mudah diakses dan dipahami merupakan salah satu hambatan besar untuk menguasai bidang steganografi dan kuantum. Memanfaatkan kemudahan akses internet, pengadaan aplikasi atau *website* yang dapat dijangkau oleh semua kalangan diperlukan agar masyarakat bisa mendapatkan pemahaman tentang teknologi steganografi mulai dari cara kerja sistem hingga metode-metode/algoritma yang digunakan. Media demonstrasi seperti aplikasi dan *website* diharapkan lebih menarik minat masyarakat untuk mempelajari teknologi steganografi.

Teknologi kuantum menawarkan banyak kelebihan yang luar biasa. Salah satunya adalah meningkatkan kapasitas data rahasia yang disembunyikan, meningkatkan kualitas citra *host* dari konten multimedia dan meningkatkan ketahanan data rahasia yang disembunyikan terhadap berbagai serangan. Namun, teknologi kuantum merupakan teknologi yang dianggap abstrak dan sulit oleh sebagian besar masyarakat sehingga masih sedikit masyarakat yang memahami teknologi kuantum. Padahal dengan memahami teknologi kuantum terutama kaitannya dengan steganografi maka membuat masyarakat semakin peduli terhadap keamanan data dengan lebih dalam secara teknis dengan berbagai kelebihan teknologi kuantum diatas.

1.2 Informasi Pendukung

Pesatnya perkembangan teknologi digital telah membawa tantangan besar bagi keamanan dalam distribusi konten. Selain itu, kemudahan akses ke dunia digital meningkatkan kasus pencurian informasi tanpa sepengetahuan atau seizin pemiliknya.

Gambar 1.1 menunjukkan data yang dikumpulkan oleh *Surfshark*. Berdasarkan data tersebut, Indonesia berada di posisi tiga negara dengan jumlah kasus kebocoran data terbanyak di dunia. Sebanyak 12.742.013 akun berhasil dicuri [3]. Data pribadi yang seharusnya disimpan dan dilindungi dengan baik, justru diperjual belikan dengan bebas oleh beberapa pelaku kejahatan. Variasi data yang umumnya diambil berupa nama, tanggal lahir, email, alamat, nomor telepon hingga Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK) dan Kartu Tanda Penduduk Elektronik (E-KTP) [4].



Gambar 1.1 Jumlah kasus kebocoran data terbanyak di dunia 2022.

Untuk menangani hal tersebut, dibutuhkan teknologi yang mampu mengamankan konten multimedia dan dapat mengirimkan pesan atau informasi rahasia di dalamnya**.** Beberapa metode *watermarking* telah dilakukan oleh peneliti terdahulu untuk mendapatkan solusi dari permasalahan diatas, namun beberapa penelitian masih memerlukan studi lebih lanjut untuk menyempurnakan metode yang sudah ada.

Pada Paper yang dipublikasi oleh X.Liu dan X.Tang tahun 2020 dengan menggunakan metode *digital signature* yang dikombinasikan dengan metode DCT dan DWT dapat melindungi konten asli dari pembajakan, tetapi metode tersebut tidak kuat terhadap beberapa transformasi yang dapat merusak *watermarking* sehingga tidak dapat diekstraksi. Untuk mengatasi masalah adalah dengan menggunakan *QR Code*. *QR Code* memiliki keuntungan karena dapat menyimpan informasi dalam jumlah besar, sangat andal, sangat aman, dan mampu mencegah pemalsuan, semuanya hanya dalam kode satu dimensi. Dengan menggunakan *QR Code* pada *digital watermarking*, ketahanannya bisa ditingkatkan secara signifikan. Cara kerja dari *QR Code watermarking* adalah dengan cara mengubah watermark menjadi bentuk *QR Code* sebelum dimasukan ke dalam gambar. Pada penelitian sebelumnya juga menunjukkan bahwa metode tahan terhadap beberapa serangan seperti rotasi, *scaling*, dan kompresi JPEG. Namun masih terdapat kekurangan pada metode , yaitu saat citra mengalami perubahan masih ada sub-blok dari *watermarking* yang tidak terbaca dikarenakan nilai *Hamming Distance* lebih dari 5 [5].

Pada tahun yang sama Tan dkk tahun mengusulkan skema XOR-ed VSS (XVSS) (k, n)-*threshold* berdasarkan *QR Code* dengan kemampuan *error correction*. Dibandingkan dengan OR-ed VSS (OVSS), XVSS dapat memulihkan gambar rahasia tanpa merusaknya, dan jumlah komputasi yang dibutuhkan rendah. Lebih penting lagi, jika beberapa serangan gambar konvensional, termasuk rotasi, kompresi JPEG, *error Gaussian, salt and pepper error, croping*, pengubahan ukuran, gambar rahasia masih dapat dipulihkan. Hasil penelitian menunjukkan bahwa citra yang telah disisipi informasi rahasia dengan metode di atas bisa tahan terhadap serangan yang ditunjukjkan dengan beberapa parameter seperti 1) JPEG *Compression*, nilai Q memiliki rentang antara 10 - 90 menunjukkan bahwa pesan rahasia masih bisa direkonstruksi, 2) *Salt and pepper error* memiliki rentang nilai 10% - 60% menunjukkan bahwa pesan rahasia masih bisa direkonstruksi, 3) *Rotation* memiliki rentang nilai 15º - 90º menunjukkan bahwa pesan rahasia masih bisa direkonstruksi [6].

Pada paper yang dipublikasi oleh Tudorache, A.-G.; Manta, V.; Caraiman, S yang memperkenalkan sebuah protokol kuantum B92 yang dapat digunakan untuk mengirimkan pesan rahasia yang disisipi pada gambar *grayscale*. Dengan bantuan server, algoritma mengeluarkan pesan secara random yang bisa bertindak sebagai kunci rahasia untuk algoritma kriptografi yang bisa mengamankan data yang dikirim oleh kedua belah pihak. Representasi gambar yang digunakan adalah NEQR dan *platform* pengujian yang digunakan adalah IBM Quantum Experience, dan *open-source library* Python Qiskit. Pada paper peneliti mendeskripsikan bagaimana gambar *grayscale* bisa disisipkan pesan rahasia untuk dikirim dengan menggunakan protokol B92. Metode juga membutuhkan server untuk bisa menghubungkan antara pengirim dan penerima dengan aman [7].

Zhou dkk pada tahun 2019 berhasil memberikan performa steganografi yang baik dalam domain kuantum. Metode kuantum *Haar Wavelet* yang diusulkan, diaplikasikan pada proses penguraian model representasi FRQI dan pengembangan dua skema *embedding* (penyisipan) baru, yaitu algoritma *non-block* dan *block*. Mekanismenya, *watermark image* yang telah diproses melalui skema algoritma *non-block* dan *block*, disisipkan ke daerah *diagonal subband* pada *carrier image*. Hasil simulasi menunjukkan PSNR bernilai antara 54.08 dB – 71.3 dB, kapasitas/*payload* sebesar ¼ bpp dan BER berkisar antara 0.014 – 0.019. Karena mmnya ketersediaan komputer kuantum, metode yang diusung oleh Zhou dkk tidak dapat memberikan analisa citra stego apabila diserang dengan berbagai macam serangan keamanan [8].

Pada tahun berikutnya, Ghai dkk (2020) mengusulkan teknik *watermarking* gambar digital menggunakan beberapa metode gabungan untuk mencegah berbagai serangan keamanan dengan tetap mempertahankan informasi rahasia yang disisipkan. Metode pertama dengan menghitung koefisien transformasi pada *cover image* menggunakan *dual-tree complex wavelet transform*, kemudian mengacak gambar *watermark* menggunakan *Arnold transform*, dan terakhir menyisipkan gambar *watermark* pada koefisien rendah di *cover image* menggunakan *quantum-based singular value decomposition* (SVD). Hasil penelitian menunjukkan bahwa metode yang diusulkan berhasil mengurangi dampak kerusakan secara signifikan pada *watermark* dan *cover image*. Hal dapat dilihat dari nilai PSNR yang berkisar antara 73.02 dB – 78.08 dB [9].

Selanjutnya paper yang dipublikasi oleh S. Miyake dan K. Nakame peneliti mengusulkan sebuah metode baru, yaitu kuantum *watermarking* menggunakan kuantum sirkuit. Citra yang digunakan merupakan citra *grayscale* dengan NEQR untuk merepresentasikan citra kuantum. Ukuran dari citra *host* dan *watermark* diasumsikan $2n \times 2n$ dan $n \times n$. Pada tahap pertama

watermark klasik dengan ukuran n x n 8 bits *grayscale* di *expand* menjadi 2n × 2n 2 bits *gray-scale*. Selanjutnya citra yang sudah di *expand* di acak menjadi sebuah citra *random* dengan menggunakan *SWAP gate* yang di kontrol oleh sebuah *key* yang hanya diketahui oleh operator. Watermark tersebut lalu dimasukkan ke dalam citra *host* menggunakan *CNOT gate* (*XOR operation*). Hasil penelitian menunjukkan bahwa citra *host* yang telah disisipi watermark memiliki performa yang cukup baik dari sisi *robustness, performance under error,* dan *visual quality* dengan nilai PSNR > 40 dB [10].

Tugas Akhir mengusulkan tiga metode steganografi berbasis kuantum, yaitu 1) *QHWT-SS,* 2) *QDCT-SS*, 3) *Quantum Spread Spectrum.* Ketiga metode steganografi diimplementasikan dalam bentuk aplikasi dan website. Diharapkan dengan adanya media demonstrasi secara gratis , masyarakat lebih sadar pentingnya pengamanan data pribadi.

1.3 Analisis Umum

1.3.1 Aspek Ekonomi

Menyediakan media demonstrasi kuantum sederhana untuk masyarakat agar semakin sadar pentingnya mempelajari teknologi kuantum dan steganografi. Materi pembelajaran disediakan dalam bentuk aplikasi dan website yang menjelaskan seputar steganografi maupun teknologi kuantum secara gratis sehingga meminimalisir biaya untuk mengedukasi masyarakat mengenai teknologi steganografi dalam domain kuantum.

1.3.2 Aspek Keamanan *(Security)*

Steganografi dengan teknologi kuantum membantu mengamankan pesan yang dikirim oleh seseorang karena pesan tersebut hanya bisa dilihat oleh pengirim dan penerima yang bersangkutan dan pesan dikirim menggunakan protokol tertentu dalam domain kuantum.

1.4 Kebutuhan yang Harus Dipenuhi

Berdasarkan analisis yang dilakukan, ditemukan beberapa persyaratan penting yang harus dipenuhi guna meningkatkan kesadaran masyarakat mengenai pentingnya teknologi kuantum dan steganografi. Untuk mencapai hal tersebut, diperlukan sistem yang mampu memfasilitasi pembelajaran dengan baik. Sistem tersebut harus bersifat menarik, mudah digunakan, mudah dimengerti, dan menjamin keamanan data. Dengan adanya sistem yang memenuhi persyaratan, diharapkan masyarakat dapat dengan mudah dan efektif belajar serta memahami konsep teknologi kuantum dan steganografi.

1.5 Solusi Sistem yang Diusulkan

Tugas Akhir ini mempertimbangkan dua alternatif solusi utama, yaitu implementasi steganografi citra pada aplikasi mobile dan implementasi steganografi citra pada *website*. Meskipun dalam penelitian lebih optimal jika fokus mengimplemetasikan salah satu sistem diatas, namun kedua platform tersebut menawarkan keuntungan yang berbeda dan relevan dalam konteks steganografi.

1.5.1 Karakteristik Produk

1.5.1.1 Aplikasi Berbasis Android

Aplikasi berbasis android yang memiliki halaman utama, yaitu *Embedding* dan *Extraction*. Halaman *Embedding* berfungsi untuk menyisipkan pesan rahasia ke dalam citra digital berwarna. Pesan rahasia berbentuk citra serta dilengkapi *key* agar menambah rasa aman bagi pengguna. Lalu, halaman *Extraction* berfungsi untuk mengekstraksi *file.mat* agar pengguna dapat melihat citra rahasia. Halaman *Extraction* mengharuskan pengguna mengetahui *key* dari *file.mat* yang ingin ekstraksi. Selain itu, terdapat halaman tambahan berupa halaman *Learn* dan *Result*. Halaman *Learn* berfungsi untuk memberikan wawasan serta pengetahuan sederhana mengenai steganografi, teknologi kuantum, serta steganografi kuantum dalam bentuk narasi dan gambar yang menarik. Sedangkan, halaman *Result* berfungsi untuk menampilkan hasil halaman *Embedding* dan *Extraction*. Hasil kedua halaman tersebut dapat diunduh pengguna.

1.5.1.2 Website

Sistem diimplementasikan dalam bentuk *website* yang memiliki halaman hampir serupa dengan solusi sistem pertama (aplikasi). Terdapat perbedaan dalam hal aksesibilitas dan kebutuhan akun pengguna. Pengguna dapat mengakses halaman *Learn* tanpa memerlukan akun. *Website* tidak memerlukan proses pengunduhan atau instalasi, sehingga dapat diakses secara langsung melalui berbagai perangkat gadget yang mendukung akses internet.

1.5.2 Skenario Penggunaan

1.5.2.1 Aplikasi

Skenario penggunaan aplikasi berbasis android sebagai berikut:

1. Pengguna mengunduh aplikasi.
2. Pengguna membuat akun untuk mengakses aplikasi.
3. Pengguna dapat mengakses aplikasi menggunakan akun yang sudah dibuat.
4. Pengguna dapat membaca materi mengenai steganografi, komputasi kuantum, dan steganografi kuantum pada halaman *Learn.*

5. Pengguna dapat menggunakan halaman *Embedding* dengan memilih metode penyisipan, citra *host*, citra rahasia, dan *key*. Jika sudah memasukan data-data yang dibutuhkan untuk halaman *Embedding*, pengguna dapat menekan tombol *embedding* untuk melihat hasil penyisipan citra. Hasil dari halaman *Embedding* tersedia di halaman *Results*.
6. Pengguna dapat mencoba halaman *Extraction* memasukan metode ekstraksi citra, *file.mat* beserta *key*. Jika sudah memasukan data-data yang dibutuhkan untuk halaman *Extraction*, pengguna dapat menekan tombol *extraction* untuk melihat hasil ekstraksi citra. Hasil dari halaman *Extraction* tersedia di halaman *Results*.
7. Pengguna dapat melihat hasil *Embedding* dan *Extraction* dengan membuka halaman *Results*. Hasil *Embedding* dan *Extraction* dapat diunduh pengguna.

1.5.2.2 Website

Sistem diimplementasikan dalam bentuk *website* yang memiliki skenario penggunaan hampir serupa dengan solusi sistem pertama (aplikasi). Namun, pengguna tidak memerlukan akun untuk mengakses halaman *Learn.*

1.6 Kesimpulan dan Ringkasan CD-1

Perkembangan teknologi mempermudah manusia dalam memperoleh informasi. Namun kemudahan justru menimbulkan permasalahan baru, yaitu keamanan pada informasi digital yang tersebar di internet. Hal dibuktikan dengan data yang dikumpulkan oleh *Surfshark*. Berdasarkan data tersebut, Indonesia berada di posisi tiga negara dengan jumlah kasus kebocoran data terbanyak di dunia. Hal tentu sangat meresahkan karena data-data yang bocor adalah data penting seperti E-KTP yang merupakan kartu identitas dan jika jatuh ke orang yang tidak bertanggung jawab bisa dijadikan alat untuk tindakan kriminal. Maka dari itu penulis mengusulkan solusi sistem berupa aplikasi dan *website* yang bisa melakukan *embedding* dan ekstraksi data rahasia, serta dilengkapi dengan materi pembelajaran guna mengedukasi masyarakat mengenai steganografi dan teknologi kuantum.