Tanda Tangan Digital Pada File Video Menggunakan Algoritma ECDSA

Bintang Hijriawan Jachja 13521003
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13521003@std.stei.itb.ac.id, bintanghijriawan433@gmail.com

***Abstract*—Perkembangan teknologi multimedia menyebabkan meningkatnya distribusi file video melalui jaringan digital, sehingga diperlukan mekanisme keamanan untuk menjamin keaslian dan integritas data. File video sangat rentan terhadap manipulasi, baik berupa pengubahan isi, pemotongan, maupun penyisipan informasi tertentu. Oleh karena itu, diperlukan suatu metode yang mampu memastikan bahwa file video yang diterima merupakan file asli dan tidak mengalami perubahan. Penelitian ini membahas penerapan tanda tangan digital pada file video menggunakan algoritma Elliptic Curve Digital Signature Algorithm (ECDSA).**

***Keywords*—Tanda tangan digital, ECDSA, video, MKV, SHA-256.**

I. Pendahuluan

Saat ini, perkembangan teknologi dan penyebaran informasi telah berkembang pesat. Kapasitas transfer data digital melalui jaringan komunikasi tidak lagi dibatasi oleh ukuran data. Dengan demikian, orang dapat mengirim tidak hanya informasi teks, tetapi juga file multimedia seperti gambar, file audio, dan video. Saat ini, distribusi file multimedia, terutama video di media sosial, semakin meluas dan populer. Namun, dampak negatif yang timbul dari penyebaran informasi ini adalah semakin mudah bagi orang untuk mengirim video tanpa memvalidasi kebenaran video tersebut dan memudahkan pihak yang tidak bertanggung jawab untuk memotong, mengubah, atau yang secara populer disebut 'framing' oleh pihak yang tidak bertanggung jawab. Ada juga peningkatan penyebaran video yang diedit yang menghasilkan video palsu. Akibatnya, orang merasa sulit untuk percaya bahwa video yang mereka terima adalah asli dan belum diubah. Tanda tangan digital adalah salah satu solusi alternatif yang dapat digunakan untuk otentikasi dan verifikasi integritas video.

II. Landasan Teori

A. Tanda Tangan Digital

Tanda tangan digital adalah tanda tangan yang dibuat dalam bentuk digital dan mewakili identitas, sama seperti tanda tangan tertulis yang umumnya digunakan. Tanda tangan digital bukanlah tanda tangan tertulis yang dikonversi menjadi gambar, melainkan nilai kriptografis yang tertanam dalam pesan. Tanda tangan bergantung pada isi pesan dan nilai kunci yang menunjukkan identitas pengirim. Oleh karena itu, jika ada dua pesan berbeda yang dikirim oleh pengirim yang sama, keduanya akan memiliki nilai tanda tangan digital yang berbeda.

Tanda tangan digital memberikan tiga aspek keamanan, yaitu integritas data, otentikasi, dan non-repudiasi. Dengan tanda tangan digital, penerima pesan dapat memverifikasi keaslian pesan dan memberikan informasi tentang identitas pengirim. Hal ini menunjukkan tanda tangan digital dapat menyediakan layanan integritas data untuk pesan yang dikirim. Tanda tangan digital juga memastikan bahwa hanya penerima yang dituju yang dapat melakukan proses verifikasi, sehingga menjaga aspek otentikasi dan mencegah pengirim menyangkal bahwa mereka mengirim pesan karena identitas mereka tercatat melalui tanda tangan.

B. Video File

File video adalah format atau wadah digital untuk menyimpan data video (gambar bergerak dan audio) beserta informasi pendukungnya, menggunakan codec dan kontainer untuk menentukan kompatibilitas, kualitas, dan ukuran file, memungkinkan video dapat diputar, diedit, atau dibagikan di berbagai perangkat dan platform. Format video umum meliputi MP4, MOV, MKV, AVI, WMV, MPEG/MPG, dan WebM, yang semuanya menyimpan video dengan codec berbeda untuk kualitas dan ukuran file yang bervariasi.

Format MKV (Matroska Video) adalah format kontainer multimedia yang fleksibel, open source, dan gratis untuk menyimpan video, audio, teks terjemahan, dan data lainnya dalam satu file, mirip dengan AVI atau MP4 tetapi lebih canggih, mendukung beberapa trek audio/teks terjemahan, bab, dan hampir semua codec. Tipe file ini yang akan digunakan dalam pengujian penambahan tanda tangan digital pada file video.

C. Algoritma ECDSA

ECDSA (Elliptic Curve Digital Signature Algorithm) adalah algoritma tanda tangan digital berbasis kriptografi

kunci publik yang menggunakan matematika kurva elips. ECDSA merupakan perluasan dari algoritma DSA (Digital Signature Algorithm) dan secara konseptual berakar pada skema tanda tangan ElGamal, namun dengan tingkat efisiensi dan keamanan yang lebih tinggi. Tujuan utama ECDSA adalah untuk menjamin keaslian pengirim, integritas pesan, dan non-repudiasi, sehingga pengirim tidak dapat menyangkal bahwa mereka telah menandatangani pesan tersebut. Secara keseluruhan, ECDSA menawarkan keamanan tinggi dengan ukuran kunci yang relatif kecil dibandingkan dengan algoritma tanda tangan digital lainnya seperti RSA, sehingga lebih efisien dalam hal komputasi dan penyimpanan. Oleh karena itu, ECDSA banyak digunakan dalam sistem modern seperti TLS/SSL, sertifikat digital, dan teknologi blockchain. Namun, implementasinya harus dilakukan dengan hati-hati, terutama dalam pembangkitan bilangan acak, agar tingkat keamanannya tetap terjaga.

D. Fungsi Hash SHA-256

SHA-256 (Secure Hash Algorithm 256-bit) adalah fungsi hash kriptografi yang digunakan untuk mengubah data berukuran apa pun menjadi nilai hash tetap berukuran 256-bit. SHA-256 merupakan bagian dari keluarga SHA-2 yang dirancang oleh NSA dan distandarkan oleh NIST, serta banyak digunakan dalam sistem keamanan modern seperti tanda tangan digital, sertifikat digital, blockchain, dan verifikasi integritas data.

SHA-256 bekerja berdasarkan prinsip fungsi satu arah, artinya nilai hash dapat dihitung dengan mudah dari data asli, tetapi hampir tidak mungkin untuk memulihkan data asli hanya dari nilai hash. Selain itu, SHA-256 memiliki ketahanan terhadap tabrakan, artinya sangat tidak mungkin dua potongan data yang berbeda menghasilkan nilai hash yang sama, serta efek avalanche, di mana perubahan satu bit pada input akan secara signifikan mengubah hasil hash.

Dalam prosesnya, data input terlebih dahulu melalui tahap padding, yang menambahkan bit untuk membuat panjang data menjadi kelipatan 512 bit. Setelah itu, data dibagi menjadi beberapa blok 512 bit dan diproses secara berurutan menggunakan serangkaian operasi logika bit, seperti rotasi, pergeseran, dan penambahan modulo. Proses ini menggunakan delapan nilai hash awal dan 64 konstanta tetap, yang menghasilkan nilai hash akhir sebesar 256 bit.

III. Rancangan

Penambahan tanda tangan digital terbagi menjadi dua proses utama, yaitu proses penandatanganan dan proses verifikasi. Kedua proses tersebut membutuhkan ringkasan dari file video yang didapatkan dari hasil perhitungan fungsi hash SHA-256. Setiap frame pada file video diproses menggunakan fungsi hash SHA-256 yang akan menghasilkan sebuah teks, yang kemudian digabungkan dan diproses lagi dengan fungsi hash SHA-256 hingga menjadi sebuah teks yang merupakan ringkasan dari seluruh frame pada video.

Pada proses penandatanganan, ringkasan akhir ini kemudian diproses menggunakan algoritma ECDSA menggunakan kunci privat. Sistem akan memilih sebuah bilangan acak yang hanya akan digunakan satu kali, yang akan digunakan bersama dengan kunci privat dan ringkasan video untuk perhitungan matematis pada kurva eliptik sehingga menghasilkan pasangan bilangan yang merupakan tanda tangan digital video tersebut.

Proses verifikasi dilakukan dengan menghitung ulang hash dari video yang diterima lalu memverifikasi tanda tangan menggunakan kunci publik ECDSA pemilik video. Jika hasil verifikasi valid berarti video tersebut tidak mengalami perubahan apapun dan berasal dari pemilik kunci tersebut.

Tahapan proses penandatanganan video dengan metode ini adalah sebagai berikut:

1. Sistem membaca file video dan mengekstraksi seluruh frame
2. Setiap frame diproses dengan fungsi hash SHA-256
3. Hasil fungsi hash tersebut digabung kemudian di proses lagi dengan fungsi hash yang sama untuk mendapatkan ringkasan video.
4. Ringkasan tersebut digunakan untuk membuat tanda tangan digital dengan algoritma ECDSA dengan kunci privat, sehingga menghasilkan tanda tangan digital berupa pasangan bilangan.
5. Nilai tanda tangan yang didapatkan kemudian disisipkan pada akhir video dengan menambahkan frame khusus.
6. Frame khusus ini berupa sebuah frame yang diinisialisasi dengan warna hitam, kemudian menyisipkan digit tanda tangan pada setiap pixel RGB dengan pixel awal digunakan untuk menyimpan panjang data tanda tangan.

Setelah selesai, video bisa dikirim dan diverifikasi menggunakan frame akhir pada file video tersebut dengan tahapan sebagai berikut:

1. Sistem membaca file video dan memisahkan frame video dengan frame terakhir
2. Frame video diproses menggunakan SHA-256 seperti pada proses penandatanganan
3. Data tanda tangan diekstrak dari frame terakhir dengan memanfaatkan informasi panjang data tanda tangan pada pixel pertama.
4. Nilai tanda tangan tersebut diverifikasi menggunakan kunci publik ECDSA apakah nilainya valid atau tidak

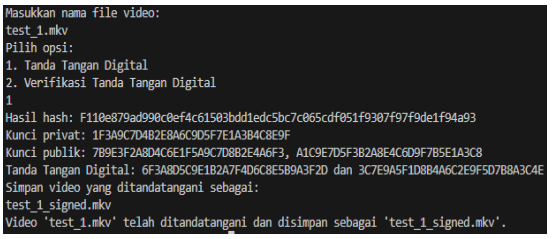
IV. Implementasi

Dilakukan 2 buah pengujian dengan ukuran video berbeda dengan hasil sebagai berikut:

A. Video 1

Spesifikasi video sebagai berikut:

a. Ukuran: 9,315,133 bytes
b. Resolusi: 2560 x 1440



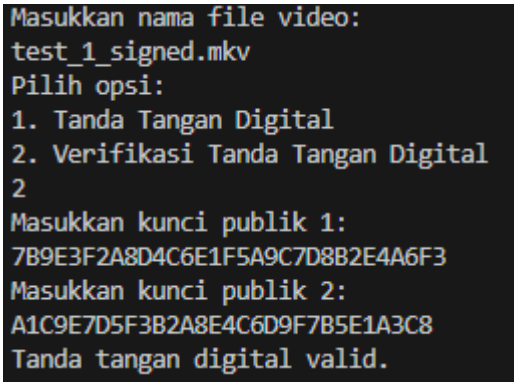
Hasil hash SHA-256:
F110e879ad990c0ef4c61503bdd1edc5bc7c065cd
f051f9307f97f9de1f94a93

Kunci privat yang digunakan:
1F3A9C7D4B2E8A6C9D5F7E1A3B4C8E9F

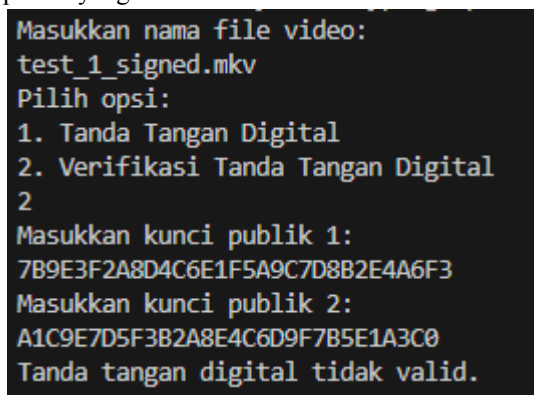
Kunci publik yang digunakan:
7B9E3F2A8D4C6E1F5A9C7D8B2E4A6F3,
A1C9E7D5F3B2A8E4C6D9F7B5E1A3C8

Hasil tanda tangan adalah pasangan bilangan yaitu 6F3A8D5C9E1B2A7F4D6C8E5B9A3F2D dan 3C7E9A5F1D8B4A6C2E9F5D7B8A3C4E

Contoh ketika dilakukan verifikasi



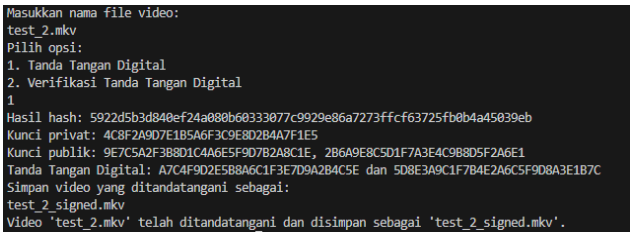
Contoh ketika dilakukan verifikasi dengan kunci publik yang berbeda



B. Video 2

Spesifikasi video sebagai berikut:

a. Ukuran: 8,273,685 bytes
b. Resolusi: 1920 x 1080



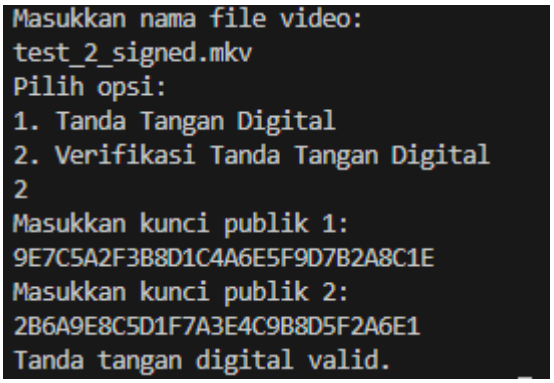
Hasil hash SHA-256:
5922d5b3d840ef24a080b60333077c9929e86a72
73ffcf63725fb0b4a45039eb

Kunci privat yang digunakan:
4C8F2A9D7E1B5A6F3C9E8D2B4A7F1E5

Kunci publik yang digunakan:
9E7C5A2F3B8D1C4A6E5F9D7B2A8C1E,
2B6A9E8C5D1F7A3E4C9B8D5F2A6E1

Hasil tanda tangan adalah pasangan bilangan yaitu A7C4F9D2E5B8A6C1F3E7D9A2B4C5E dan 5D8E3A9C1F7B4E2A6C5F9D8A3E1B7C

Ketika dilakukan verifikasi



V. Conclusion

Tanda tangan digital berhasil diimplementasikan pada file video menggunakan fungsi hash SHA-256 dan algoritma enkripsi ECDSA. Proses pemberian tanda tangan dan verifikasi tanda tangan berhasil dilakukan namun dengan waktu yang terbilang cukup lama. Tanda tangan digital hanya akan terverifikasi dengan kunci publik yang sesuai dan frame video asli, jika ditemukan perubahan pada frame hasil verifikasi menunjukan ketidaksesuaian. Namun, terdapat beberapa batasan pada rancangan tanda tangan digital ini, yaitu proses tanda tangan digital diterapkan pada bagian frame dari video saja, sehingga jika terdapat perubahan pada audio dari video tersebut belum dapat diverifikasi.

VI. Ucapan Terima Kasih

Penulis berterima kasih kepada Allah SWT atas rahmat-Nya penulis bisa menyelesaikan makalah ini. Penulis juga mengucapkan terima kasih kepada seluruh pihak yang telah membantu baik secara langsung maupun

tidak langsung, terutama Dr. Ir. Rinaldi Munir, yang telah memberikan wawasan yang berguna dalam penulisan makalah ini.

REFERENCES

[1] Munir, Rinaldi. "Tanda Tangan Digital". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/29-Tanda-tangan-digital-2025.pdf . Diakses pada 20 Desember 2025

[2] Munir, Rinaldi. "Digital Signature Algorithm (DSA) dan Elliptic Curve DSA (ECDSA)". https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2025-2026/29-Tanda-tangan-digital-2025.pdf . Diakses pada 20 Desember 2025

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, 23 Desember 2025

Bintang Hijriawan Jachja 13521003