Management of Information System Journal
Vol 2, No 1, November 2023, Hal 7 - 13
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Analisa Fungsi Hash Untuk Mendeteksi Otentikasi File Video Menerapkan Metode N-Hash

Marjadi Hebert Harianja
Program Studi Teknik Informatika, Universitas Budi Darma Medan, Indonesia
Email: marjadi12031997@gmail.com
Email Korespoden: marjadi12031997@gmail.com

Abstrak− Masalah yang terdapat pada ruang lingkup video adalah video tersebut dapat ditonton oleh orang yang tidak berhak jika file video perlu diamankan dengan pengaman yang baik. Sehingga perlu merancang aplikasi pemutar video dan menerapkan enkripsi dan deskripsi pada aplikasi yang dirancang tersebut. N-HASH hanya dapat menghasilkan16 byte cipherteks sementara masukan atau input yang berbeda tersebut yaitu jika input 4 byte maka outputnya 16 byte dan jika input 16 byte maka outputnya 4 byte. Hasil dari mendeteksi otentikasi file video memiliki banyak data jika dalam byte data tersebut sangat sulit untuk enkripsi dengan N-HASH.

Kata Kunci : N-HASH, Video; Otentokasi File

Abstract− *The problem with the video scope is that the video can be watched by unauthorized people if the video file needs to be secured with good security. So it is necessary to design a video player application and apply encryption and description to the designed application. N-HASH can only produce 16 bytes of ciphertext while the input is different, namely if the input is 4 bytes then the output is 16 bytes and if the input is 16 bytes then the output is 4 bytes. The results of detecting authentication of video files have a lot of data if in bytes the data is very difficult to encrypt with N-HASH.*

Keywords: *N-HASH, Video; File Authentication*

1. PENDAHULUAN

Video adalah bentuk rekaman periodik waktu dari muatan data audio dan visual citra digital. Video bukan hanya karya dari sebuah rumah produksi perfilman. Saat ini siapa saja dapat membuat video asalkan memiliki perangkat pembuat video. Terdapat beberapa perangkat yang dimiliki secara umum dan memiliki fungsi kamera video seperti, Handycam, kamera digital, smartphone dan webcam.Pembuatan video sekarang bisa dilakukan dengan perangkat smartphone.Orang yang memiliki smartphone dapat membuat video untuk dokumentasi video pribadinya seperti video kenang-kenangan keluarga. Video pribadi tersebut tentunya aman dan tidak diinginkan ditonton oleh orang lain dengan alasan tertentu. Masalah yang terdapat pada ruang lingkup video adalah video tersebut dapat ditonton oleh orang yang tidak berhak jika tanpa pengamanan video. Dengan demikian penulis merasa file video perlu diamankan dengan pengaman yang baik. Sehingga perlu merancang aplikasi enkripsi dan dekripsi pada file video. Untuk dapat menjaga integritas data dari suatu file video, diciptakan suatu mekanisme yang disebut digital signature atau sering juga nilai hash, yaitu kode khusus yang dihasilkan dari fungsi penghasil digital signature. Salah satu algoritma yang digunakan untuk menghasilkan digital signature adalah fungsi hash.

Fungsi hash atau one-way hashing algorithm adalah fungsi satu arah yangberfungsi dalam pengecekan keaslian atau integritas suatu pesan. Fungsi hash dapatmenerima masukan yang panjangnya bernilai random dan mengubahnya menjadi nilaihash yang berukuran tetap. Fungsi hash bekerja dengan mengubah pesanmenjadi message digest atau pesan singkat yang terlihat acak dan tidak akan dapatdikembalikan menjadi pesan semula. Nilai hash yang dihasilkan tidak akan memiliki nilai yang sama pada pesan yang berbeda. Ada banyak algoritma hash yang telah ditemukan yaitu: MD2, MD4, MD5, MD6, dan lain-lain. Salah satu algoritma yang ditemukan yaitu algoritma N-Hash. Semua algoritma tersebut memiliki kelebihan dan kelemahan masing-masing.

Adapun permasalahan dalam mendeteksi otentikasi sebuah file videokarena sering terjadinya perubahan pada file video baik dari ukuran file video tersebut maupun setiap frame yang terdapat pada file video. Algoritma N-Hash merupakan algoritma hash yang diusulkan pada tahun 1990 oleh Miyaguchi. Algoritma N-Hash memiliki ukurane 128-bit. Pesan dibagi menjadi 128-bit, dan setiap blok digabungkan dengan nilai hash yang dihitung sejauh ini menggunakan fungsi kompresi. Berisi delapan putaran, yang masing-masing menggunakan fungsi F, mirip dengan yang digunakan oleh feal. Pada tahun 1991 Eli Biham dan Adi Shamir menerapkan teknik diferensial pembacaan sandi untuk N-Hash. Algoritma ini juga merupakan algoritma hashing yang cepat dan sederhana yang mencoba untuk mengirimkan nilai secara merata tetapi tidak berusaha menghindari tabrakan. Algoritma ini diharapkan dapat mendeteksi keaslian suatu file video

Management of Information System Journal
Vol 2, No 1, November 2023, Hal 7 - 13
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

2. METODOLOGI PENELITIAN

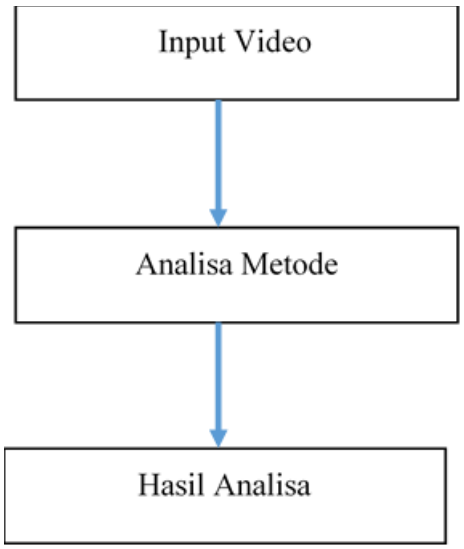
2.1 Analisa Masalah

Video bukan hanya karya dari sebuah rumah produksi perfilman. Saat ini siapa saja dapat membuat video asalkan memiliki perangkat pembuat video. Pembuatan video sekarang bisa dilakukan dengan perangkat smartphone. Orang yang memiliki smartphone dapat membuat video untuk dokumentasi video pribadinya seperti video kenang-kenangan keluarga. Video pribadi tersebut tentunya aman dan tidak diinginkan ditonton oleh orang lain dengan alasan tertentu. Masalah yang terdapat pada ruang lingkup video adalah video tersebut dapat ditonton oleh orang yang tidak berhak jika tanpa pengamanan video. Dengan demikian penulis merasa file video perlu diamankan dengan pengaman yang baik.

Fungsi *hash* atau *one-way hashing algorithm* adalah fungsi satu arah yang berfungsi dalam pengecekan keaslian atau integritas suatu pesan. Fungsi *hash* dapat menerima masukan yang panjangnya bernilai *random* dan mengubahnya menjadi nilai hash yang berukuran tetap. Fungsi *hash* bekerja dengan mengubah pesan menjadi *message digest* atau pesan singkat yang terlihat acak dan tidak akan dapat dikembalikan menjadi pesan semula. Nilai *hash* yang dihasilkan tidak akan memiliki nilai yang sama pada pesan yang berbeda.

Adapun permasalahan dalam mendeteksi otentikasi sebuah file video karena sering terjadinya perubahan pada file video baik dari ukuran file video tersebut maupun setiap *frame* yang terdapat pada file video. Algoritma N-Hash merupakan algoritma *hash* yang diusulkan pada tahun 1990 oleh Miyaguchi. Algoritma N-Hash memiliki ukurane 128-bit. Pesan dibagi menjadi 128-bit, dan setiap blok digabungkan dengan nilai *hash* yang dihitung sejauh ini menggunakan fungsi kompresi. Berisi delapan putaran, yang masing-masing menggunakan fungsi F, mirip dengan yang digunakan oleh *feal*. Pada tahun 1991 Eli Biham dan Adi Shamir menerapkan teknik *diferenial* pembacaan sandi untuk N-Hash. Algoritma ini juga merupakan algoritma *hashing* yang cepat dan sederhana yang mencoba untuk mengirimkan nilai secara merata tetapi tidak berusaha menghindari tabrakan. Algoritma ini diharapkan dapat mendeteksi keaslian suatu file video.

Untuk mempermudah dalam melakukan proses analisa, maka perlu adanya sebuah bagan yang dapat mempermudah untuk menganalisa proses otentikasi file video. Bagan tersebut dapat dilihat seperti pada gambar 3.1



Gambar 1 Bagan Alir Analisa

2.2 Autentikasi

Autentikasi adalah metode untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Terdapat tiga tipe kompenen yang terlihat pada proses autentikasi user[1].

1. Supplicant: proses autentikasi yang akan memberikan identitasnya dan bukti. Proses ini juga dapat dirujuk sebagai pengguna autentikasi atau client.
2. Authenticator: proses autentikasi yang menyediakan sumber daya untuk client dan kebutuhan,guna memastikan identitas pengguna untuk mengotorisasi dan mengakses pengguna audit sumber daya. Autentikasi juga dapat diarahkan sebegai server.
3. Security authority / database: penyimpanan atau mekanisme untuk memeriksa user credentials. Kondisi ini dapat menjadi lebih sederhana, seperti flat file atau server yang berada pada jaringan yang menyediakan autentikasi pengguna terpusat, atau satu set server autentikasi yang terdistribusi menyediakan autentikasi pengguna dalam perusahaan atau di jaringan komputer.

Management of Information System Journal
Vol 2, No 1, November 2023, Hal 7 - 13
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Adanya tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermaking (untuk menjaga "intellectual property", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat dan***digital signature***. Access control yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometic (ciri-ciri khas orang) dan sejenisnya[1].

2.3 Enkripsi dan Deskripsi

Proses menyandikan plainteks menjadi chiperteks disebut enkripsi*(encryption)* atau*enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan cipherteks menjadi plainteks semula dinamakan deskripsi *(decrytion)* atau *deciphering* (standard nama menurut ISO 7498-2). Enkripsi dan deskripsi dapat diterapkan baik pada pesan yang dikirim maupun pada pesan tersimpan. Istilah *encryption of data in motion* mengacu pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, sedangkan istilah *encryption of data at-rest* mengacu pada enkripsi dokumen yang disimpan di dalam storage. Contoh *encryption of data in motion*adalah pengiriman nomor PIN dari mesin ATM ke komputer server dikantor bank pusat. Contoh *encryption of data at-rest* adalah enkripsi file basis data di dalam hard disk.

2.4 Metode N-HASH

Pada proses analisa yang dilakukan pada penelitian ini, video adalah merupakan objek yang digunakan untuk melakukan pengujian dari metode N-HASH. Pada proses pengujian yang dilakukan pada penelitian ini, jumlah sampel data yang diambil dari video adalah sebanyak 16 byte. Untuk mengambil nilai hexa dari pada video, maka membutuhkan bantuan aplikasi *HexWorkshop*.Dikutip oleh Andara Livia (2010), Fast Data Encipherment Algorithm atau yang lebih dikenal dengan FEAL merupakan sebuah enskripsi tipe simetris block ciphers. Algoritma ini diciptakan sebagai bentuk alternatif dari Data Encryption Standard (DES) serta diprogram agar mampu bekerja lebih cepat pada software. FEAL memiliki peranan penting dalam pengembangan teknik kriptanalis, seperti kriptanalis liner dan diferesnsial. Pada 1987, FEAL pertama kali dikenalkan oleh Shimizu dan Miyaguchi dari NTT. Chipers ini bersifat rentan terhadap berbagai macam kriptanalis, namun dapat berfungsi sebagai katalis pada pertemuan kriptanalis diferensial dan linear. FEAL, seperti halnya DES juga berlandaskan pada algoritma Fiestal[2, 2].
Dalam perkembangannya, terdapat beberapa perbaikan untuk FEAL walaupun secara keseluruhan merupakan cipher Fiestal. FEAL menggunakan basis putaran kunci yang sama yang bekerja pada blok 64-bit. FEAL-N menempatkan bit blok plaintext dengan memanfaatkan kunci rahasia 64-bit. FEAL menggunakan N putaran cipher Fiestal dengan fungsi f yang lebih sederhana. Hal ini lalu dijumlahkan dengan desain awal dan akhir dari FEAL dengan melakukan XOR secara sebagian dari dua data yang sama halnya dengan mengaplikaskan subkey dengan sebagaian data.

2.5 Fungsi Hash Satu arah

Fungsi*hash*satu arah *(One-way hash)* adalah fungsi *hash* yang bekerja dalam satu arah.*String*yang telah diubah menjadi *message digest* tidak dapat lagi dikembalikan menjadi *string* semula. Dua *string* yang berbeda akan selalu mengahasilkan nilai *hash*yang berbeda pula[2].
Sifat-sifat dari fungsi *hash* satu arah adalah sebagai berikut:

1. Fungsi H dapat diterapkan pada block data berukuran apa saja.
2. H menghasilkan nilai *(h)* dengan panjang tetap *(fixed-length output).*
3. H*(x)* mudah dihitung untuk setiap nilai *x* yang diberikan.
4. Setiap *h* yang diberikan, tidak mungkin menemukan *x*sehingga H*(x) = h.*
5. Untuk setiap *x* yang diberikan, tidak mungkin mencari *y = x* sedemikian sehingga H*(y)* = H*(x).*
6. Secara komputasi tidak mungkin mencari pasangan *x dan y* sedemikian sehingga H*(x)* = H*(y).*

2.5.1 Secure Hash Algorithm (SHA)

SHA adalah fungsi hash satu arah yang dibuat oleh NIST dan digunakan bersama DDS*(Digital signature standard).* Oleh NSA, SHA dinyatakan sebagai standard fungsi hash satu arah. SHA dapat dianggap sebagai kelanjutan pendahulunya, MD5, yang telah digunakan secara luas. SHA disebut aman *(secure)* karena ia dirancang sedemikian rupa sehingga secara komputasi tidak mungkin menemukan pesan yang berkoresonden dengan *messsagedigest* yang diberikan[2].

3. HASIL DAN PEMBAHASAN

3.1 Penerapan Metode N-HASH

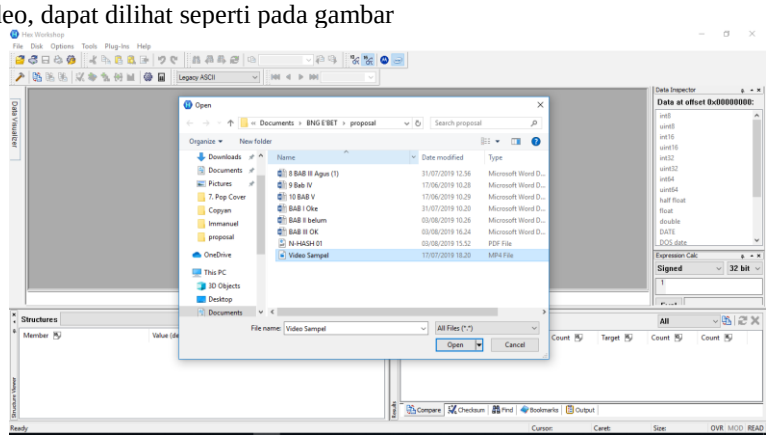
Pada proses analisa yang dilakukan pada penelitian ini, video adalah merupakan objek yang digunakan untuk melakukan pengujian dari metode N-HASH. Pada proses pengujian yang dilakukan pada penelitian ini, jumlah sampel data yang diambil dari video adalah sebanyak 16 byte. Untuk mengambil nilai hexa dari pada video, maka membutuhkan bantuan aplikasi *HexWorkshop*. Adapun langkah dengan menggunakan metode *HexWorkshop* adalah sebagai berikut:

a. Jalankan aplikasi *Hexworkshop*

Management of Information System Journal
Vol 2, No 1, November 2023, Hal 7 - 13
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

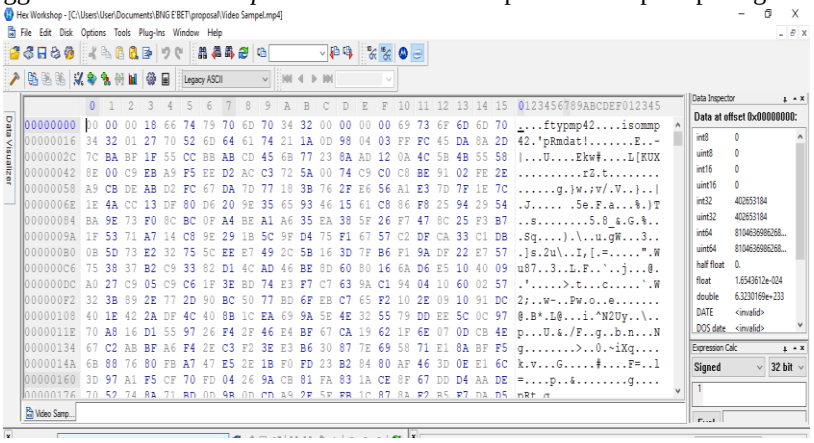
b. Pilih menu file untuk mendapatkan file yang digunakan sebagai sampel data dalam penelitian ini.
c. Telusuri dan temukan file video yang akan di otentikasi.

Berikut ini merupakan langkah langkah pengambilan video dengan menggunkan *HexWorkshop*. Berikut merupakan langkah pemilihan video, dapat dilihat seperti pada gambar



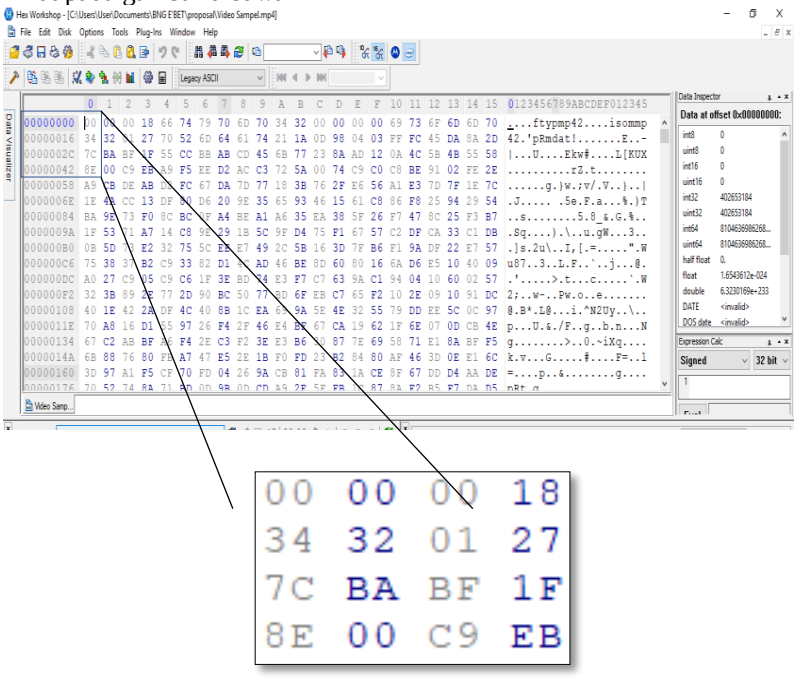
Gambar 2 Memilih Video

Setelah menemukan video yang akan diolah, maka langkah selanjutnya menampilkan nilai *hexadesimal* dari video tersebut dengan menggunakan *HexWorkshop*. Nilai *Hex* tersebut dapat dilihat seperti pada gambar dibawah



Gambar 3 Nilai *Hex* Dari Video

Setelah mendapatkan nilai *Hex*, maka menentukan dan mengambil nilai *hex* tersebut sebanyak 4x4 atau 16 *byte*. Nilai tersebut dapat dilihat pada gambar dibawah



Gambar 4 Nilai *Byte* Video Dengan Ukuran 4x4 (16 *Byte*)

Management of Information System Journal
Vol 2, No 1, November 2023, Hal 7 - 13
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Sampel nilai dari video dengan ukuran 4x4 atau 16 byte dapat dilihat seperti pada tabel

Tabel 1 Nilai 4x4 atau 16 *byte*

00	00	00	18	34	32	01	27	7C	BA	BF	1F	8E	00	C9	EB

Nilai yang terdapat pada tabel diatas merupakan nilai penyangga atau nilai *buffer* awal yang kemudian digunakan untuk otentikasi file video. Nilai yang ada pada tabel 1 kemudian dikonversikan kedalam nilai biner dengan 8 bit. Nilai konversi tersebut dapat dilihat seperti pada tabel

Tabel.2 Konversi Nilai Hexadecimal Kedalam Nilai Biner

Nilai Hexadesimal Awal	Nilai Biner (8 bit)
00	00000000
00	00000000
00	00000000
18	00011000
34	00110100
32	00110010
01	00000001
27	00100111
7C	01111100
BA	10111010
BF	10111111
1F	00011111
8E	10001110
00	00000000
C9	11001001
EB	11101011

Langkah-Langkah Penerapan Metode N-HASH :

1. Menentukan plaintex dan kunci
   Plainteks yang digunakan diambil dari nilai hexadesimal yang merupakan nilai hexadesimal dari file video. Nilai tersebut dapat dilihat seperti pada tabel 3.

Plainteks	00000000 00000000 00000000 00011000 00110100 00110010 00000001 00100111 01111100 10111010 10111111 00011111 10001110 00000000 11001001 11101011
Key	MARJADI = 77 65 82 74 65 68 73
	01001101 01000001 01010010 01001010 01001101 01000100 010001001

2. Menentukan nilai ML dan MR dimana nilai Ml dan MR dibentuk dengan ukuran 64 bit dari plainteks yang sudah ada.
   ML : 00000000 00000000 00000000 00011000 00110100 00110010 00000001 00100111

   MR : 01111100 10111010 10111111 00011111 10001110 00000000 11001001 11101011

3. Melakukan operasi XOR terhadap nilai
   0000000000000000 0000000000011000
   0000000000000000 0100110101000001 ⊕
   0000000000000000 0100110101011001

   0011010000110010 0000000100100111
   0000000000000000 01010010 01001010 ⊕
   0011010000110010 0101001101101111

   0111110010111010 1011111100011111
   0000000000000000 01001101 01000100 ⊕
   0111110010111010 1111111101011111

   1000111000000000 1100100111101011
   0000000000000000 0000000010001001 ⊕
   1000111000000000 1100100111101111

   Untuk i=1 hingga dengan i=4, lakukan langkah seperti dibawah ini:
   Li ⟵ Ri-1
   Ri-1 ⟵ Li ⊕ f(Ri-1, Ki-1)

Management of Information System Journal
Vol 2, No 1, November 2023, Hal 7 - 13
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Pada fungsi tersebut terdapat dua *byte-oriented* data subtistusi S0 dan S1
$S_0 (X_1, X_2) = Rot2 ((X_1 + X_2) \bmod 256)$
$S_1 (X_1, X_2) = Rot2 ((X_1 + X_2 + 1) \bmod 256)$

Perulangan 1:
Li = 0000000000000000 0100110101011001

f(Ri-1, Ki-1)=
0000000000000000 0100110101000001
0000000000000000 0100110101011001⊕
0000000000000000 0100110101011001

Perulangan 2:
Li = 0011010000110010 0101001101101111

f(Ri-1, Ki-1)=
0000000000000000 01010010 01001010
0011010000110010 0101001101101111⊕
0011010000110010 0101001101101111

Perulangan 3:
Li = 0111110010111010 1111111101011111

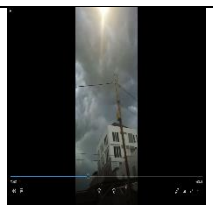
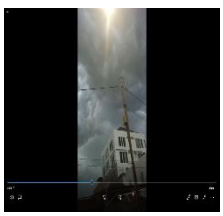
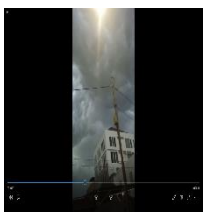
f(Ri-1, Ki-1)=
0000000000000000 01001101 01000100
0111110010111010 1111111101011111⊕
0111110010111010 1111111101011111

Perulangan 4:
Li = 1000111000000000 1100100111101111

F (Ri-1, Ki-1)=
0000000000000000 0000000010001001
1000111000000000 1100100111101111⊕
1000111000000000 1100100111101111

Hasil dari perulangan 1 adalah R1 = 1000111000000000 1100100111101111
dan Li = 1000111000000000 1100100111101111 lakukan kembali 1 kali perulangan. jika sudah 1 kali perulangan, untuk mendapatkan nilai Ls Akhir ialah dengan cara Ls ⊕ Rs, kemudian Rs akhir=Rs. Maka didapatlah nilai Ls Akhir dan Rs Akhir kemudian gabungkan Ls Akhir dan Rs Akhir untuk mendapatkan chipper teks. Dari nilai yang diperoleh yaitu dengan nilai R1 dan L1 maka metode N-Hash dapat mendeteksi orginalitas file video dengan nilai *hash* adalah : SE0C9DFSE0C9DF

Tabel 3 Hasil Pengujian Citra

Parameter	Citra Awal	Citra Yng Sudah diEdit	Nilai Hash Citra Awal	Nilai Hash Citra Edit	Ket.
Melakukan Perubahan pada file video dengan menambahkan durasi pada file video			SE0C9DFSE0C9DF	fd2bb6bf73aa2f494be0874e181ffc532e43c9d2	Nilai *Hash* File Video Terdeteksi
Melakukan Perubahanpada file video dengan menambahkan gambar pada file video			SE0C9DFSE0C9DF	f5b7601d9061e69bba76369df00ef6c1f4ee559f	Nilai *Hash* File Video Terdeteksi

Management of Information System Journal
Vol 2, No 1, November 2023, Hal 7 - 13
ISSN 2964-9455 (media online)
Website https://journal.fkpt.org/index.php/mis

Melakukan Perubahan Perubahan pada file video dengan memotong durasi video			SE0C9DFS E0C9DF	821b82b1f0 8c90e9461 1df989eb72 bb645576c 2eb89e996 2d227c15ea b9f0c6a	Nilai *Hash* File Video Terdeteksi

4. KESIMPULAN

Kesimpulan dari suatu penelitian merupakan penjelasan tentang hasil akhir yang menguraikan pencapaian dari tujuan penelitian. Dari hasil penulisan dan analisa dari bab-bab sebelumnya, maka dapat diambil kesimpulan-kesimpulan, dimana kesimpulan-kesimpulan tersebut kiranya dapat berguna bagi para pembaca, sehingga penulisan skripsi ini dapat lebih bermanfaat. Setalah melakukan penelitian dapat di simpulkan mendeteksi otentikasi file video digunakan setelah data-data yang telah diperoleh dari wawancara dan observasi yang dikumpulkan kemudian dilakukan suatu analisis yang sesuai dengan permasalahan mendeteksi otentikasi file video menerapkan metode N-Hash. Dari hasil penelitian metode N-Hash dalam mendeteksi otentikasi file video dapat disimpulkan bahwa menggunakan metode N-Hash jauh lebih mudah. Setelah melakukan pengujian metode N-HASH menggunakan aplikasi Hasher-pro untuk mendeteksi otentikasi file video

UCAPAN TERIMAKASIH

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

REFERENCES

[1] K. W. Argakusumah and S. Hansun, “Implementasi Algoritma Boyer-Moore pada Aplikasi Kamus Kedokteran Berbasis Android,” J. Ultim., vol. 6, no. 2, pp. 70–78, 2014.
[2] A. Mushofan, I. T. Bandung, and J. G. Bandung, “Pengembangan Algoritma Boyer Moore,” 2014.
[3] R. fitri riyanarto sarwono, yeni Anistyasari, SEMANTIC SEARCH, Andi Offse. Yogyakarta, 2012.
[4] K. W. Argakusumah and S. Hansun, “Implementasi Algoritma Boyer-Moore pada Aplikasi Kamus Kedokteran Berbasis Android,” J. Ultim., vol. 6, no. 2, pp. 70–78, 2014.
[5] S. S. Wicida, “PENELUSURAN KATALOG PERPUSTAKAAN PADA SMA IT YABIS BONTANG DENGAN ALGORITMA BOYER-MOORE,” pp. 15–21, 2008.
[6] K. W. Argakusumah and S. Hansun, “Implementasi Algoritma Boyer-Moore pada Aplikasi Kamus Kedokteran Berbasis Android,” J. Ultim., vol. 6, no. 2, pp. 70–78, 2014.
[7] rosa A. S. M.shalahuddin, Rekayasa perangkat lunak. Bandung: informatika bandung, 2016.
[8] Murtiwiyati and G. Lauren, “J U R N A L I L M I A H KOMPUTASI Komputer & Sistem Informasi 1-10,” J. Ilm., vol. 12, p. 2,3, 2013.
[9] S. K. Alfa Satyaputra, M.cs & Eva maulina Aritonang, java for beginners with eclipse 4.2 juno. jakarta: PT. Elex Media komputindo, 2012.
[10] M. R. Arief, "AUTENTIKASI, KENDALI AKSES, AUDIT SISTEM," AUTENTIKASI, KENDALI AKSES, AUDIT SISTEM, vol. 11, pp. 73-76, 2010.
[11] C. Y.-m. Z. Mei-ling, "Sampling Based N-Hash Algorithm for Searching," Sampling Based N-Hash Algorithm for Searching, vol. 12, pp. 1-4, 2015.
[12] a. r. r. Hasan abdurahman, "aplikasi pinjaman pembayaran secara kredit kepada bank yudha bhakti," aplikasi pinjaman pembayaran secara kredit kepada bank yudha bhakti, vol. 8, pp. 61-69, 2014.