Buletin Ilmiah Informatika Teknologi
Vol 1, No 1, September 2022, Hal. 8 - 14
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Aplikasi Deteksi Keaslian File Audio Dengan Menerapkan Metode SHA-512

Mawan Br Hutahaean
Fakultas Ilmu Komputer, Teknik Informatika, Universitas Budidarma, Medan, Indonesia
Email: mawanhutahaean121@yahoo.com
Email Penulis: mawanhutahaean121@yahoo.com

Abstrak− Dalam era teknologi informasi yang berkembang sangat pesat.audio sangat sering digunakan untuk barang bukti oleh pihak hokum, seiring munculkannya kebutuhan otentikasi suatu data atau berkas yang digunakan secara digital. audio adalah suatu skema matematika untuk menunjukkan keaslian suara digital atau rekaman. Sebuah audiohanya valid memberikan alasan untuk percaya bahwa penerima audio yang dibuat oleh pengirim yang diketahui, bahwa itu tidak diubah dalam perjalanan. Metode Secure Hash Algoritma (SHA-512) yang merupakan algoritma hash dari jenis SHA-512 yang menghasilkan message digest sepanjang 256 bit. Algoritma SHA-512dapat digunakan untuk melakukan pengecekan integritas data, pembuatan digital signature, dan lain-lain.

Kata Kunci: Deteksi, File Audio, SHA-512

Abstract− In the era of information technology that is developing very rapidly, audio is often used as evidence by legal parties, along with the emergence of the need to authenticate data or files that are used digitally. audio is a mathematical scheme for indicating the authenticity of digital or recorded sound. A valid audioonly gives reason to believe that the audio receiver is made by a known sender, that it was not modified in transit. The Secure Hash Algorithm (SHA-512) method is a hash algorithm of the SHA-512 type that produces a 256-bit message digest. The SHA-512 algorithm can be used to check data integrity, create digital signatures, and so on.

Keywords: Detection, Audio Files, SHA-512

1. PENDAHULUAN

Audio adalah suara atau bunyi yang di hasilkan oleh getaran suatu benda, agar dapat tertangkap oleh telinga manusia. Audio sering kali disalah gunakan oleh pihak-pihak yang tertentu untuk memanipulasi sebuah rekaman dengan memalsukan file audio. File audio merupakan salah satu alat bukti digital yang biasanya dimanipulasi untuk menghilangkan bukti-bukti yang ada didalamnya.

Keaslian file audio pada saat ini menjadi hal yang sangat penting dan terus berkembang. Karena itu audio sangat penting untuk dijadikan sebagai sumber utama informasi. Berbagai software editing audio menyulitkan seseorang untuk membedakan antara audio otentik atau audio.Berikut ini adalah beberapa contoh peristiwa mengapa mendeteksi pemalsuan audio diperlukan: Sebuah frame audio dapat dirusak atau dirubah dengan berbagai cara, hal itu digunakan untuk mencemarkan nama baik seseorang. Penjahat sering dibebaskan karena adannya audio (yang digunakan sebagai barang bukti), yang menunjukkan kejahatan mereka tidak bisa digunakan karena audio tersebut telah dimanipulasi

Untuk membedakan audio asli atau audio tampering maka diperlukan pendeteksian terhadap audio tersebut Metode yang digunakan untuk mendeteksi audio secara umum dibedakan menjadi dua kategori kategori pertama adalah tampering detection, yaitu metode deteksi yang hanya mengecek integritas dari audio tanpa menunjukkan bagian mana pada audio yang telah dimanipulasi. Namun tidak dapat memberikan informasi lokasi mana yang telah dimanipulasi pada audio. Kategori kedua adalah tampering localization, yaitu metode deteksi yang menunjukkan bagian pada Audio yang telah dimanipulasi. Berbeda dengan tampering detection yang hanya mengecek validasi dari sebuah Audio, pada metode tampering localization ini kita dapat menunjukkan bagian pada audio yang telah dimanipulasi. Lokasi manipulasi berupa posisi spasial dalam bentuk koordinat pixel dan posisi temporal dalam bentuk urutan frame yang telah dimanipulasi. Penelitian tentang mendeteksi audio tampering telah banyak dilakukan oleh peneliti sebelumnya, seperti yang dilakukan oleh penelitian tampering. [1] Mendeteksi adalah menemukan untuk menentukan dan melacak keberadaan file audio. Keamanan dalam mendeteksi keaslian audio adalah hal sangat penting dan tidak bisa diabaikan. Akhirnya yang mengembangkan berbagai cara untuk mengatasi persoalan, dan bagaimana cara untuk medeteksi keaslian file audio tersebut.

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. Kriptograpi menangani informasi spesifik tentang persyaratan keamanan seperti integritas data, kerahasian, dan ontentikasi asal data. SHA adalah standar kompres terkenal yang digunakan dalam kriptografi komputer. SHA merupakan singkatan Secure Hash Algoritma merupakan fungsi Hash Standart yang dipublikasikan oleh NIST (National Institute of Standart and Technology)[2].

Fungsi Hash SHA-512 menghasilakan digest berukuran 512 bit dengan menggunakan iterasi terhadap blok pesan berukuran 1024 bit. Algoritma SHA-512 termasuk fungsi hash yang meghasilkan nilai hash terpanjang yaitu 512 bit. Berdasarkan penelitian sebelumnya yang berjudul analisis algoritma sha-512 dan watermarking dengan metode leastsignificant[3]

SHA-512 berbeda dari SHA - 0 hanya dengan rotasi bitwise tunggal dalam jadwal pesan dari fungsi kompresinya. ini dilakukan oleh NSA untuk memperbaiki kesalahan pada algoritma asli yang mengurangi keamanan kriptografiknya.

Buletin Ilmiah Informatika Teknologi
Vol 1, No 1, September 2022, Hal. 8 - 14
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

2. METODOLOGI PENELITIAN

2.1 Perancangan

Proses perancang atau pengembangan perangkat lunak menjadi perhatian yang serius selama decade terakhir. Mendefinisikan proses perancangan perangkat lunak sebagai sebuah kerangka kerja untuk tugas-tugas yang dibutuhkan untuk membangun perangkat lunak dengan kualitas yang tinggi. Proses perangkat lunak menentukan pendekatan perangkat lunak dengan kualitas yang tinggi.
Perancangan adalah penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam satu kesatuan yang utuh dan berfungsi. Perancangan sistem dapat dirancang dalam flowchart, yang merupakan alat bentuk grafik yang dapat digunakan untuk menunjukan urutan-urutan proses [4].
Tahapan perancangan mempunyai dua tujuan utama [5] yaitu sebagai berikut.

a. Untuk memenuhi kebutuhan kepada pemakai sistem aplikasi
b. Untuk memeberikan gambaran yang jelas dan rancang bangun yang lengkap kepada pemograman komputerdan ahli-ahli lainya yang terlibat.

Beberapa langkah-langkah dalam tahap perencanaan sistem [6] yaitu sebagai berikut :

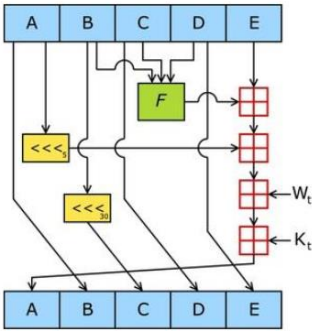
a. Menyiapkan rancangan sistem yang terinci.
b. Mengidentifikasi berbagai alternative konfigurasi sistem.
c. Mengevaluasi berbagai alternatif konfigurasi sistem.
d. Memilih konfigurasi yang terbaik.
e. Menyiapkan usulan penerapan.
f. Menyetujui atau menolak penerapan sistem.

2.2 Aplikasi Hasher Pro

Hasher Pro adalah suatu aplikasi yang digunakan untuk memverifikasi memverifikasi integritasfile menggunakan beragam algoritma seperti CRC32, MD2, MD4, MD5, SHA1, SHA256, SHA512, RipeMD128, RipeMD160, ED2K. Hasher Pro merupakan solusi yang tepat sebagai media untuk perbandingan yang memberikan banyak fitur dan kemudahan. Dengan fungsi perbandingan hash dan file yang mudah, seperti memegang SHIFT untuk membandingkan dengan file berikutnya atau CTRL untuk membandingkan dua file dengan membuat suatu kode berdasakan algoritma yang digunakan[9]

2.3 Algoritma SHA-512

Algoritma SHA-512 adalah algoritma yang menggunakan fungsi hash satu arah yang diciptakan oleh Ron Rivest. Algoritma merupakan pengembangan dari algoritma-algoritma sebelumnya yaitu algoritma SHA-0, SHA-1, SHA-256 dan algoritma SHA-384.
Cara kerja kriptografi algoritma SHA-512 adalah menerima input berupa pesan dengan ukuran sembarang dan menghasilkan message diggest yang memiliki panjang 512 bit. Berikut illustrasi gambar dari pembuatan message diggest pada kriptografi algoritma SHA-512 :



Gambar 1. cara kerja SHA-512

Langkah-langkah pembuatan message digest dengan algoritma SHA-512 [sumber] adalah sebagai berikut:

1. Penambahan Bit-bit PengganjalProses pertama yang dilakukan adalah menambahkan pesan dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 896 mod 1024 Ini berarti setelah menambahkan bit-bit pengganjal, kini panjang pesan adalah 128 bit kurang dari kelipatan 1024. Hal yang perlu diingat adalah angka 1024 muncul karena algoritma SHA-512 memproses pesan dalam blok-blok yang berukuran 1024.Apabila terdapat pesan dengan panjang 24 bit, maka pesan tersebut akan tetap ditambahkan dengan bit-bit pengganjal. Pesan akan ditambahkan dengan 896 - (24 + 1) = 871 bit. Jadi panjang bit-bit pengganjal adalah antara 1 sampai 896. Lalu satu hal lagi yang perlu diperhatikan adalah bahwasanya bit-bit pengganjal terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0.

Buletin Ilmiah Informatika Teknologi
Vol 1, No 1, September 2022, Hal. 8 - 14
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

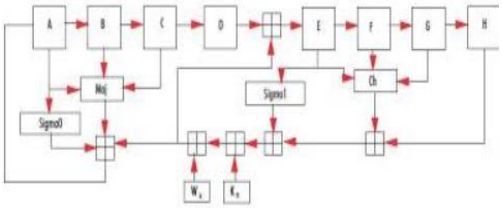
2. Penambahan Nilai Panjang PesanSemulaKemudian proses berikutnya adalah pesan ditambah lagi dengan 128 bit yang menyatakan panjang pesan semula. Apabila panjang pesan lebih besar dari 2128 maka yang diambil adalah panjangnya dalam modulo 2128. Dengan kata lain, jika pada awalnya panjang pesan sama dengan K bit, maka 128 bit yang ditambahkan menyatakan K modulo 2128. sehingga setelah proses kedua ini selesai dilakukan maka panjang pesan sekarang adalah 1024 bit.
3. Inisialisasi Nilai HashPada algoritma SHA-512 nilai Hash, H(0) terdiri dari 8 words dengan besar 64 bit dalam notasi hexadesimal sebagai berikut :

Tabel 1. Notasi Heksadesimal SHA 512

Penyangga	Nilai awal ()
A	6a09e667f3bcc908
B	bb67ae8584caa73b
C	3c6ef372fe94f82b
D	a54ff53a5f1d36f1
E	510e527fade682d1
F	9b05688c2b3e6c1f
G	1f83d9abfb41bd6b
H	5be0cd19137e2179

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 :



Gambar 2. Operasi fungsi hash SHA-512

Nilai A sampai H adalah 8 buah penyangga yang telahditentukan sebelumnya. Fungsi Maj yang ada pada gambar diatas adalah fungsi yang menerima 3 buah variabel dengan aturan melakukan operasi (((A ∨ B) ∧C) ∨ (A ∧ B)). ([25]

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 memilikioperasi 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))

Pada gambar terlihat ada Wx dan Kx. Yang dimaksud dengan nilai Kx adalah nilai konstanta yang telah ditentukan pada tiap putaran. Sedangkan, nilai Wx adalah nilai dari tulisan yang akan di-hash yang sudah ditambah bitnya dan diperpanjang ukurannya sampai 80 buah potongan. Untuk mendapatkan nilai W ke 16 sampai dengan 79 (jika nilai W pertama adalah nilai W ke 0), operasi yang dilakukan adalah melakukan operasi penambahan antara Gamma1 dari W[i-2] dengan W[i-7] dan juga ditambah dengan hasil penjumlahan antara Gamma0 dari W[i-15] dan W[i-16] Kemudian, terdapat juga fungsi Ch. Fungsi ini melakukan operasi (G ⊕ (E ∧ (F ⊕ G))).

Buletin Ilmiah Informatika Teknologi
Vol 1, No 1, September 2022, Hal. 8 - 14
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Setelah melakukan operasi-operasi yang ada, nilai selanjutnya dapat ditentukan. Penentuan nilai selanjutnya dilakukan dari H sampai ke A. Nilai H ditentukan dari nilai G, nilai G ditentukan dari nilai F, nilai F ditentukan dari nilai E, nilai E ditentukan dari penjumlahan dari D dan operasi penjumlahan, nilai D ditentukan dari nilai C, nilai C ditentukan dari nilai B,nilai B ditentukan dari nilai A,dan nilai A diperoleh dari penjumlahan. Fungsi hash diperoleh dengan menggabungkan nilai-nilai hasil penjumlahan sebelumnya. Fungsi hash SHA-512 melakukan operasi hash yang sama dengan operasiSHA-2 pada umumnya.
Yang menjadi perbedaan dengan algoritma hash SHA-2 yang lainnya adalah angkanya memiliki panjang 64 bit, sedangkan SHA-256 hanya memiliki panjang 32 bit. Selain itu, pada SHA-512 terdapat 80 buah putaran, sedangkan SHA-256 hanya memiliki 64 putaran. Pada SHA-512, nilai 8 buah penyangganya dan konstanta penambahnya diperpanjangmencapai 64 bit. Operasi shift dan rotasi yang dilakukan pada SHA-512 juga berbeda.

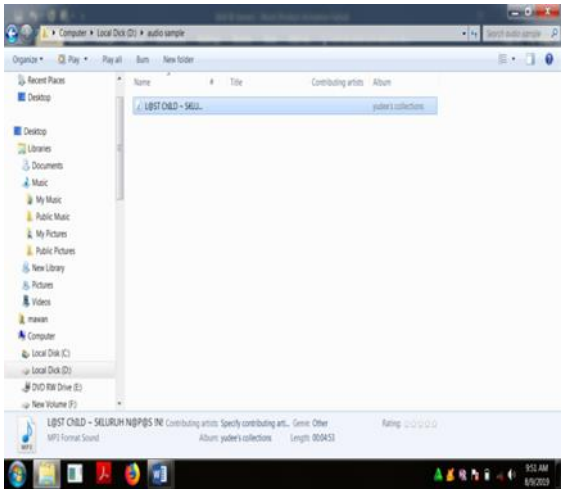
3. HASIL DAN PEMBAHASAN

3.1 Implementasi

Contoh kasus dalam proses ini seperti dijelaskan dalam analisa yaitu file audio (L@ST CHILD.MP3). data yang diambil hanya sebanyak 25 byte untuk plainteks, cara pengambilan nilai hex data audio menggunakan aplikasi HexWorkShop dan langkah-langkahnya sebagai berikut:

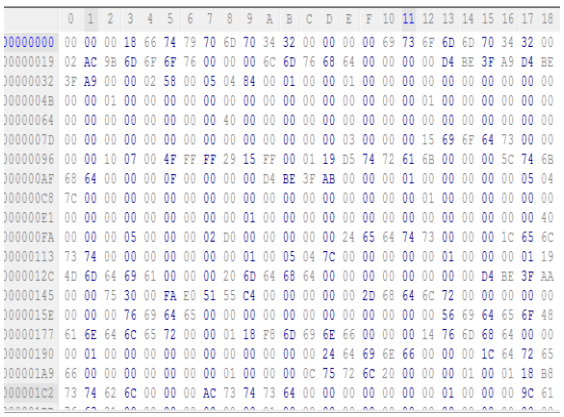
a. Jalankan Aplikasi HexworkShop
b. Klik menu File pilih Open
c. Telusuri dan pilih file audio di drive harddisk dan klik OK

Gambar dibawah adalah pemilihan file audio yang akan digunakan untuk contoh kasus yaitu audioL@ST CHILD.MP3



Gambar 3. File Audio di Drive Penyimpanan

Gambar di bawah ini adalah data heksadesimal dari file audioL@ST CHILD.MP3 menggunakan aplikasi HexWorkShop.



Gambar 4. Data *audio*

Dari data tersebut diambil sebanyak 25 *byte* atau 80 karakter heksadesimal dan dikonversi ke biner sebagai sampel metode, yang berguna untuk mengetahui nilai biner dari bilangan tersebut.

Buletin Ilmiah Informatika Teknologi
Vol 1, No 1, September 2022, Hal. 8 - 14
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

Dari gambar data video di atas diambil sebanyak 24 byte untuk plainteks, yaitu :

02,AC,9B,6D,6F,6F,76,00,00,00,6C,6D,76,68,64,00,00,00,00,D4,BE,3F,A9,D4,BE
Pemprosesan merupakan bagian inti yang terdiri atas 1 *round* yang mempunyai 64 operasi untuk memproses setiap satu blok pesan 512 bit diperlukan 64 operasi, setiap blok pesan $M^{(0)}$, $M^{(1)}$, $M^{(2)}$,....$M^{(N)}$ dengan N adalah jumlah blok pesan.

Tabel 2 Penambahan Bit

W0=a215fafafbfafafb	W21=aa4cb53eeb7ea000	W42=81f8f118d61d799	W63=f566f9797a02f97b
W1=bbababdc4cfcfdd	W22=c1be0a3a45bbc0c8	W43=efad621e771fc8a0	W64=f5f6f9797a79f97b
W2=fdfcdcfcfdfdfcfcf	W23=70d185c95a21f97b	W44=2f8f118d61d780c8	W65=536f8797a79f97b
W3=0000000000000000	W24=33c81ac764e6ddf5	W45=d8054b1e14ad2202	W66=372f35dc271f4c48
W4=0000000000000000	W25=fg27c2de7974aba7c	W46=d8054b1e14ad0120	W67=126f35dc271f4780
W5=0000000000000000	W26=861fd33a28227a80	W47=890d46dd1b754e00	W68=1549f35dc271f52c8
W6=0000000000000000	W27=5975026636458e00	W48=9646dd1b754e0011	W69=06e67b5dc271f40c8
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=1f4689h761d780c8
W17=f5777777fc36abf5	W38=5a3f8dd006f72c72	W59=74bf6e1c4c49c021	
W18=8f728a8e53a45bbc	W39=463afebfd12dc3c6	W60=74a16e1c4c49cf21	
W19=43e23c4a5202fd40	W40=40d8054b1e14ad22	W61=f5f6f9797a790000	
W20=b333c81ac764e6dd	W41=162974cce6f10202	W62=137f4f5f6ff7fh880h	

Karena t sebanyak 64 iterasi maka selanjutnya adalah hasil iterasi dan telah mengalami rotasi 1 kali keseluruhannya dari 16 hingga 63 untuk W_t. Untuk $W_t = W_{29}$ atau selanjutnya, yaitu :

Tabel 4. Hasil Iterasi 16-63

W0=a215fafafbfafafb	W21=aa4cb53eeb7ea000	W42=81f8f118d61d799	W63=f566f9797a02f97b
W1=bbababdc4cfcfdd	W22=c1be0a3a45bbc0c8	W43=efad621e771fc8a0	W64=f5f6f9797a79f97b
W2=fdfcdcfcfdfdfcfcf	W23=70d185c95a21f97b	W44=2f8f118d61d780c8	W65=536f8797a79f97b
W3=0000000000000000	W24=33c81ac764e6ddf5	W45=d8054b1e14ad2202	W66=372f35dc271f4c48
W4=0000000000000000	W25=fg27c2de7974aba7c	W46=d8054b1e14ad0120	W67=126f35dc271f4780
W5=0000000000000000	W26=861fd33a28227a80	W47=890d46dd1b754e00	W68=1549f35dc271f52c8
W6=0000000000000000	W27=5975026636458e00	W48=9646dd1b754e0011	W69=06e67b5dc271f40c8
W7=0000000000000000	W28=597244d8c81d4000	W49=ad621e771fc8a000	W70=12eff5fc271f40c8
W8=0000000000000000	W29=12ef35dc271f40c8	W50=cfab5138a9785175	W71=96af35dc271f46c8

Buletin Ilmiah Informatika Teknologi
Vol 1, No 1, September 2022, Hal. 8 - 14
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

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=1f4689h761d780c8
W17=f5777777fc36abf5	W38=5a3f8dd006f72c72	W59=74bf6e1c4c49c021	
W18=8f728a8e53a45bbc	W39=463afebfd12dc3c6	W60=74a16e1c4c49cf21	
W19=43e23c4a5202fd40	W40=40d8054b1e14ad22	W61=f5f6f9797a790000	
W20=b333c81ac764e6dd	W41=162974cce6f10202	W62=137f4f5f6ff7fh880h	

Maka nilai t_{63} digunakan untuk mendapatkan *cipher* atau biasa disebut *digest* dalam SHA-512 dengan cara di XOR dengan nilai a, b, c, d,e,f, g dan h awal (penyangga).

$H_i = a_0 + a_n$

$h0^{(0)}$ =6a09e667f3bcc908 + ece3e03dff0b4ddd =56edc6a5f2c816e5
$h1^{(0)}$ =bb67ae8584caa73b + ea6b38016824fa2b = a5d2e686ecefa166
$h2^{(0)}$ =3c6ef372fe94f82b + 8a0eb6ac66a7d4d8 = c67daa1f653ccd03
$h3^{(0)}$ = a54ff53a5f1d36f1 + 8577a6fc34caafac = 2ac79c3693e7e69d
$h4^{(0)}$ =510e527fade682d1 + 8d406c11e7545a1b = de4ebe91953adcec
$h5^{(0)}$ =9b05688c2b3e6c1f + 1bad6730176d2901 = b6b2cfbc42ab9520
$h6^{(0)}$ = 1f83d9abfb41bd6b + 39d839b4f9751416 = 595c1360f4b6d181
$h7^{(0)}$ = 5be0cd19137e2179 + 1b7b2c2e2a29f112 = 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 pendeteksian file audio tersebut asli.

4. KESIMPULAN

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

1. Dengan Penererapan Metode SHA-512 audio akan mudah terdeteksi dan mengetahui audio tersebut asli atau editan.
2. 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 audio asli atau audio 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.

Buletin Ilmiah Informatika Teknologi
Vol 1, No 1, September 2022, Hal. 8 - 14
ISSN 2962-0945 (media online)
https://ejurnal.amikstiekomsu.ac.id/index.php/BIIT

[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.
[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.
[19] P. H. Arjana, "Penerapan Algoritma Vernam Cipher (One Time) untuk Pengamanan Login," Penerapan Algoritma Vernam Cipher (One Time) untuk Pengamanan Login, p. 4, 2019.
[20] d. Arius, "Pengantar Ilmu Kriptografi," KRIPTOGRAFI FILE CITRA MENGGUNAKAN, p. 23, 2008.
[21] Menezes, " Handbook ofApplied Cryptography," DESAIN DAN IMPLEMENTASI PROTOKOL KRIPTOGRAFI UNTUK APLIKASI SECURECHATPADA MULTIPLATFORMSISTEM OPERASI , p. 9, 1996.
[22] Kelvin, "Fungsi Hash dan Metode," Fungsi Hash dan Metode , no. , p. 5, 2016.
[23] Noldi Krisandi, "KONSEP KRIPTOGRAFI DAN FUNGSI HASH," KONSEP KRIPTOGRAFI DAN FUNGSI HASH, p. 25, 2018.
[24] I. R. Meiliana Sumagita, "notasi Heksa desimal," notasi Heksa desimal, p. 15, 2018.
[25] H. w. m. a. h. SHA-512, "Halaman website mengenai algoritma hash SHA-512," Halaman website mengenai algoritma hash SHA-512, pp. 2 : http://en.wikipedia.org/wiki/SHA-2 , 8 Mei 201.
[26] T.Indra Wardana ,Eko Aribowo , "Visuan studio Basic 2008," PERANCANGAN DAN IMPLEMENTASI SISTEM INFORMASI MANAJEMEN KEGIATAN MASJID , p. 25, 2018.
[27] M. Wardana, "Visual Studio 2008," RUANG LINGKUP KERJA VISUAL BASIC 2008, p. 17, 2008.
[28] F. H, "Mendeteksi pemalsuan digital menggunakan analisis bispectral [R]," 1999.
[29]. Karim, S. Esabella, M. Hidayatullah, and T. Andriani, “Sistem Pendukung Keputusan Aplikasi Bantu Pembelajaran Matematika Menggunakan Metode EDAS,” vol. 4, no. 3, 2022, doi: 10.47065/bits.v4i3.2494.
[30]. M. Bobbi, K. Nasution, S. Suryadi, and A. Karim, “Sistem Pendukung Keputusan Dalam Rekomendasi Kelayakan nasabah Penerima Kredit Menerapkan Metode MOORA dan MOOSRA,” vol. 4, no. 3, pp. 1284–1292, 2022, doi: 10.47065/bits.v4i3.2610.