

Watermarking

Watermarking adalah proses menyisipkan informasi rahasia ke dalam suatu objek digital, seperti gambar, audio, atau video, untuk melindungi hak cipta, mengidentifikasi kepemilikan, atau memberikan tanda autentikasi. Tujuan utama dari watermarking adalah untuk memberikan perlindungan terhadap pemalsuan, manipulasi, atau penyalinan ilegal objek digital tersebut.

Ada dua jenis utama dalam *watermarking*, yaitu *visible watermarking* dan *invisible watermarking*. *Visible watermarking* biasanya berupa teks, logo, atau simbol yang dapat terlihat secara jelas pada objek digital. Tujuannya adalah untuk memberikan informasi tentang kepemilikan atau hak cipta objek tersebut. *Invisible watermarking* memiliki teknik yang lebih kompleks untuk menyisipkan data ke dalam objek digital tanpa mengubah penampilan visualnya secara signifikan. *Invisible watermarking* lebih banyak digunakan dalam keperluan forensik digital atau perlindungan terhadap manipulasi. Pada *watermarking* terdapat beberapa proses utama yang perlu diperhatikan seperti *embedding*, *attacking* dan ekstraksi. *Embedding* adalah proses menyisipkan suatu objek atau informasi ke dalam objek lainnya, sementara *attacking* adalah usaha perusakan *watermark* yang disisipkan untuk mengetahui ketahanan dari sistem *watermarking* yang telah dibuat. Ekstraksi merupakan proses pemisahan kembali file *watermark* dengan file host.

Proses Kuantum

Pada komputasi kuantum, informasi dalam bentuk bit akan diubah dan disimpan dalam bentuk bit kuantum atau biasa disebut *qubit*. Berbeda dengan bit klasik, bit kuantum dapat berada pada keadaan *superposisi*. Persamaan berikut adalah representasi dari $|0\rangle$ dan $|1\rangle$.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ dan } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Persamaan dibawah adalah rumus superposisi untuk $|0\rangle$ dan $|1\rangle$ dimana α dan β adalah bilangan kompleks, $|\alpha|^2 + |\beta|^2 = 1$

$$|\psi\rangle = |\alpha|^2 + |\beta|^2$$

Quantum Representation of Digital Audio

Quantum Representation of Digital Audio (QRDA) menyimpan amplitudo dan informasi waktu dari audio dengan menggunakan dua urutan qubit yang saling berkaitan (terjerat). Kedua deret qubit berada dalam keadaan dasar $|0\rangle$ dan $|1\rangle$. Bentuk representasi sinyal audio dalam QRDA berupa sinyal audio digital $A = [a_0, a_1, a_2, \dots, a_{i-1}]$, dimana i adalah panjang audio dan $a_i \in \{-2^{q-1}, \dots, -1, 0, 1, 2^{q-1}-1\}$, setelah itu sinyal audio harus diubah ke dalam bentuk bilangan bulat positif $a_i \in \{-2^{q-1}, \dots, -1, 0, 1, 2^{q-1}-1\} + 2^{q-1}$. Perubahan ini tidak akan mengubah bentuk gelombang. Secara matematis QRDA dapat dituliskan sebagai berikut:

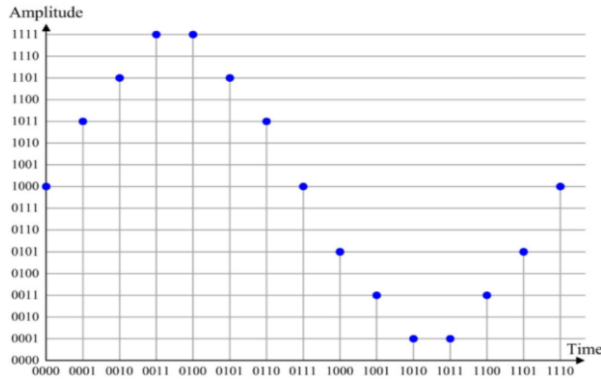
$$|A\rangle = \frac{1}{\sqrt{2^L}} \sum_{T=0}^{i-1} |D_T\rangle \otimes |T\rangle$$

$$|T\rangle = |t_0 t_1 \dots t_{i-1}\rangle, t_i \in \{0, 1\}$$

$$|D_T\rangle = |D_T^0 D_T^1 \dots D_T^{q-2} D_T^{q-1}\rangle, D_T^i \in \{0, 1\},$$

$$L = \begin{cases} \lceil \log_2 L \rceil, & i > 1 \\ 1, & i = 1 \end{cases}$$

Dimana $|D_T\rangle$ adalah nilai amplitudo dan $|T\rangle$ adalah informasi waktu yang mengikat setiap nilai biner amplitudo. Gambar 1 merupakan ilustrasi dari audio sinyal dengan 15 sampel dan ekspresi representatifnya dalam bentuk QRDA



$$|A\rangle = \frac{1}{\sqrt{2^4}} (|1000\rangle \otimes |0000\rangle + |1011\rangle \otimes |0001\rangle + |1101\rangle \otimes |0010\rangle + |1111\rangle \otimes |0011\rangle + |1111\rangle \otimes |0100\rangle + |1101\rangle \otimes |0101\rangle + |1011\rangle \otimes |0110\rangle + |1000\rangle \otimes |0111\rangle + |0101\rangle \otimes |1000\rangle + |0011\rangle \otimes |1001\rangle + |0001\rangle \otimes |1010\rangle + |0001\rangle \otimes |1011\rangle + |0011\rangle \otimes |1100\rangle + |0101\rangle \otimes |1101\rangle + |1000\rangle \otimes |1110\rangle)$$

Quantum Discrete Cosine Transform (DCT)

DCT pada audio *watermarking* adalah teknik pengolahan sinyal yang digunakan untuk mengubah domain waktu pada audio menjadi domain frekuensi. DCT menggunakan serangkaian fungsi cosinus sebagai dasar untuk merepresentasikan sinyal. Fungsi-fungsi kosinus ini diterapkan pada segmen-segmen sinyal dalam domain waktu, dan koefisien hasilnya merepresentasikan amplitudo frekuensi yang terkandung dalam sinyal. Secara matematis persamaan DCT dapat dituliskan sebagai berikut:

$$DCT[i] = \alpha(i) * \sum(x[n] * \cos((\pi/N) * (n + 0.5) * i))$$

Setelah diubah menjadi domain frekuensi, maka dilakukan penyisipan *watermark*. Teknik penyisipan yang digunakan pada Apps dan Web ini yaitu *Spread Spectrum*.

Spread Spectrum

Spread Spectrum (SS) merupakan sebuah teknik pentransmisian yang menggunakan *pseudo-noise* (PN) sebagai kunci rahasia untuk penyematan *watermark*. Konsep *watermarking* berbasis SS adalah menyebarkan setiap bit *watermark* di atas spektrum sinyal *host*. Malyar dkk. [9] mengusulkan formula untuk *watermarking* berbasis SS seperti yang ditunjukkan di bawah ini

$$r_w = r_0 + \alpha wp$$

Dimana r_0 adalah sampel dari data host, alfa adalah parameter penskalaan, w adalah elemen dari *watermark* dengan nilai $\{-1, +1\}$, p adalah PN acak yang mengambil nilai dari $\{-1, +1\}$. Pada penelitian ini nilai suatu baris hadamard digunakan sebagai representasi PN acak.

Attack

Proses *attack* dilakukan untuk pengujian ketahanan jika terjadinya serangan noise terhadap *audio host*, serangan ini dilakukan menggunakan matriks gerbang logika kuantum serangan kuantum berupa matriks Pauli-X, Pauli-Z dan Pauli-CNOT. Berikut penjelasan mengenai ketiga gerbang logika tersebut:

- Gerbang logika Pauli X, juga dikenal sebagai gerbang NOT kuantum, merupakan gerbang yang mengubah keadaan kuantum suatu qubit. Gerbang ini setara dengan operasi flipping atau invert pada keadaan kuantum. Jika qubit awalnya dalam keadaan $|0\rangle$, setelah melewati gerbang Pauli X, qubit akan berada dalam keadaan $|1\rangle$, dan sebaliknya. Secara matematis, gerbang Pauli X dinyatakan oleh matriks Pauli X:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Gerbang logika Pauli Z adalah gerbang yang memutar fasa atau fase shift pada keadaan kuantum suatu qubit. Gerbang ini mengubah tanda kompleks amplitudo qubit, tetapi tidak mempengaruhi probabilitasnya. Jika qubit awalnya dalam keadaan $|0\rangle$, setelah melewati gerbang Pauli Z, keadaan qubit tetap tidak berubah. Namun, jika qubit awalnya dalam keadaan $|1\rangle$, keadaan qubit akan berubah menjadi $-|1\rangle$. Secara matematis, gerbang Pauli Z dinyatakan oleh matriks Pauli Z:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Gerbang logika CNOT (Controlled-NOT) adalah gerbang yang mengendalikan dan mengubah keadaan satu qubit berdasarkan keadaan qubit kontrol. Gerbang ini terdiri dari dua qubit, yaitu qubit kontrol dan qubit target. Jika qubit kontrol dalam keadaan $|1\rangle$, maka keadaan qubit target akan di-flip atau di-invert. Namun, jika qubit kontrol dalam keadaan $|0\rangle$, qubit target tetap tidak berubah. Gerbang CNOT digunakan untuk melakukan operasi logika XOR pada dua qubit. Secara matematis, gerbang CNOT dinyatakan oleh matriks:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$