Analisis Digital Fingerprint pada Content ID System untuk Mendeteksi Youtube's Copyrights

Gilbert Christian Sinaga - 18219005
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: gilbertchristiansinaga@gmail.com

***Abstract*—Perkembangan teknologi semakin mempermudah penyebaran audiovisual melalui berbagai media yang ada. Youtube sebagai media sosial dengan pengguna terbanyak menyediakan akses tak terbatas bagi setiap penggunanya. Setiap pengguna dapat mengunggah apapun sesuai keinginannya. Untuk mengimbangi kebebasan tersebut, Google menciptakan sebuah sistem bernama Content ID System[1]. Sistem ini memanfaatkan teknologi *digital fingerprint* untuk mendeksi konten yang diunggah pada kanal pengguna. *Copyright* dapat dideteksi dari audio maupun video yang dihasilkan. Video yang menerima klaim *copyright* akan mendapatkan sanksi dari Youtube sendiri.**

Keywords—youtube; content ID; copyright; digital fingerprint; audio, video

I. PENDAHULUAN

Era digital mendorong penyebaran media dan informasi menjadi sangat cepat. Setiap orang yang memiliki akses pada *gadget* dan internet dapat melakukan penyebaran tersebut. Media sosial juga berkembang dengan kecepatan yang pesat, serta pemakaian algoritma algoritma yang ditujukan kepada kepuasan penggunanya. Salah satu media sosial yang dijumpai setiap hari adalah Youtube. Saat ini, Youtube merupakan media sosial dengan pengguna terbanyak. Setidaknya, Youtube memunculkan 720 ribu jam[2] video baru untuk 122 juta pengguna aktif setiap hari[3].

Dari sejumlah video tersebut, tak jarang ditemui kesamaan penggunaan audio, cuplikan video, maupun konten sejenis *reaction* yang mulai dikenal sejak tahun 2007[4]. Pada tahun yang sama, Google memperkenalkan sebuah sistem yang dapat mendeteksi kesamaan kesamaan tersebut, yang sekarang dikenal dengan istilah *copyright*[5]. Sistem tersebut dikenal dengan nama Content System ID.

Pada awal kemunculan sistem ini, banyak terjadi kesalahan klaim yang menimpa para pengguna dan kreator Youtube. Seiring waktu, sistem ini sudah berkembang menjadi sistem yang lebih mutahir dan dapat diandalkan. Hingga saat ini, Content ID System dapat menangani hingga 98% kasus *copyright* yang terjadi setiap harinya[6], menyisakan 2% pada klaim yang ditentukan secara tradisional melalui pengajuan pengguna.

Teknologi utama yang menjadi pendukung Content ID System ini adalah *digital fingerprint*. Melalui *digital fingerprint*, setiap video unggahan pengguna diperiksa baik visual maupun suaranya. Konten kreator yang terkena klaim *copyright* mengakibatkan video nya gagal dimonetisasi bahkan dapat menyebabkan permintaan *take down* secara paksa dan sepihak.

Pada makalah ini, akan dibahas bagaimana Youtube secara spesifik memanfaatkan *digital* fingerprint untuk mendeteksi copyright dan mengembangkan Content ID System miliknya. Pada bagian II terdapat penjelasan dari cara kerja *digital fingerprint* beserta jenis jenis yang dimiliki. Pada bagian III terdapat pembahasan dari Content ID System secara sekeluruhan beserta kriteria penilaian *copyright* yang dihasilkan. Pada bagian IV terdapat kesimpulan dari makalah ini.

II. TEORI DAN STUDI LITERATUR

A. Definisi Digital Fingerprint

Digital fingerprint merupakan sebuah tanda pengenal unik yang berisi satu set data untuk mengidentifikasikan pengaturan perangkat sebagai unik. Sebagai contoh, ketika menggunakan browser, *software fingerprint* akan menyimpan *fingerprint* kita pada data server. Penyimpanan ini tidak bisa dikendalikan oleh pengguna sendiri. Dengan *fingerprint* yang tersimpan, segala penggunaan internet dan aktivitas pemilik *fingerprint* dapat dilacak. Bahkan menghapus cookie atau tindakan semacamnya tidak dapat mencegah hal tersebut. *Fingerprint* sangat penting sehingga dapat digunakan untuk membongkar data milik pribadi dan menganalisis kebiasaan pengguna ketika sedang menjelajah internet.

B. Alur Kerja Digital Fingerprint

Karena *digital fingerprint* tersimpan pada data server secara otomatis, banyak cara dilakukan untuk menghindari hal tersebut. Namun upaya menghindari pencatatan *fingerprint* seringkali memberikan efek negatif pada pengalaman *browsing* pengguna.

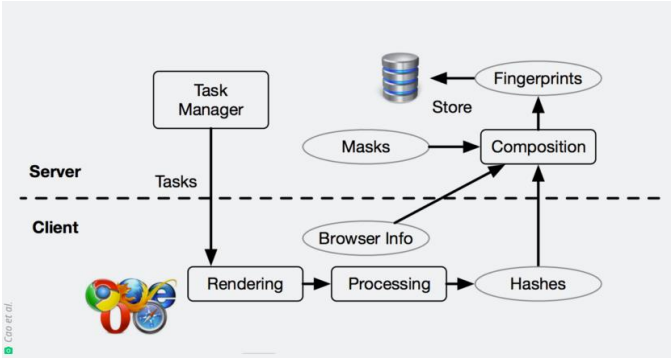

Fig. 1. Workflow Digital Fingerprint
(sumber: https://lh4.googleusercontent.com/gjwaDIux-q-s71TEw2OStHrdZWmOfwxm4GL4tpj7llrIQE89_nnS_DNDsHraNlgLRhldVGTveZGnPCDOJNqqsfOh7u2GU9BZtexPEyrX835vNgtLSv_-qY5foZEfoKQRxdr0Gy_1)

Saat memasuki sebuah website, sistem otomatis mengumpulkan data dari browser dan perangkat pengguna. Sistem ini berupa *script* pelacakan *fingerprint* (biasanya menggunakan JavaScript). Kemudian data tersebut masuk kedalam tahap *rendering*, *processing*, hingga *hashing*. Setelah proses pada *client* selesai, data tersebut dikirimkan Bersama dengan informasi browser yang digunakan kepada server untk disimpan. *Script* ini dapat dignakan untuk mengakses informasi yang sangat kompleks[7].

C. Algoritma Fingerprinting

Dalam penggunaaan *digital fingerprint* ini, terdapat dua algoritma umum yang sering digunakan. Berikut adalah penjelasan algoritma tersebut.

- Algoritma Rabin-Karp

  Algoritma Rabin-Karp merupakan sebuah algoritma yang dibuat untuk mencari suatu *string* pada *string* lainnya.

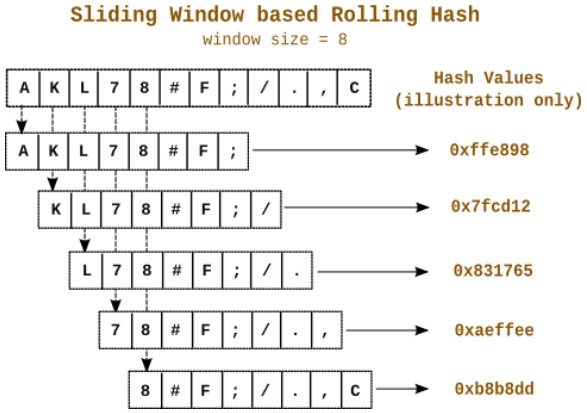

Fig. 2. Rabin Fingerprint
(sumber:
https://moinakg.files.wordpress.com/2013/06/rolling_hash.png)

Pada ilustrasi diatas, digambarkan sebuah *string* 12 karakter berisikan “AKL78#F;/.,C”. Kemudian akan dicari sebuah *string* 8 karakter yang sesuai dengan *string* pertama. Untuk menghasilkan perhitungan yang efisien, maka digunakan nilai hash sebagai pembanding.

Namun, penggunaan hash saja tidak cukup untuk mengatasi kolisi yang mungkin terjadi pada metode ini. Sehingga algoritma dikembangkan dengan menambahkan *multiplier* sebagai penanda posisi penanda karakter (misalnya 10^{n-1} dengan n sebagai posisi karakter dari kiri).

Lagi-lagi, penambahan *multiplier* tidak cukup efisien. Meskipun angka kemungkinan terjadinya kolisi menurun, namun efisiensi perhitungan juga jadi menurun. Untuk membatasi perhitungan menjadi lebih kecil, ditambahkan fungsi *mod* pada setiap perhitungan. Dengan ini, masalah efisiensi perhitungan bisa terselesaikan[8].

- Algoritma Hash Kriptografi

  Algoritma Hash Kriptografi adalah sebuah algoritma matematika yang dapat mengubah suatu pesan teks menjadi bit bit array dengan panjang ukuran tertentu dan tetap.

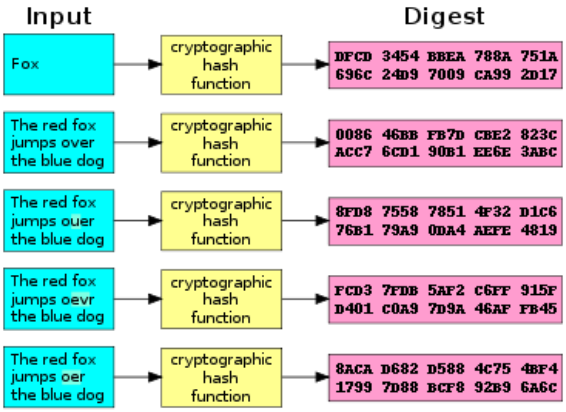

Fig. 3. Cryptographic Hash Function
(sumber:
https://upload.wikimedia.org/wikipedia/commons/thumb/2/2b/Cryptographic_Hash_Function.svg/375px-Cryptographic_Hash_Function.svg.png)

Pada ilustrasi diatas, dapat dilihat bahwa panjang teks input yang berbeda-beda akan menghasilkan nilai hash dengan panjang yang sama. Fungsi hash ini juga bersifat satu arah dan sulit ditemukan kolisinya karena merubah satu karakter pada input dapat merubah lebih dari satu karakter pada nilai hash nya.

D. Sisi Gelap Digital Fingerprint

Terlepas dari segala kelebihan dan kecanggihan yang ditawarkan, penggunaan *digital fingerprint* memiliki sisi yang tidak dapat diketahui dengan jelas. Data *fingerprint* yang tersimpan di data server tidak diterkonfirmasi bagaimana penggunaannya. Tidak ada bukti yang sah juga apabila data tersebut digunakan secara illegal. Sebagai contoh, banyak orang menganggap penggunaan *digital fingerprint* untuk keperluan pemasaran dan periklanan itu tidak apa-apa. Menurut Marketing Tech News, terlepas dari maraknya penggunaan *adblocker*, 78% pengguna ponsel tidak keberatan dengan adanya iklan yang relevan dan sesuai target. Meskipun

pengalaman pengguna yang nyaman ditukarkan dengan penyimpanan data *fingerprint* pengguna pada server[7].

III. Pembahasan

A. Pengertian Content ID System

Content ID System merupakan sebuah sistem unik yang didesain untuk menjaga keaslian hasil karya seorang kreator. Video yang diunggah ke Youtube akan dibandingkan terhadap *file* audio maupun video yang terdaftar pada sistem. Sistem memiliki daftar *file* audio dan video yang diregistrasi berdasarkan Content ID dan pemilik/kreatornya.

B. Cara Kerja Content ID System

Terdapat dua sisi utama dalam sistem Content ID ini. Pertama adalah dari sisi kreator dimana video miliknya di cek dan kedua adalah dari sisi pemilik yang memiliki hak yang mendapati kecocokan pada pengecekan konten seseorang. Seperti sebelumnya, video yang di unggah ke Youtube akan di *scan*, diperiksa, dibandingkan, dengan *database* yang ada. Ketika ditemukan kecocokan, maka ada 3 hal yang dapat terjadi:

- Seluruh video akan di blok oleh Youtube.

  Pada kasus pertama, semua pengguna Youtube tidak akan dapat melihat video ini lagi baik secara publik maupun tidak. Jika ini terjadi, kreator memiliki opsi untuk menghapus bagian yang dianggap *copyright* dan kembali menggunggah video tersebut ke Youtube. Youtube Studio sendiri sudah menyediakan fitur *cut and trim* sehingga pemotongan bagian tersebut bisa dilakukan langsung melalui Youtube Studio. Opsi lain yang bisa dipilih adalah menghilangkan audio pada durasi yang dianggap *copyright*. Dengan ini visual video yang dimiliki setidaknya tidak terpotong sama sekali.

- Pemilik hak/lisensi video original melakukan klaim terhadap video tersebut dan mendapatkan hasil monetasi dari video tersebut.

  Kasus kedua ini biasa dikenal dengan istilah “dollar kuning” dikalangan kreator. Dollar kuning adalah sebuah simbol dimana video tersebut tidak dapat dimonetisasi karena masalah *copyright*. Dengan penalty, hasil monetisasi sebagian besar atau bahkan sepenuhnya akan diberikan kepada pemilik hak video.

- Statistik penonton menjadi milik pemilik hak video.

  Di kasus ketiga, pemilik hak video dapat melakukan klaim terhadap statistik yang dihasilkan dari video yang terkena klaim.

Pemilik hak video dapat memilih salah satu dari ketiga penalti diatas untuk diberikan kepada kreator yang terkena *copyright claim*. Namun kreator yang terkena *copyright claim* juga memiliki hak untuk mengajukan banding kepada pemilik hak video[9].

C. Dibalik Content ID System

Content ID System menggunakan *database* yang berisikan audio dan video beserta pemilik pemiliknya. Untuk mencapai efisiensi dan akurasi seperti sekarang, Youtube menggunakan teknologi *digital fingerprint* pada sistem ini. Secara umum, video yang diunggah akan dipisahkan menjadi *file* audio dan video, kemudian dilakukan proses ekstraksi terhadap keduanya untuk menghasilkan *fingerprint* dan disimpan kedalam *database*. Ketika ada konten baru yang diunggah, video tersebut akan diekstrak *fingerprintnya*, dan dibandingkan dengan *fingerprint* di *database*. Jika hasil perhitungan kemiripan berapa diatas ambang batas, konten tersebut akan dianggap sebagai tiruan/*copyright*[5].

- Audio *Fingerprinting*

  Audio *Fingerprinting* adalah sebuah proses yang merepresentasikan sinyal audio menjadi ringkas dengan cara mengekstraksi fitur yang relevan dari konten audio. Proses ekstraksi ini sama prinsipnya dengan ekstraksi sidik jari manusia. Audio *fingerprint* memungkinkan pemantauan audio terlepas dari apapun jenis format audionya.. Acoustic *fingerprint* yang kuat bahkan dapat mengidentifikasi audio yang sudah melalui proses kompresi dan degradasi kualitas suara. Sebagai contoh aplikasi yang memanfaatkan hal tersebut adalah Shazam[10].

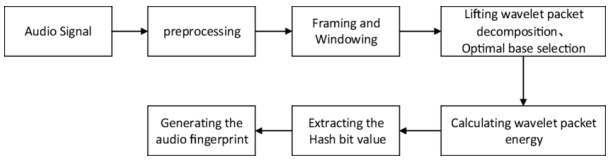

Fig. 4. Proses Ekstraksi Audio Fingerprint
(sumber: https://www.researchgate.net/publication/329075957/figure/fig5/AS:941746166972418@1601541191189/The-process-of-extracting-the-audio-fingerprinting.png)

Ilustrasi diatas merupakan alur proses ekstraksi sebuah Audio *Fingerprint*. Proses dimulai menerima input audio *signal* yang kemudian diproses sebelum dilanjutkan. Selanjutnya audio akan pecahkan berdasarkan *frame* (atau bisa disebut *group sampling*) dan diperhalus frekuensinya dengan proses yang disebut *windowing*. Kemudian masing masing *frame* didekomposisi lagi berdasarkan *wavelet packet*. *Wavelet packet* inilah yang akan menjadi input pada fungsi hash sehingga dapat menghasilkan audio *fingerprint*.

Pemecahan audio harus sampai ke tahap paket *wavelet* karena dua sifat yang dimilikinya yaitu:

1. Scaling; dimana *wavelets* dapat diubah berdasarkan frekuensi menjadi lebih rapat/renggang
2. Shifting; dimana *wavelets* dapat diubah berdasarkan waktu menjadi lebih lambat, cepat, atau terlambat (*delay*)[11].

Kedua sifat inilah yang menyebabkan pemecahan audio hingga tahap paket *wavelets*. Dengan ekstraksi *fingerprint* di tahap ini, akurasi deteksi audio *copyright* menjadi lebih tinggi.

- Video Fingerprinting

  Video Fingerprint adalah sebuah representasi digital ringkas dari video dengan merangkum karakteristik unik dari konten video. Video *fingerprint* menghasilakn *digital profile* khas yang kemudian dapat digunakan untuk melakukan analisis dan identifikasi konten media yang original, yang berasal dari sumber mana saja.

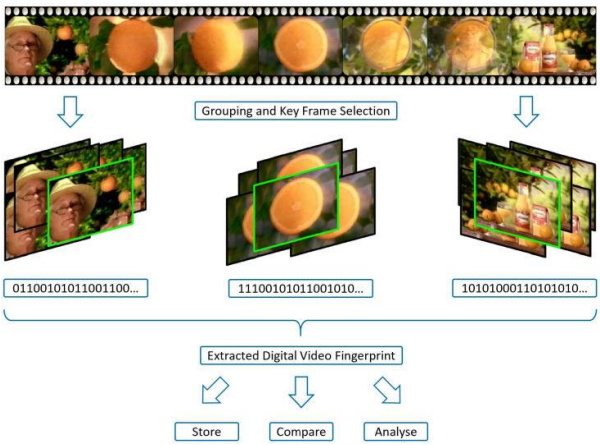

Fig. 5. Proses Ekstraksi Video Fingerprint (sumber: https://ivitec.com/assets/images/what-is-digital-video-fingerprinting-ivitec.com-732x537.jpg)

Pada proses ekstraksi *fingerprint* video, komponen audio pada video dapat diekstraksi menggunakan cara yang sama seperti sebelumnya. Dibandingkan dengan ekstraksi pada audio, proses ekstraksi video lebih singkat. Video akan di pecah menjadi kelompok *frame* dan langsung diekstrak menjadi sebuah *fingerprint.*

Video dapat diklasifikasikan menjadi 3 dimensi:

1. Dimensi warna; dimensi yang bergantung dengan warna, *hue*, saturasi, dsb.
2. Dimensi spasial; dimensi yang memperhatikan distribusi warna pada frame, sehingga bisa melacak perbedaan tiap frame melalui lokasi *pixel*.
3. Dimensi temporal; dimensi yang memerhatikan keterurutan *frame*, *motion detection*.

Dengan ketiga dimensi tersebut, area perbandingan menjadi lebih luas dan akurat[12].

IV. Kesimpulan dan Saran

Content ID System adalah sebuah sistem yang menyimpan *digital fingerprint* dari seluruh media yang terdaftar di satu *database*. Sistem ini digunakan oleh Youtube sejak tahun 2007 untuk mengotomatisasi proses pemeriksaan *copyright*. Sistem ini menggunakan *digital fingerprint* sebagai teknologi utamanya. Pada konsepnya, proses menghasilkan *fingerprint* terbagi menjadi dua, yaitu audio dan video. Kedua nya dihasilkan melalui proses ekstraksi yang serupa.

Meskipun dengan *properties* dan parameter yang cukup kompleks, namun Content ID System masih memiliki celah yang bisa dimanfaatkan para kreator. Hal ini dapat dibuktikan dari 2% konten Youtube yang harus diperiksa secara manual. Konten yang dicek melalui sistem juga masih bisa menghasilkan klaim yang salah. Untuk perkembangan selanjutnya, transparansi kriteria Content ID System bisa menjadi pilihan untuk mengantisipasi klaim *copyright* yang salah.

Ucapan Terimakasih

Saya ingin mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas karunia-Nya saya dapat menyelesaikan makalah ini, kepada orang tua saya yang selalu memberikan dukungan, kepada Pak Rinaldi Munir selaku dosen pengampu mata kuliah II4031 Kriptografi dan Koding yang telah membimbing saya selama satu semester dan kepada semua teman teman di kelas II4031 Kriptografi dan Koding ini, terutama Natasya sebagai teman sekelompok semua tugas di kelas Kriptografi. Dan tidak lupa juga mengucapkan terimakasih kepada semua penulis referensi yang saya gunakan atas ilmu dan wawasan yang disediakan.

Referensi

[1] Qualify for Content ID - YouTube Help. (n.d.). Youtube Help. Retrieved May 25, 2022, from https://support.google.com/youtube/answer/1311402?hl=en&ref_topic=9282364

[2] Wise, J. (2022, May 20). *How Many Videos Are Uploaded To Youtube A Day in 2022?* EarthWeb. Retrieved May 25, 2022, from https://earthweb.com/how-many-videos-are-uploaded-to-youtube-a-day/

[3] *YouTube Statistics 2022 [Users by Country + Demographics]*. (2022, May 11). Official GMI Blog. Retrieved May 25, 2022, from https://www.globalmediainsight.com/blog/youtube-users-statistics/

[4] Wikipedia contributors. (2022, March 6). *Reaction video*. Wikipedia. Retrieved May 25, 2022, from https://en.wikipedia.org/wiki/Reaction_video

[5] J. (2021, November 28). *How Does The YouTube Content ID System Work?* Jdhao's Digital Space. Retrieved May 25, 2022, from https://jdhao.github.io/2021/08/02/the_youtube_content_id_system/

[6] *Unfiltered: How YouTube's Content ID Discourages Fair Use and*. (2020, December 11). Electronic Frontier Foundation. Retrieved May 25, 2022, from https://www.eff.org/wp/unfiltered-how-youtubes-content-id-discourages-fair-use-and-dictates-what-we-see-online

[7] Phoenix, J. (2021, November 19). *What is a Digital Fingerprint?* Just Understanding Data. Retrieved May 25, 2022, from https://understandingdata.com/what-is-a-digital-fingerprint/

[8] *What are Cryptographic Hash Functions?* (2018, January 16). YouTube. Retrieved May 25, 2022, from https://www.youtube.com/watch?v=UswqcbncliE

[9] *Unfiltered: How YouTube's Content ID Discourages Fair Use and*. (2020b, December 11). Electronic Frontier Foundation. Retrieved May 25, 2022, from https://www.eff.org/wp/unfiltered-how-youtubes-content-id-discourages-fair-use-and-dictates-what-we-see-online

[10] Sandeep G, C. P. (2020, July 9). *Audio Fingerprinting- Understanding the Concept, Process & Application*. PathPartnerTech. Retrieved May 25, 2022, from https://www.pathpartnertech.com/audio-fingerprinting-understanding-the-concept-process-application/

[11] *Understanding Wavelets, Part 1: What Are Wavelets*. (2016, August 18). YouTube. Retrieved May 25, 2022, from https://www.youtube.com/watch?v=QX1-xGVFqmw

[12] Lee, S., & Yoo, C. D. (2008). Robust video fingerprinting for content-based video identification. *IEEE Transactions on Circuits and Systems for Video Technology*, *18*(7), 983–988. https://doi.org/10.1109/tcsvt.2008.920739

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 25 Mei 2021

Gilbert Christian Sinaga
18219005