Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Implementasi Metode Sha-12 Untuk Mendeteksi Orisinalitas File Video

Serdima Siregar
Fakultas Ilmu Komputer, Teknik Informatika, Universitas Budidarma, Medan, Indonesia
Email: [1] serdimasiregar@gmail.com
Email Penulis Korespondensi: serdimasiregar@gmail.com

Abstrak− Seiring dengan perkembangan zaman yang semakin maju, serta didukung oleh perkembangan teknologi yang sangat pesat khususnya untuk menghasilkan file video untuk saat ini menghasilkan file video sangatlah mudah dengan bermacam merk handphone dan sangat banyak model-model kamera yang dapat digunakan untuk merekam video yang hampir dimiliki setiap orang.Video salah satu objek representasi data yang telah diolah. Bentuk data video merupakan hasil penggabungan dari pada gambar dan suara. Media video jugadapat diartikan seperangkat komponen atau media yang mampu menampilkan gambar sekaligus suara dalam waktu bersamaan. Kriptografi metode SHA-512 menghasilkan digest berukuran 512 bit dengan menggunakan iterasi terhadap blok pesan berukuran 1024 bit. Algoritma SHA-512 termasuk fungsi hash yang menghasilkan nilai hash terpanjang yaitu 512 bit.)

Kata Kunci : Kriptografi , Mendeteksi Otentikasi File Video, Metode SHA-512

Abstract− As times progress, and supported by very rapid technological developments, especially for producing video files, currently producing video files is very easy with various brands of cellphones and there are many models of cameras that can be used to record video, which almost everyone has. person. Video is one of the data representation objects that has been processed. The form of video data is the result of combining images and sound. Video media can also be interpreted as a set of components or media that is capable of displaying images and sound at the same time. The SHA-512 cryptography method produces a 512 bit digest using iteration over a 1024 bit message block. The SHA-512 algorithm includes a hash function that produces the longest hash value, namely 512 bits.)

Keywords: Cryptography, Detecting Video File Authentication, SHA-512 Method

1. PENDAHULUAN

Seiring dengan perkembangan zaman yang semakin maju, serta didukung oleh perkembangan teknologi yang sangat pesat khususnya untuk menghasilkan file video. untuk saat ini menghasilkan file video sangatlah mudah dengan bermacam merk handphone dan sangat banyak model-model kamera yang dapat digunakan untuk merekam video yang hampir dimiliki setiap orang.

Video salah satu objek representasi data yang telah diolah. Bentuk data video merupakan hasil penggabungan dari pada gambar dan suara. Media video juga dapat diartikan seperangkat komponen atau media yang mampu menampilkan gambar sekaligus suara dalam waktu bersamaan. video adalah teknologi untuk menangkap,merekam,memproses,mentransmisikan dan menata ulang gambar gerak. Biasanya menggunakan film,seluloid,sinyal elektronik atau media digital. Video juga bisa dikatakan sebagai gabungan gambar-gambar mati yang dibaca berurutan dalam suatu waktu dengan kecepatan tertentu.gambar-gambar yang digabung tersebut dinamakan frame dan kecepatan pembacaan gambar disebut dengan frame rate.

Otentikasi file video merupakan identifikasi yang dilakukan oleh masing-masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengindetifikasi satu sama lainya.“Video authentication in digital forensic [1] Informasi yang didapatkan oleh suatu pihak dari pihak lain harus diindetifikasi untuk memastikan keaslian dari informasi yang diterima .

Kriptografi adalah salah satu bidang yang paling berguna dibidang komunikasi nirkabel dan sistem komunikasi pribadi, dimana keamanan informasi telah menjadi bidang minat yang semakin penting.Hash adalah salah satu bagian dari kriptografi.Berdasarkan penelitian sebelumnya yang berjudul Pengamanan Sertifikat Tanah Digital Menggunakan Digital Signature SHA-512 dan RSA[2]SHA-512 merupakan variasi dari SHA-2. SHA-2 adalah perkembangan dari fungsi SH1 yang menjadi perbedaan adalah ukuran blok yang dipakai.

Fungsi hash SHA-512 menghasilkan digest berukuran 512 bit dengan menggunakan iterasi terhadap blok pesan berukuran 1024 bit. Algoritma SHA-512 ternmasuk fungsi hash yang menghasilkan nilai hash terpanjang yaitu 512 bit. Berdasarkan penelitian sebelumnya yang berjudul analisa algoritma SHA-512 dan watermaking. SHA merupakan singkatan Secure Hash Algorithm merupakan fungsi hash standard yang dipublikasikan oleh NIST (National Institute of Standard and Technology), [3], SHA diterbitkan dengan beberapa versi. SHA pada dasarnya Ide dasar dari fungsi hash adalah bahwa dibutuhkan pesan panjang variabel sebagai input dan menghasilkan pesan panjang tetap sebagai output yang juga bisa disebut sebagai hash atau pesan-digest. Trik di balik membangun fungsi hash kriptografi yang baik dan aman adalah untuk merancang fungsi kompresi yang baik di mana setiap bitinput mempengaruhi bit output sebanyak mungkin. Ini digunakan dengan Digital Signature Standard (DSA) untuk tanda tangan digital sehingga memiliki kepentingan tertentu. SHA-512dirancangsehinggapraktistidaklayakuntukmenemukanoutput daridua pesan input yang sama. Juga tidak mungkin untuk mendapatkan kembali pesan input dari intisari pesan yang diperoleh..

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

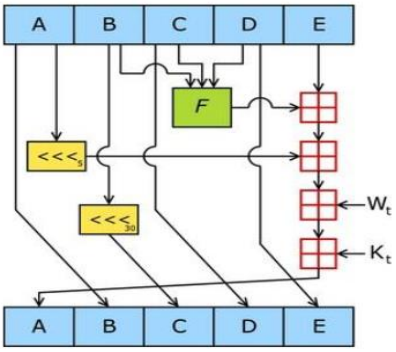
Gambar 3.1. Tahapan Peneliian

1. Identifikasi Masalah
   Identifikasi masalah dilakukan untuk menjelaskan dan mendefenisikan masalah-masalah yang dihadapi. Pada tahap ini juga dicari solusi atas masalah tersebut.
2. Pengumpulan Data
   Pengumpulan data dilakukan dengan mencari penelitian-penelitian terdahulu yang pernah dilakukan untuk mendukung penyelesaian masalah yang dihadapi.
3. Pengolahan data dengan Metode SHA-512
   Pengolahan data ini di lakukukan disaat data sudah terkumpul dan dilakukan pengujian dengan metode Metode SHA-512
4. Kesimpulan dan Saran
   Disini penulis menyimpulkan dari hasil penelitain yang ada dan memberikan saran yang tebaik.

2.6 Metode SHA-512

Fungsi hash SHA-512 merupakan versi SHA dengan ukuran digest 512 bit dan berbasis pada skema Merkle dan Damgrad. SHA merupakan singkatan Secure Hash Algorithm merupakan fungsi hash standard yang dipublikasi oleh NIST (National Institute of Standard and Technology), (NIST,1995 a) SHA diterbitkan dengan beberapa versi diantaranya SHA-1 dengan ukuran digest 160 bit, SHA-256 (ukuran digest 256 bit) dan SHA-512. Fungsi hash 512 merupakan versi yang terakhir dari SHA pada tahun 2012 NIST berencana menerbitkan SHA-3 meskipun SHA terdiri dari berbagai versi secara prinsip cara kerja fungsi hash SHA adalah sama.
Fungsi yang terjadi pada algoritma SHA-2 mirip dengan yang terjadi pada SHA-1. Proses yang terjadi pada SHA-512 adalah :
+ Sebelum pemrosesan
- Mengubah string masukan menjadi kumpulan bit 0 dan 1
- Penambahan bit ‘1’ ke pesan
- Penambahan k bit ‘0’,dimana k adalah nilai minimum
> = 0 sehingga pesan yang memiliki kelipatan 1024 bit
- Tambahkan panjang pesan, dalam bit, sebagai 64-bit integer.
+ Pada saat pemrosesan
- Memiliki 8 buah penyangga yang berukuran 64 bit
- Memiliki 80 buah konstanta yang berukuran 64 bit
- Bagi kumpulan bit setiap 1024 bit
- Pada tiap kumpulan 1024 bit tersebut, bagi tiap bit tersebut menjadi 16 bagian
- Perpanjang jadi 80 bagian, dengan menggunakan fungsi Gamma0 dan Gamma1
- Operasi yang terjadi pada tiap putaran adalah :

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT



Gambar 2 Cara kerja SHA-512

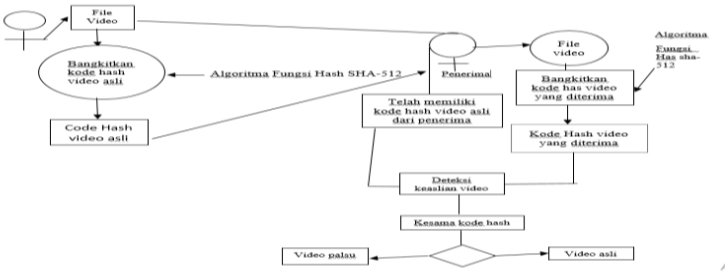
Nilai A sampai H adalah 8 buah penyangga yang telah ditentukan sebelumnya. Fungsi Maj yang ada pada gambar diatas adalah fungsi yang menerima 3 buah variabel dengan aturan melakukan operasi : (((A ∨ B) ∧ C) ∨ (A ∧ B)). Sedangkan fungsi Sigma0 adalah fungsi yang melakukan operasi : (ROR (x,28) ⊕ ROR (x,34) ⊕ ROR (x,39)). Yang dimaksud dengan ROR adalah rotasi bit yang ada ke kanan. Sehingga, yang terjadi pada fungsi Sigma0 adalah rotasikan x ke kanan sebanyak 2 kali , kemudian dilakukan operasi xor dengan x yang dirotasi ke kanan sebanyak 13 kali dan xor dengan x yang dirotasi kanan sebanyak 22 kali. Fungsi Sigma1 juga memiliki operasi yang mirip, yaitu : (ROR (x,14) ⊕ ROR (x,18) ⊕ ROR (x,41)).

Fungsi Gamma0 dan Gamma1 adalah fungsi yang dilakukan untuk memperbanyak jumlah potongan pada tiap bagian menjadi 80 bagian dari 16 bagian. Fungsi ini mirip dengan fungsi sebelumnya, yaitu fungsi Sigma0 dan Sigma1.Fungsi Gamma0 memiliki persamaan (ROR (x,1) ⊕ ROR (x,8) ⊕ R (x,7)). Fungsi R berbeda dengan fungsi rotasi kanan. Fungsi R merupakan fungsi untuk melakukan shift bit ke kanan sebanyak yang telah ditentukan. Sedangkan, fungsi Gamma1 memiliki persamaan (ROR (x,19) ⊕ ROR (x,61) ⊕ R (x,6)).

3. HASIL DAN PEMBAHASAN

3.1 Analisa Deteksi Keaslian File Video

Analisa deteksi keaslian sebuah file video sangat penting dilakukan mengingat pada kemajuan teknologi saat ini sangat banyak terjadi kasus-kasus penyalagunaan data termasuk video. Penyalahgunaan yang dimaksud seperti pemalsuan sebuah video sehingga orisinalitasnya akan hilang.Salah satu solusi yang dapat dilakukan untuk mengatasi permasalahan diatas adalah pemanfaatan teknik pendeteksian keaslian (orisinalitas) file video , dengan tujuan penerima data dapat membuktikan apakah video yang diterima asli atau palsu. Teknik deteksi orisinalitas data dalam ilmu keamanan data salah satunya adalah memanfaatkan perbandingan nilai atau kode hash dari sebuah data.
Pemilik video asli akan melakukan proses untuk menghasilkan kode hash dari sebuah video yang akan dikirimkan atau dibagikan kepada orang lain. Kode hash yang dihasilkan akan diberikan atau diberitahukan kepada orang lain (penerima video) dengan tujuan agar penerima dapat memastikan video yang diterima dari pengirim asli atau palsu.
Penerima video akan membangkitkan ulang kode hash dari video yang diterima, sehingga kode hash yang dihasilkan dibandingkan dengan kode hash yang pernah diterima nya dari pengirim. Bila kode hash yang dihasilkan oleh penerima sama dengan kode hash yang diberikan oleh pengirim, maka video yang diterimanya adalah asli, namun bila berbeda berarti video yang diterima telah mengalami perubahan atau telah dimonifikasi (palsu).
Proses deteksi keaslian file video dapat disajikan pada diagram bawah ini



Gambar 3. Deteksi Keaslian File Video

3.2 Contoh Kasus

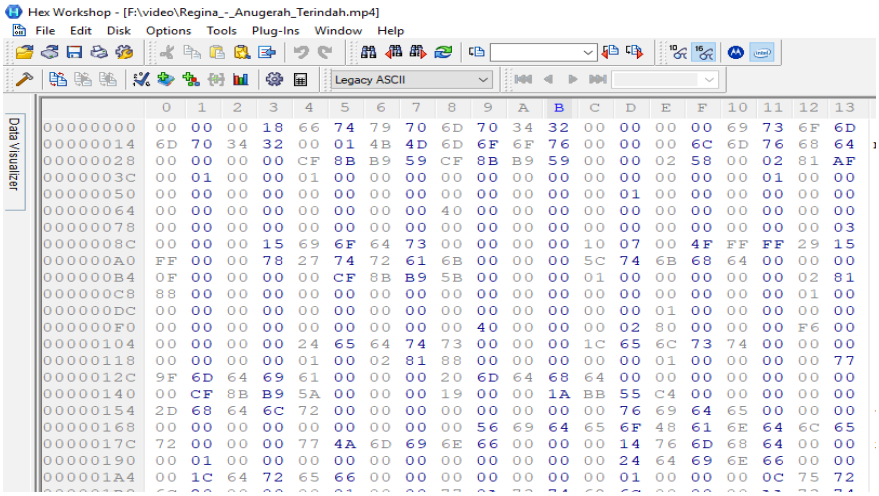
Contoh kasus dalam proses ini seperti dijelaskan dalam analisa yaitu file video MP4. data yang diambil hanya sebanyak 25 byte untuk plainteks, cara pengambilan nilai hex data video menggunakan aplikasi HexWorkShop dan langkah-langkahnya sebagai berikut:

1. Jalankan Aplikasi HexworkShop

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

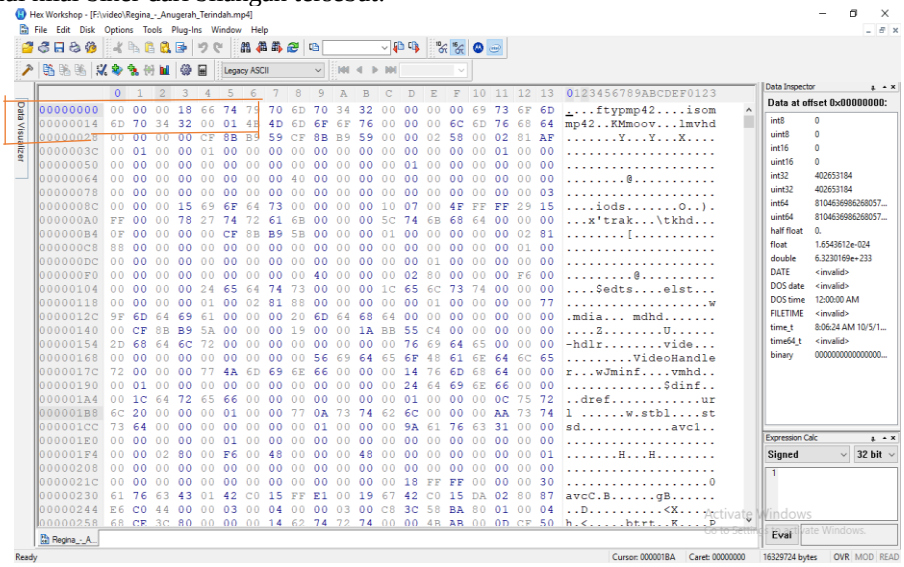
2. Klik menu File pilih Open
3. Telusuri dan pilih file video di drive harddisk dan klik OK

Gambar di bawah ini adalah data heksadesimal dari file video sha-512 menggunakan aplikasi HexWorkShop



Gambar 4. Data video

Dari data tersebut diambil sebanyak 25 byte atau 80 karakter heksadesimaldan dikonversi ke biner, yang berguna untuk mengetahui nilai biner dari bilangan tersebut.



Gambar 5. Sampel Data

Dari gambar data video di atas diambil sebanyak 25 byte untuk plainteks, yaitu :00 00 00 18 66 74 79 70 6D 70 34 6D 70 34 32 00 01 4B 4D 6D 6F 6F 00 00 00

A. Penambahan Bit-bit Pengganjal Dan Nilai Panjang Pesan Semula
Dari data yang digunakan sebagai plainteks diubah ke biner.
Heksadesimal: 00 00 00 18 66 74 79 70 6D 7034 6D 70 34 32 00 01 4B 4D 6D 6F 6F 00 0000

Data dalam biner :

00000000 00000000 00000000 00011000 01100110

01110100 01111001 01110000 01101101 01110000

01101000 01101101 01110000 00110100 00110010

00000000 00000001 01001011 01001101 01101101

01101111 01101111 00000000 00000000 00000000

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Berikut langkah- langkah perhitungan nilai videomengunakan metode SHA-512 yang terdiri dari 0 - 79 putaran.

1. Penambahan *padding* bit:

$ll + 1 + k = 896 \bmod 1024$

$\longrightarrow$ $25 \times 8 = 200$

Jadi, $l + 1 + k = 896 \bmod 1024 \longrightarrow 200 + 1 + k = 896 \bmod 1024$

$k = 896 - 201 \bmod 1024$

$k = 695 \bmod 1024$

$k = 695$

695

M = 11110111 11111000 11111010 11111010 1000000….0000

695 64

M = 11110111 11111000 11111010 11111010 1000000….0000….11001000

Lakukan penambahan bit sebanyak 695 dan penambahan panjang pesan sebanyak 64 bit.

$M^{(0)}$	11110111	11111000	11111010	11111010
	11111011	11111010	11111010	11111011
$M^{(1)}$	11111011	11111011	11111011	11111100
	11111100	11111100	11111101	11111101
$M^{(2)}$	11111101	11111100	11111100	11111100
	11111101	11111101	11111100	11111100
$M^{(3)}$	11111101	10000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(4)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(5)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(6)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(7)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(8)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(9)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(10)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(11)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(12)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(13)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(14)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000
$M^{(15)}$	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	11001000

Tabel 1 Hasil Nilai Penjadwalan Pesan dari Biner ke Hexadesimal

W0=f7f8fafafbfafafb	W21=bb4cb53eeb7ea000	W42=e1f8f118d61d780	W63=f5f6f9797a02f97b
W1=fbfbfbfcfcfcfdfd	W22=c1be0a3a45bbc0c8	W43=efad621e771fc8a0	W64=f5f6f9797a79f97b
W2=fdfcfcfcfdfdfcfc	W23=70d10dc95a21f97b	W44=1f8f118d61d780c8	W65=1536f9797a79f97b
W3=fd80000000000000	W24=33c81ac764e6ddf5	W45=d8054b1e14ad2202	W66=12ef35dc271f4c48
W4=0000000000000000	W25=c97c2de7974aba7c	W46=40d8054b1e14ad00	W67=12ef35dc271f4780
W5=0000000000000000	W26=c81fd33a28227a80	W47=866d46dd1b754e00	W68=12ef35dc271f52c8
W6=0000000000000000	W27=b908026636458e00	W48=6d46dd1b754e0000	W69=10edb5dc271f40c8

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

W7=0000000000000000	W28=597244d8c81d4000	W49=ad621e771fc8a000	W70=12eff5fc271f40c8
W8=0000000000000000	W29=12ef35dc271f40c8	W50=cfab5138a9785175	W71=96af35dc271f46c8
W9=0000000000000000	W30=eb2884a16172a70b	W51=12ef35dc271f40d0	W72=f2ef35dc271f47c8
W10=0000000000000000	W31=2f5ca1f0d86d4534	W52=52ef35dc271f4040	W73=32ef35dc271f0000
W11=0000000000000000	W32=74bf6e1c4c49cf21	W53=33c81ac764e6dd80	W74=cf8b513829785100
W12=0000000000000000	W33=cf8b513829785175	W54=33c81ac764e6ddc8	W75=cf8b513829780000
W13=0000000000000000	W34=866d46dd1b754ec0	W55=a333c81ac764e6dd	W76=5b3f59784e7ae483
W14=0000000000000000	W35=11eb172ed451f880	W56=74bf6e1c4c49cfa9	W77=5b3f59784e7ae48c
W15=00000000000000c8	W36=65efad621e771fc8	W57=54bb6e5c4c49cf21	W78=5b3f59784e7ae480
W16=f5f6f9797a79f97b	W37=318622954a9a6d1b	W58=74bf6e1c4c49cf00	W79=1f8f118d61d780c8
W17=f5777777fc36abf5	W38=5a3f8dd006f72c72	W59=74bf6e1c4c49c021	
W18=8f728a8e53a45bbc	W39=463afebfd12dc3c6	W60=74a16e1c4c49cf21	
W19=43e23c4a5202fd40	W40=40d8054b1e14ad22	W61=f5f6f9797a790000	
W20=b333c81ac764e6dd	W41=162974cce6f10202	W62=15d6f9797a79f97b	

Tabel 2 hasil Menginisialisasi 5 variabel

	a / e	**b / f**	**c / g**	**d / h**
Int	b4eb11bc77cb57aa	6a09e667f3bcc908	bb67ae8584caa73b	510e527fade682d1
	9a7d6eac01412bd8	510e527fade682d1	9b05688c2b3e6c1f	1f83d9abfb41bd6b
T1	f56dc7fddeb5c3a4	b4eb11bc77cb57aa	6a09e667f3bcc908	bb67ae8584caa73b
	5b6597ac5e43ceb7	9a7d6eac01412bd8	510e527fade682d1	9b05688c2b3e6c1f
T2	7fc551d1ca0e9df6	f56dc7fddeb5c3a4	b4eb11bc77cb57aa	6a09e667f3bcc908
	f4fde75aa7f3d0e2	5b6597ac5e43ceb7	9a7d6eac01412bd8	510e527fade682d1
T3	c7c2d9a95d13e495	7fc551d1ca0e9df6	f56dc7fddeb5c3a4	b4eb11bc77cb57aa
	7e4784ae17f655c4	f4fde75aa7f3d0e2	5b6597ac5e43ceb7	9a7d6eac01412bd8
T4	3eea2b2447ac4bb1	c7c2d9a95d13e495	7fc551d1ca0e9df6	f56dc7fddeb5c3a4
	946c0f0484699bbd	7e4784ae17f655c4	f4fde75aa7f3d0e2	5b6597ac5e43ceb7

Lanjutan T5

T5	a61487db1feb90ef	3eea2b2447ac4bb1	c7c2d9a95d13e495	7fc551d1ca0e9df6
	bfd9d5f7a41dee55	946c0f0484699bbd	7e4784ae17f655c4	f4fde75aa7f3d0e2
T6	d05b09cfe3bbd1c	a61487db1feb90ef	3eea2b2447ac4bb1	c7c2d9a95d13e495
	2a3fe5e1bd382286	bfd9d5f7a41dee55	946c0f0484699bbd	7e4784ae17f655c4
T7	dcaf0adc4cfec27	d05b09cfe3bbd1c	a61487db1feb90ef	3eea2b2447ac4bb1
	56c5d359de9b86d5	2a3fe5e1bd382286	bfd9d5f7a41dee55	946c0f0484699bbd
T8	922cc5cfc7353a7a	dcaf0adc4cfec27	d05b09cfe3bbd1c	a61487db1feb90ef

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

	bfc1130bfb85120c	56c5d359de9b86d5	2a3fe5e1bd382286	bfd9d5f7a41dee55
T9	f6833da30a3c7821	922cc5cfc7353a7a	dcaf0adc4cfec27	d05b09cfe3bbd1c
	7eb802097bd083d1	bfc1130bfb85120c	56c5d359de9b86d5	2a3fe5e1bd382286
T10	29c5934b6bcd4122	f6833da30a3c7821	922cc5cfc7353a7a	dcaf0adc4cfec27
	6f88299f0f9014be	7eb802097bd083d1	bfc1130bfb85120c	56c5d359de9b86d5
T11	5b3e213e47a224e1	29c5934b6bcd4122	f6833da30a3c7821	922cc5cfc7353a7a
	13684096ececf36b	6f88299f0f9014be	7eb802097bd083d1	bfc1130bfb85120c
T12	743ccd6693c6107e	5b3e213e47a224e1	29c5934b6bcd4122	f6833da30a3c7821
	8fdd60e9d16e2a0c	13684096ececf36b	6f88299f0f9014be	7eb802097bd083d1
T13	45f4036d6438a50b	743ccd6693c6107e	5b3e213e47a224e1	29c5934b6bcd4122
	73c47ec31fda1abf	8fdd60e9d16e2a0c	13684096ececf36b	6f88299f0f9014be
T14	254644c89afa6da5	45f4036d6438a50b	743ccd6693c6107e	5b3e213e47a224e1
	5fbce2fe99ac9c1d	73c47ec31fda1abf	8fdd60e9d16e2a0c	13684096ececf36b
T15	eb712651d9a9fda2	254644c89afa6da5	45f4036d6438a50b	743ccd6693c6107e
	549a70c790968f03	5fbce2fe99ac9c1d	73c47ec31fda1abf	8fdd60e9d16e2a0c

Lanjutan T16

T16	317c19e5e0077dcc	eb712651d9a9fda2	254644c89afa6da5	45f4036d6438a50b
	72af9d1e39bf0c0	549a70c790968f03	5fbce2fe99ac9c1d	73c47ec31fda1abf
T17	bdd010785e1a53c5	317c19e5e0077dcc	eb712651d9a9fda2	254644c89afa6da5
	81ed6fe4c74ff01b	72af9d1e39bf0c0	549a70c790968f03	5fbce2fe99ac9c1d
T18	e159b06248534bd5	bdd010785e1a53c5	317c19e5e0077dcc	eb712651d9a9fda2
	25f3196970909551	81ed6fe4c74ff01b	72af9d1e39bf0c0	549a70c790968f03
T19	68564ee80eb498d2	e159b06248534bd5	bdd010785e1a53c5	317c19e5e0077dcc
	f36aa25f64318f0f	25f3196970909551	81ed6fe4c74ff01b	72af9d1e39bf0c0
T20	9237f0df340a25ae	68564ee80eb498d2	e159b06248534bd5	bdd010785e1a53c5
	2e30a8874226b9c3	f36aa25f64318f0f	25f3196970909551	81ed6fe4c74ff01b
T21	2b2f85c4a24bf3f1	9237f0df340a25ae	68564ee80eb498d2	e159b06248534bd5
	26f5d58efddca308	2e30a8874226b9c3	f36aa25f64318f0f	25f3196970909551
T22	52366d496155b54	2b2f85c4a24bf3f1	9237f0df340a25ae	68564ee80eb498d2
	66b204f68944077d	26f5d58efddca308	2e30a8874226b9c3	f36aa25f64318f0f
T23	33c79ecf63e784fa	52366d496155b54	2b2f85c4a24bf3f1	9237f0df340a25ae

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

	b3bf665c3c686e1f	66b204f68944077d	26f5d58efddca308	2e30a8874226b9c3
T24	59cb1f56d0fe06f5	33c79ecf63e784fa	52366d496155b54	2b2f85c4a24bf3f1
	45afcb918bb9ff86	b3bf665c3c686e1f	66b204f68944077d	26f5d58efddca308
T25	2847bea516df3900	59cb1f56d0fe06f5	33c79ecf63e784fa	52366d496155b54
	6143968a2c7a8bd	45afcb918bb9ff86	b3bf665c3c686e1f	66b204f68944077d
T26	9de64992f902eb1c	2847bea516df3900	59cb1f56d0fe06f5	33c79ecf63e784fa
	d6934e9d4dc439dc	6143968a2c7a8bd	45afcb918bb9ff86	b3bf665c3c686e1f

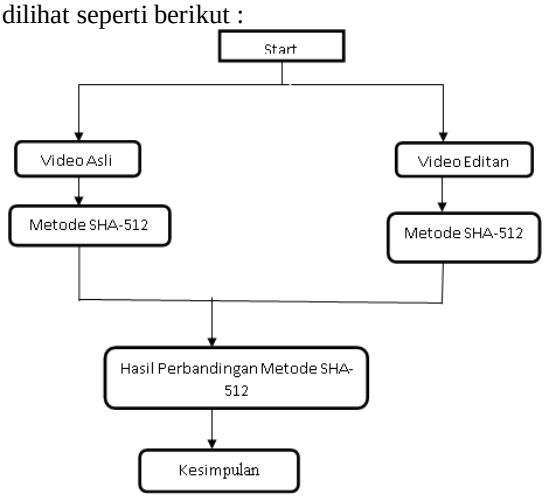
Tabel 3 Hasil Nilai SHA-512

56edc6a5f2c816e5
a5d2e686ecefa166
c67daa1f653ccd03
2ac79c3693e7e69d
de4ebe91953adcec
b6b2cfbc42ab9520
595c1360f4b6d181
775bf9473da8128b

Berdasarkan dari perhitungan di atas diperoleh nilai SHA-512 berbentuk bilangan hexadesimal 8 karakter 128 byte, yaitu " 56edc6a5f2c816e5, a5d2e686ecefa166, c67daa1f653ccd03, 2ac79c3693e7e69d, de4ebe91953adcec, b6b2cfbc42ab9520, 595c1360f4b6d181, 775bf9473da8128b". Jadi nilai *hash value* yang terakhir adalah nilai yang didapat merupakan file video tersebut. Jika terjadiperubahan sedikit saja maka nilai ini akan berubah sehingga jika nilainya berubah maka file video tersebut telah di manipulasi.

3.3 Pembahasan Mendeteksi Keaslian *Video*

Pengujian dalam mendeteksi keaslian *video* diperlukan karena dengan adanya pengujian kita dapat mengetahui hasil dari perbedaan dari *video* asli dan *video* yang telah dirubah. Pengujian mendeteksi keaslian *video* yang akan diuji merupakan hasil dari pembentukan kode *fungsi Hash*dengan menerapkan metode SHA-512 yang digunakan. Sehingga kita akan dapat melihat kekurangan dan perubahan dari file video asli dan yang telah dirubah Adapun prosedur mendeteksi keaslian *video* dapat dilihat seperti berikut :



Gambar 6. Pembahasan Mendeteksi Keaslian Video

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Tabel 7: Hasil Deteksi Otentikasi video

No	Nama Video Asli	Hasil Metode	Nama Video Editan	Hasil Metode	Kesimpulan
1.	Anugerah Terindah	56edc6a5f2c816e5 a5d2e686ecefa166 c67daa1f653ccd032ac79c3693e7e69dde4ebe91953adcecb6b2cfbc42ab9520595c1360f4b6d181775bf9473da8128b	Anugerah terindah	99C7D06BEE1A9BB8A4D68022BF49F856151E6C58CD4FA9D11AEE4DF869956F588d406c11e7545a1b1BAD6730176D2901E55EE733E3B45056 8DF4B0B8E8A5C448	DariHasil Perbandingan metadata *file video* Asli dan editan dinyatakan berbeda berdasarkan kode dari metode yang di dapatkan.

Berdasarkan data hasil pengujian mendeteksi keaslian file video menggunakan metode SHA-512menunjukkan bahwa perubahan sekecil apapun sangat mempengaruhi hasil dari pendeteksi atau keaslian dari *file* tersebut sehing tingkat akurat dari perbedaan *file audio* asli dan yang telah di edit sangat besar perbedaanya.

4. KESIMPULAN

Setelah dilakukan pengujian dan analisas sistem, Maka dapat diperoleh simpulan sebagai berikut :

a Dengan Penererapan Metode SHA-512 audio akan mudah terdeteksi dan mengetahui audio tersebut asli atau editan.
b Dengan Perancangan aplikasi deteksi keaslian file video Menggunakan Microsoft Visual Basic Net 2008 ,maka dapat diketahui bahwa Dengan menggunakan hash pada metode SHA-512 yang akan menghasilkan video asli atau video editan.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

REFERENCES

[1] P. G. F. M. C. Q. F. R. Rigoni, ""Tampering detection of audio-visual content using encrypted watermarks,"," "Tampering detection of audio-visual content using encrypted watermarks,", p. 8, 2014.

[2] NIST, national institute of standart and Technology, American : Dede Djuhana, Ph.D, 1999.
[3] W. Dai, "Speed Benchmarks for Various Ciphers and Hash Functions.," algoritma SHA-512, 2009.
[4] Yeni Agusti, "PERANCANGAN," PERANCANGAN APLIKASI PEMBELAJARAN FISIKA TINGKAT, p. 6, 2013.
[5] Donny Yulianto, "Tahapan Perancangan," ANALISIS & PERANCANGAN SISTEM, p. 40, 2015.
[6] Mariyana, "Langkah-langkash dalam tahap perencanaan sistem," Langkah-langkash dalam tahap perencanaan sistem, p. 8, 2015.
[7] s. sembiring, "PERANCANGAN SISTEM INFORMASI PEMBELIAN PADA PT. TEKNOTAMA LINGKUNGAN INTERNUSA," PERANCANGAN , p. 31, 2013.
[8] R. A. d. M. Shalahudin, " Rekayasa Perangkat Lunak Struktur dan Berorientasi Objek," Rekayasa Perangkat Lunak Struktur dan Berorientasi Objek, p. 10, 2014.
[9] P. P. Widodo, "UML," VOL.I NO.1 FEBRUARI 2015JURNAL TEKNIK KOMPUTER AMIK BSI11ISSN. 2442-2436 // SISTEM PAKAR PENDETEKSIAN ....SISTEM PAKAR PENDETEKSIAN PERMASALAHAN KOMPUTER PADA PT. PASIFIK SATELIT NUSANTARA CIKARANG, 2011.
[10] Indraja, "Bagian alir (Flowchart)," Penggunaan Citra Penginderaan Jauh untuk Mendukung Mitigasi Dampak Perubahan Iklim di Sektor Pertanian, p. 14, 2015.
[11] Wicaksono, "deteksi," deteksi, p. 17, 2013.
[12] Nurasyiah, " Struktur File WAV dalam bentuk Hexa," Struktur File WAV dalam bentuk Hexa, p. 7, 2013.
[13] Nurasyiah, " Perancangan Aplikasi Kompresi File," APLIKASI KEAMANAN FILE AUDIO WAV (WAVEFORM) DENGAN, p. 7, 2013.

Buletin Ilmiah Informatika Teknologi
Vol 2, No 2, Januari 2024, Hal. 70 - 79
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

[14] D. Arius, "Pengantar Ilmu Kriptografi," Jurnal Teknik Informatika Kaputama (JTIK), Vol 1 No 1, Januari 2017ISSN :2548-97041PERANCANGAN APLIKASI KEAMANAN PESAN MENGGUNAKAN ALGORITMA ELGAMAL DENGAN MEMANFAATKAN ALGORITMA ONE TIMEPADSEBAGAI PEMBANGKIT KUNCI, p. 7, 2008.
[15] R. Sadikin, " Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java," Perbandingan, p. 5, 2012.
[16] R. Munir, " Kriptografi," PEMANFAATAN KRIPTOGRAFI DALAM MEWUJUDKAN KEAMANAN INFORMASI PADA e-VOTING DI INDONESIA, p. 7, 2006.
[17] Novi dian Natasyah,anang eko wicaksono, "Penerapan Teknik Kriptografi Stream Cipher Untuk Pengaman Basis Data," Penerapan Teknik Kriptografi Stream Cipher Untuk Pengaman Basis Data, p. 22, 2011.
[18] D. Arius, "Pengantar Ilmu Kriptografi," KRIPTOGRAFI FILE CITRA MENGGUNAKAN, p. 23, 2018.