Journal of Informatics Management and Information Technology
ISSN XXXX-XXXX (Media Online)
Vol 1, No 1, Januari 2021
Hal 23-29
https://hostjournals.com/jimat

Analisa Metode SHA-512 Untuk Tanda Tangan Digital Pada File Video

Mhd. Ipdal

Program Studi Teknik Informatika Universitas Budi Darma, Medan, Indonesia
Email: muhammadipdal123@gmail.com

Abstrak−Kriptografi yaitu ilmu untuk menjaga keamanan data. Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan menjaga keaslian data, kerahasiaan data, serta keaslian pengiriman data. SHA-512 merupakan fungsi hash satu arah yang didesain oleh *National Security Agency* (NSA) dan dipublikasi oleh *National Institute of Standards and Technology* (NIST) sebagai *Federal Information Processing Standard* (FIPS) pada tahun 1993 dan disebut sebagai SHA-0, dua tahun kemudian dipublikasikan SHA 1 generasi selanjutnya yang merupakan perbaikan dari algoritma SHA-0. Pada tahun 2002 dipublikasikan empat variasi lainnya, yaitu SHA-224, SHA- 256, SHA-384, dan SHA-512, keempatnya disebut sebagai SHA-2. Fungsi hash SHA-512 merupakan fungsi yang menghasilkan message digest ukuran 512 bit dan panjang blok 1024 bit. Terdapat 80 putaran dalam fungsi ini.Penelitian ini akan menggunakan Metode SHA-512 untuk mengamankan suatu keaslian, kerahasiaan, integritas, dan auntentikasi tanda tangan digital pada file video. Penelitian ini menguraikan proses pengamanan untuk mendeteksi keaslian tanda tangan digital pada file video dengan menggunakan Metode SHA-512 dalam bentuk pendeteksian tanda tangan digital pada file video yang bersifat rahasia yang dikirim melalui telekomunikasi umum tidak dapat dirubah atau dimodifikasi oleh orang yang tidak berhak atau orang yang tidak berkepentingan. Hal ini dilakukan sebagai upaya untuk meminimalisir tindakan-tindakan penipuan, pemalsuan, hoax, atau-pun penyalahgunaan tanda tangan digital pada file video.

Kata Kunci: Kriptografi; Tanda Tangan Digital; *File Video*; SHA-512

Abstract−Cryptography is the science of maintaining data security. Cryptography is a data security method that can be used to maintain data authenticity, data confidentiality, and data transmission authenticity. SHA-512 is a one-way hash function designed by the National Security Agency (NSA) and published by the National Institute of Standards and Technology (NIST) as the Federal Information Processing Standard (FIPS) in 1993 and referred to as SHA-0, two years later. published next generation SHA 1 which is an improvement of the SHA-0 algorithm. In 2002 four other variations were published, namely SHA-224, SHA-256, SHA-384, and SHA-512, four of which were referred to as SHA-2. The SHA-512 hash function is a function that produces a message digest of 512 bits in size and 1024 bits in length. There are 80 loops in this function. This research will use the SHA-512 Method to secure the authenticity, confidentiality, integrity, and authentication of digital signatures on video files. This study describes the security process to detect the authenticity of digital signatures on video files using the SHA-512 method in the form of detecting digital signatures on confidential video files sent via public telecommunications that cannot be changed or modified by unauthorized persons or persons who not concerned. This is done as an effort to minimize fraudulent acts, forgery, hoaxes, or misuse of digital signatures on video files.

Keywords: Cryptography; Digital Signature; Video File; SHA-512

1. PENDAHULUAN

Keamanan informasi adalah bagaimana kita dapat mencegah penipuan, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak bersifat fisik. Untuk itu diperlukanlah sebuah pendekatan dalam melakukan pengamanan pada informasi, seperti melakukan enkripsi, steganografi, cipher dan hashing terhadap informasi tersebut.

Tanda tangan biasa berupa goresan simbol yang unik sedangkan tanda tangan digital berupa kode-kode yang berisi nilai kriptografis dimana kode-kode tersebut bergantung pada pesan dan pengirim pesan. Keberadaan tanda tangan sebagai salah satu media yanga banyak digunakan. Tanda tangan digital atau yang lebih dikenal dengan *digital signature* merupakan salah satu solusi untuk mengatasi masalah. Tanda tangan digital memiliki fungsi sama seperti mentrasfer tulisan, dokumen atau file secara digital memunculkan kebutuhan terkait otentikasi suatu tanda tangan.
Defenisi tanda tangan digital adalah suatu skema matematika untuk menunjuk- kan keaslian pesan digital atau dokumen. Sebuah tanda tangan digital hanya falid jika memberikan alasan percaya bahwa penerima pesan yang dibuat oleh pengirim yang diketahui, bahwa itu tidak diubah dalam perjalanan. Proses kerja tanda tangan digital adalah tanda tangan yang terdiri atas informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi. Tanda tangan digital berbeda dengan tanda tangan yang dipindai kemudian ditempelkan ke dalam dokumen elektronik. Tanda tangan digital yang tersertifikasi atau tanda tangan digital berbentuk rangkaian data yang ditambahkan kedalam dokumen elektronik menggunakan perhitungan matematika. Untuk memeriksa sebuah tanda tangan digital harus dilakukan secara elektronik.Dalam penerapannya, tanda tangan digital bersifat unik. Tanda tangan seseorang akan berbeda dengan tanda tangan orang lain. tanda tangan sehingga dokumen tidak dapat diterima, tanda tangan digital membutuhkan jaminan keaslian data yang dikirim melalui media jaringan. Penggunaan tanda tangan digital pada file video dapat dilakukan dengan menggunakan enkripsi terhadap pesan yang dikirim dengan mengunakan kriptografi fungsi *hash*.

Penggunaan tanda tangan digital berupa tulisan akan menghasilkan dokumen tanda tangan yang terlihat secara jelas karena ditulis dengan kode yang terlihat. Hal ini dapat memunculkan potensi pemalsuan dan gangguan dengan menghilangkan tanda tangan sehingga dokumen tidak dapat diterima, tanda tangan digital membutuhkan jaminan keaslian data yang dikirim melalui media jaringan. Penggunaan tanda tangan digital pada file video dapat dilakukan

dengan menggunakan enkripsi terhadap pesan yang dikirim dengan mengunakan kriptografi fungsi *hash* Kriptografi adalah ilmu untuk menjaga suatu keamanan data. Kriptografi ini merupakan suatu metode pengamanan data yang dapat digunakan untuk menjaga keaslian data, serta kerahasiaan data tersebut. pada tahap ini teknik anlisa akan diperlukan, melakukan identifikasi masalah yang ada untuk cek keaslian tanda tangan pada file video dengan membandingkan metadata, pengumpulan data yang diperlukan untuk menganalisa sistem keamanan pada tanda tangan digital, selanjutnya tahapan enkripsi, enkripsi yang digunakan dalam kriptografi adalah fungsi *hash*. *Hash* adalah suatu teknik klasik dalam ilmu Komputer yang banyak digunakan dalam praktek enkripsi. *Hash* merupakan suatu metode yang secara langsung mengakses record-record dalam suatu tabel dengan melakukan transformasi aritmatik pada suatu input dari user yang biasanya merupakan bentuk string. Fungsi *hash* yang digunakan untuk mengenkripsi sebuah data menjadi data yang lebih kecil yang mengandung nilai unik yang merepresentasikan data sebelumnya. Nilai hash dari suatu fungsi hash akan memiliki panjang bit yang tetap untuk masukan apapun dengan panjang bit berapapun.

2. METODOLOGI PENELITIAN

2.1 Analisa

Teknik analisa adalah untuk menyederhanakan data sehingga dapat lebih di mengerti. Pertama-tama penganalisis harus menganalisis atau mengumpulkan data yang diperlukan, mengukur dan kemudian menganalisis dan menginterprentasikan sehingga data itu menjadi lebih berarti [1].

Analisis diartikan sebagai penguraian suatu pokok atas berbagai penelahan bagian itu sendiri, serta hubungan antar bagian untuk memperoleh pengertian yang tepat dan pemahaman arti keseluruhan. Analisis adalah suatu kegiatan berpikir untuk menguraikan suatu keseluruhan menjadi komponen sehingga dapat mengenali tanda-tanda komponen, serta hubungannya satu sama lain dan fungsi masing-masing dalam satu keseluruhan yang terpadu [2].

2.2 Keamanan Infomasi

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting bagi sebuah organisasi, perguruan tinggi, lembaga pemerintahan maupun individual, kemampuan dalam mengakses dan menyediakan informasi secara cepat. Karena pentingnya sebuah informasi, sering kali informasi yang diinginkan hanya dapat diakses oleh orang tertentu misalnya pihak penerima yang di inginkan akan berdampak kerugian pada pihak pengirim. Keamanan informasi adalah bagaimana kita dapat mencegah penipuan, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak bersifat fisik. Untuk itu diperlukan. sebuah pendekatan dalam melakukan pengamanan pada informasi, seperti melakukan Enkripsi, Stanoganografi, Cipher dan Hashing terhadap informasi tersebuit

2.3 Kriptografi

Pengamanan terhadap data (informasi) dapat dilakkan dengan beberapa cara. Yaitu Steganografi, *Watermarking*, Kriptografi.[6]. Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi, terutama dalam bidang komputer. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan data atau informasi [2]. Karena itu kriptografi menjadi suatu ilmu yang berkembang pesat dan dalam waktu singkat banyak muncul algoritma-algoritma baru yang dianggap lebih unggul daripada algoritma pendahulunya.

2.4 Algoritma SHA-512

SHA adalah fungsi hash satu arah yang didesain oleh National Security Agency (NSA) dan dipublikasi oleh National Institute of Standards and Technology (NIST) sebagai Federal Information Processing Standard (FIPS) pada tahun 1993 dan disebut sebagai SHA-0, dua tahun kemudian dipublikasikan SHA 1 generasi selanjutnya yang merupakan perbaikan dari algoritma SHA-0. Pada tahun 2002 dipublikasikan empat variasi lainnya, yaitu SHA-224, SHA- 256, SHA-384, dan SHA-512, keempatnya disebut sebagai SHA-2.

Fungsi hash SHA-512 merupakan fungsi yang menghasilkan message digest ukuran 1024 bit . Terdapat 80 putaran dalam fungsi ini. Untuk melakukan padding bit dilakukan dengan cara yang sama dengan SHA-1[7].

2.5 *Secure Hash Algorithm* -1 (SHA-1)

SHA-1 menerima masukan berupa *string* dengan ukuran maksimum 264 bit. Untuk setiap *string*, SHA-1 akan menghasilkan keluaran sebanyak 160 bit dari string tersebut dan *string* keluaran itu disebut *message digest*. Panjang jarak *message digest* dapat berkisar antara 160 sampai 512 bit tergantung algoritmanya. Berdasarkan cirinya SHA-1 dapat digunakan dengan algoritma kriptografi lainnya seperti *Digital Signature Algorithms* atau dalam generasi angka yang acak *(bits)*. SHA-1 dikatakan aman karena proses SHA-1 dihitung secara infisibel untuk mencari *string* yang sesuai untuk menghasilkan *message digest* atau dapat juga digunakan untuk mencari dua *string* yang berbeda yang akan menghasilkan *message digest* yang sama. Untuk SHA-1 ukuran *blokstring* -m bit- dapat ditentukan tergantung dari algoritmanya. Pada SHA-1 masing-masing *blokstring* mempunyai 512 bit dimana dapat dilakukan dengan 16 urutan sebesar 32 bit. SHA-1 digunakan untuk menghitung *message digest* pada *string* atau *file* data yang diberikan sebagai

input. Tujuan pengisian *string* adalah untuk menghasilkan total dari string yang diisi menjadi perkalian dari 512 bits. Beberapa hal yang dilakukan dalam pengisian *string* [8] :

a. Panjang dari *string*, M adalah k bit dimana panjang $k < 2^{64}$. Tambahkan bit "1" pada akhir string. Misalkan string yang asli adalah "01010000" maka setelah diisi menjadi "010100001".

b. Tambahkan bit "0", angka bit "0" tergantung dari panjang string. Misalnya : String asli yang merupakan bit string : abcde
01100001 01100010 01100011 01100100 01100101.
Setelah langkah (a) dilakukan
01100001 01100010 01100011 01100100 01100101.
Panjang k = 40 dan angka bit di atas adalah 41 dan 407 ditambah bit "0"
(448 – (40 + 1) = 407). Kemudian diubah dalam *hex* :
61626364 65800000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000

c. Untuk memperoleh 2 kata dari k, angka bit dalam *string* asli yaitu jika $k < 2^{32}$ maka kata pertama adalah semua bit "0". Maka gambaran dari 2 kata dari
k = 40 dalam *hex* adalah
00000000 00000028
61626364 65800000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000028

SHA-1 menggunakan urutan fungsi logika yang dilambangkan dengan f_0, f_1,, f_{79}. Untuk masing-masing ft, dimana $0 \leq t < 79$ akan menghasilkan *output* sebanyak 32 bit. Fungsinya adalah sebagai berikut :

$$f_t(B, C, D) = \begin{cases} (B \wedge C) \vee (\neg B \wedge D) & 0 \leq t \leq 19 \\ B \oplus C \oplus D & 20 \leq t \leq 39 \\ (B \wedge C) \vee (B \wedge D) \vee (C \wedge D) & 40 \leq t \leq 59 \\ B \oplus C \oplus D & 60 \leq t \leq 79 \end{cases}$$

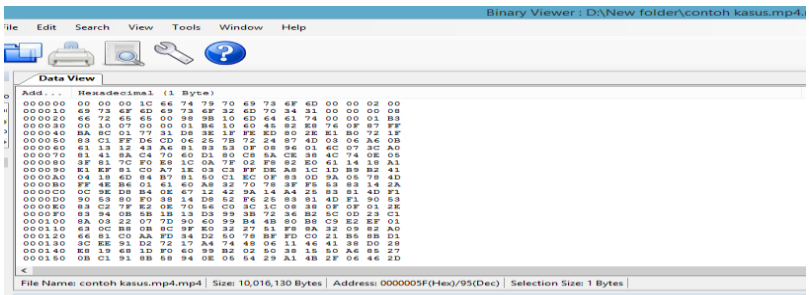
$\oplus$ = fungsi XOR

3. HASIL DAN PEMBAHASAN

Contoh kasus dalam proses ini seperti dijelaskan dalam analisa yaitu file video MP4 (contoh kasus) yang di dalamnya di sisipkan tanda tangan digital, tandatangan digital seperti di bawah ini:

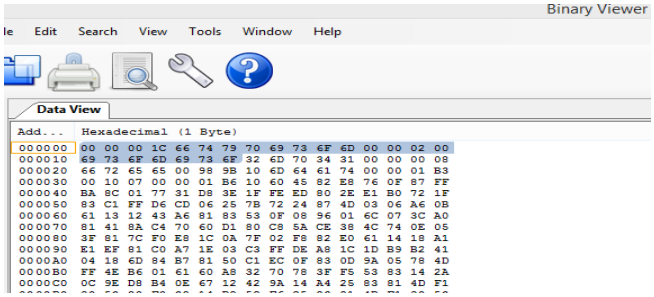
Gambar 1. Tanda Tangan Digital pada File Video

Data yang diambil hanya sebanyak 24 byte, cara pengambilan nilai hex data video menggunakan aplikasi Binary Viewer. Gambar di bawah ini adalah data heksadesimal dari file video contoh kasus.mp4 menggunakan aplikasi



Gambar 2. Data video MP4

Dari data tersebut diambil sebanyak 24 byte atau 48 karakter heksadesimal dan dikonversi ke biner sebagai sampel metode, yang berguna untuk mengetahui nilai biner dari bilangan tersebut.



Gambar 3. Data byte video "contoh kasus.mp4"

Dari gambar data di atas diambil sebanyak 24 bit, yaitu : 0000001C6674797069736F6D000002069736F6D69736f32.
A. Penambahan bit-bit pengganjal dan nilai panjang pesan semula dari data yang digunakan dan diubah ke biner.
Heksadesimal:
0000 001C 6674 7970 6973 6F6D 0000 0200 697 36F6D 6973 6f32
Data dalam biner :
00000000 00000000 00000000 00011100 01100110 01110100 01111001 01110000 01101001 01110011 01101111 01101101 00000000 00000000 00000010 00000000 01101001 01110011 01101111 01101101 01101001 01110011 01101111 0110010.

Data sebanyak 24 byte di atas diketahui 192 bit, untuk mencukupi 1024 bit ditambah bit-bit pengganjal (*padding bits*) sebanyak 824 dan 8 bit, karena pada SHA-2 memproses blok-blok bit yang berjumlah 120 blok atau 1024 bit. Bit pengganjal yang ditambahi dimulai bit 1 diikuti bit 0 selebihnya hingga urutan bit 979 Untuk 8 bit terakhir menyatakan jumlah karakter dalam notasi biner yaitu 128= 10000000.

Berikut ini adalah urutan blok-blok bit setalah ditambahkan :
00000000 00000000 00000000 00011100 01100110 01110100 01111001 01110000 01101001 01110011 01101111 01101101 00000000 00000000 00000010 00000000 01101001 01110011 01101111 01101101 01101001 01110011 01101111 00110010 01101101 01110000 00110100 00110001 00000000 00000000 00000000 00001000 01100110 01110010 01100101 01100101 00000000 10011000 10011011 00010000 01101101 01100100 01100001 01110100 00000000 00000000 00000001 10110011 00000000 00010000 00000111 00000000 00000000 00000001 10110110 00010000 01100000 01000101 10000010 11101000 01110110 00001111 10000111 11111111 10111010 10001100 00000001 01110111 00110001 11011000 00111110 00011111 11111110 11101101 10000000 00101110 11100001 10110000 01110010 00011111 10000011 11000001 11111111 11010110 11001101 00000110 00100101 01111011 01110010 00100100 10000111 01001101 00000011 00000110 10100110 00001011 01100001 00010011 00010010 01000011 10100110 10000001 10000011 01010011 00001111 00001000 10010110 00000001 01101100 00000111 00111100 10100000 10000001 01000001 10001010 11000100 01110000 01100000 11010001 **10000000**

Bit yang bercetak tebal adalah bit dari plainteks file video, bit 1 pada urutan ke 193 yang bercetak tebal adalah awal dari bit pengganjal dan dikuti bit-bit 0 dan 8 bit terakhir bercetak tebal adalah bit yang menyatakan jumlah 128.
B. Inisialisasi Penyangga Nilai Hash Message Diggest (MD)

Penyangga SHA-512 terdiri dari delapan yang setiap penyangga memiliki panjang 64 bit, berarti total 512 bit yaitu 8 x 64, dan dalam notasi HEX yaitu :

A = 6a09e667f3bcc908
B = bb67ae8584caa73b
C = 3c6ef372fe94f82b
D = a54ff53a5f1d36f1
E = 51e527fade683d1
F = 9b05688c2b3e6c1f
G = 1f83d9abfb41bd6b
H = 5be0cd19137e2179

Inisialisasi penyangga dalam biner, yaitu :

A = 6 a 0 9 e 6 6 7 f 3 b c c
9 0 8
= 0110 1010 0000 1001 1110 0110 0110 0111 1111 0011 1011 1100 1100
1001 0000 1000
B = b b 6 7 a e 8 5 8 4 c a
a 7 3 b
= 1011 1011 0110 0111 1010 1110 1000 0101 1000 0100 1100 1010
1010 0111 0011 1011
C = 3 c 6 e f 3 7 2 f e 9 4 f

8 2 b
= 0011 1100 0110 1110 1111 0011 0111 0010 1111 1110 1001 0100 1111
1000 0010 1011

D = a 5 4 f f 5 3 a 5 f 1 d
3 6 f 1
= 1011 0101 0100 1111 1111 0101 0110 1011 0101 1111 0001 1101
0110 1011 1111 0001

E = 5 1 0 e 5 2 7 f a d e 6 8
2 d 1
= 0101 0001 0000 1110 0101 0010 0111 1111 1010 1101 1110 0110 1000
0010 1101 0001

F = 9 b 0 5 6 8 8 c 2 b 3 e 6 c 1 f
= 1001 1011 0000 0101 0110 1000 1000 1100 0010 1011 0011 1110 0110 1100 0001 1111

G = 1 f 8 3 d 9 a b f b 4 1 b
d 6 b
= 0001 1111 1000 0011 1101 1001 1010 1011 1111 1011 0100 0001 1011
1101 0110 1011

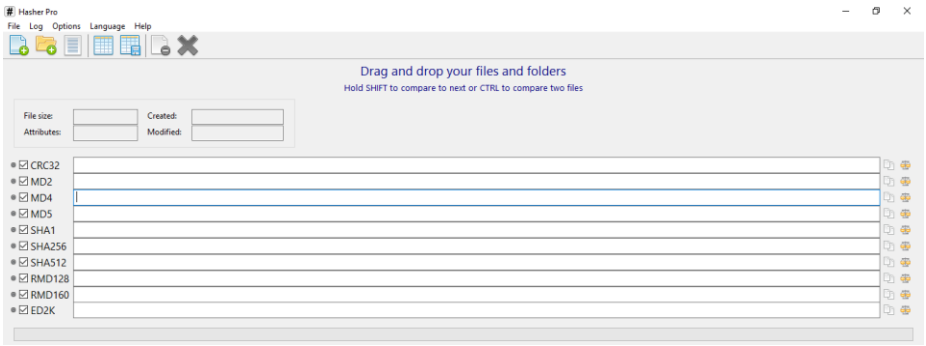
H = 5 b e 0 c d 1 9 1 3 7 e 2
1 7 9
= 0101 1011 1110 0000 1110 1101 0001 1001 0001 0011 0111 1110 0010
0001 0111 1001

C. Pengolahan Pesan Dalam Blok Berukuran 1024 Bit (Parsing)

Semua bit plainteks yang berjumlah 1024 bit dibagi 16 blok yang mana setiap satu blok berisi 64 bit bagian. Berikut adalah 16 blok bit tersebut :

3.1 Pengujian

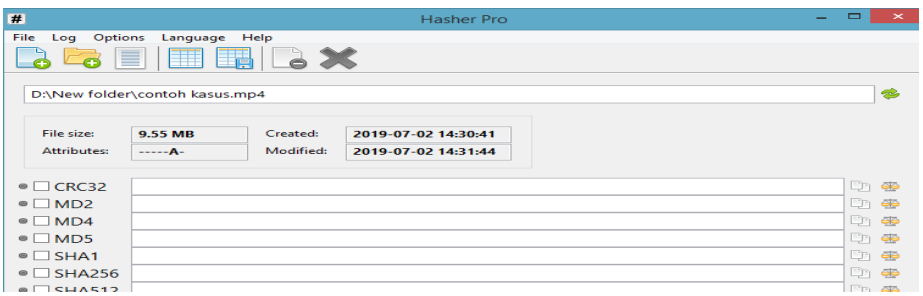
Aplikasi pengujian implementasi metode SHA-512 untuk medeteksi tanda tangan digital pada *file video* yang akan diuji merupakan hasil dari pembuatan kode fungsi *hash* dengan menerapkan metode SHA-512 yang digunakan. Berikut hasil dari implementasi metode SHA-512 untuk mendeteksi tanda tangan digital pada *file video* dengan menggunakan aplikasi *Hasher Pro* sebagai berikut:



Gambar 4. Aplikasi *Hasher Pro*

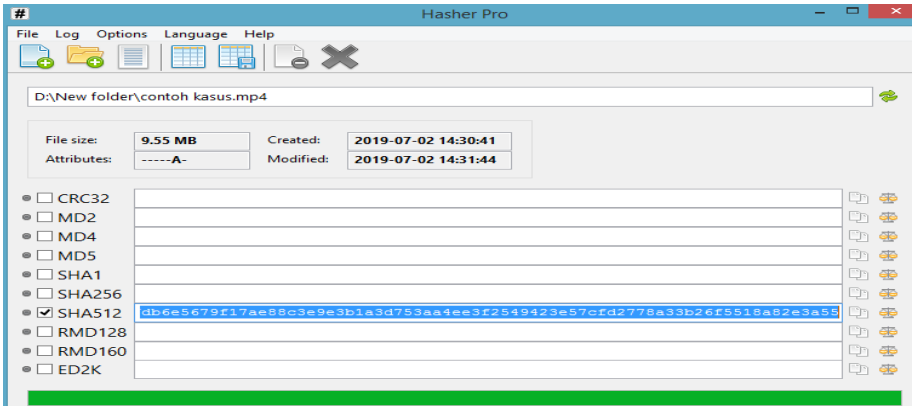
Pada *From* aplikasi *Hasher Pro* terdapat beberapa langkah yang dapat dilakukan *user* untuk menjalankan pengujian implementasi metode SHA-512 untuk mendeteksi tanda tangan digital pada *file video* diantaranya adalah sebagai berikut:

1. menginputkan tanda tangan digital pada *file video*
   Meninputkan tanda tangan digital pada *file video* adalah proses dimana memanggil tanda tangan digital pada *file video* yang akan dicari nilai SHA-512 seperti tampilan gambar 5:

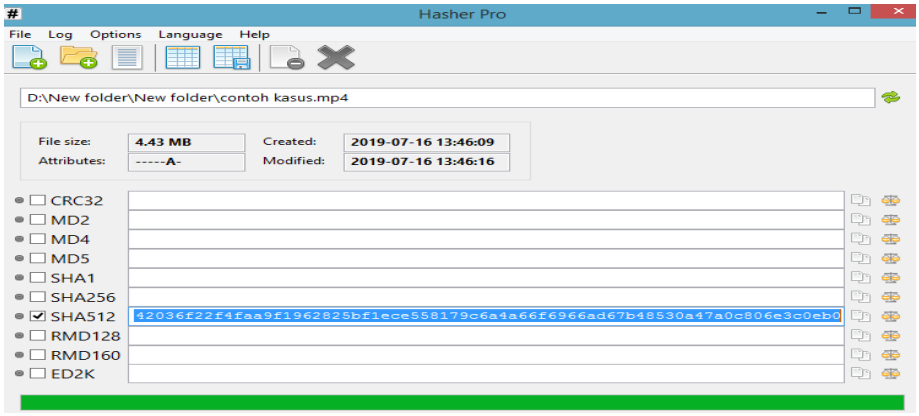


Gambar 5. Menginputkan *File* Awal

2. Memilih Metode SHA-512
   Memilih metode SHA-512 adalah proses dimana memilih metode yang akan digunakan untuk mendapatkan hasi dari metode SHA-512.



Gambar 5. Hasil SHA-512 Asli



Gambar 6. Hasil SHA-512 Editan

Dengan menggunakan aplikasi *Hasher Pro* pada pengujian implementasi metode SHA-512 untuk mendeteksi tanda tangan digital pada *file video* maka didapat sebuah hasil sebagai berikut:

Tabel 1. Hasil Implementasi

No	Nama Video Asli	Size	Hasil SHA-512	Nama Video Editan	Size	Hasil SHA-512
1	Contoh kasus	9,55	2E1BF4C05918F596BD9E2F A7EE61B5D6B216DE5A2B9 66013C370FBFFDB6E5679F 17AE88C3E9E3B1A3D753A A4EE3F2549423E57CFD277 8A33B26F5518A82E3A55	Contoh kasus	4,43 MB	9795EC32166CDA471CD98 E84B7D9E409AF7D9A0292 A6B1556751A48742036F22F 4FAA9F1962825BF1ECE558 179C6A4A66F6966AD67B48 530A47A0C806E3C0EB0

Dari hasil perbandingan meta data tanda tangan digital pada *file video* asli dan editan nyatakan berbeda berdasarkan kode dari metode yang didapatkan

4. KESIMPULAN

Berdasarkan dari penelitian yang telah dilakukan maka hasil akhir berdasarkan proses pengamanan tandatangan digital pada *file* video telah berhasil, dengan melakukan *hash* satu arah terhadap tanda tangan digital pada *file* Video. Penerapaan metode SHA-512 untuk tanda tangan digital pada *file* video telah membuktikan bahwa tanda tangan yang telah berubah akan menunjukan hasil yang berbeda dengan yang asli. Pengamanan tanda tangan digital pada *file* video dapat dilakukan dengan proses SHA-512 dengan menggunakan *Hash Pro*

REFERENCES

[1] A. Massey-omura, M. Reza, M. A. Budiman, and D. Arisandi, “Simulasi Pengamanan File Teks Menggunakan,” vol. 1, no. 1, pp. 20–27, 2012.

[2] T. Zebua, R. K. Hondro, and E. Ndruru, "Message Security on Chat App based on Massey Omura Algorithm," vol. 1, no. 2, pp. 16–23, 2018.
[3] I. Pendahuluan, "PENGAMANAN APLIKASI CHATTING MENGGUNAKAN METODE," vol. 12, no. September, pp. 295–300, 2017.
[4] A. Rohmanu, "Implementasi Kriptografi dan Steganografi Dengan Metode Algoritma Des dan Metode End Of File Ajar Rohmanu," *J. Inform. SIMANTIK*, vol. 1, no. 2, pp. 1–11, 2017.
[5] V. M. Amal and A. R. Yohannis, "Aplikasi Steganografi," pp. 77–88.