Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 1-6
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3123
Website https://ejurnal.seminar-id.com/index.php/jussi

Implementasi Checksum Dengan Menggunakan Algoritma Fletcher Untuk Mendeteksi Keaslian Sertifikat Rumah

Syifa

Program Studi Tenik Informatika, Fakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Budi Darma,
Jalan Sisingamangaraja No.338, Medan, Sumatera Utara, Indonesia
Email: syifasauqiyah83@gmail.com

Abstrak-Pada era sekarang ini, pembaharuan terus dilakukan demi mencapai integritas yang lebih baik. Penerbitan sertifikat yang biasa di cetak dalam bentuk kertas, dianggap masih rawan akan rusak dan hilang. Seiring perkembangan zaman, kini sertifikat juga diterbitkan dalam bentuk digital. Sehingga banyak orang beralih menggunakan sertifikat dalam bentuk digital. Sehingga diperlukan mekanisme untuk membantu keamanan pada sertifikat tersebut. Penerbitan sertifikat digital hanya dapat dilakukan oleh pihak yang berwenang. Kemudian pihak yang berwenang tersebut mengeluarkan sertifikat kepada orang lain yang mempunyai hak atas sertifikat tersebut. Tentu keaslian informasi sertifikat telah dia amankan terlebih dahulu melalui fungsi checksum sehingga pesan didalamnya sudah di enskripsi. Dalam kriptografi ada banyak metode dan algoritma yang bisa digunakan salah satunnya yaitu algoritma fletcher checksum. Tujuan dari fletcher yaitu untuk menyediakan sifat deteksi kesalahan yang mendekati pemeriksaan redudansi siklik tetapi dengan upaya komputansi yang lebih rendah terkait dengan teknik penjumlahan. Sehingga sertifikat digital yang mengalami perubahan akan terdeteksi keasliannya.

Kata Kunci: Kriptografi; Checksum; Fletcher-32

Abstract-In today's era, renewal is continuously carried out in order to achieve better integrity. The issuance of certificates, which are usually printed on paper, is considered to be prone to damage and loss. Along with the times, certificates are now also issued in digital form. So many people switch to using certificates in digital form. So a mechanism is needed to help secure the certificate. Digital certificates can only be issued by authorized parties. Then the competent authority issues a certificate to another person who has the right to the certificate. Of course, the authenticity of the certificate information has been secured first through the checksum function so that the message in it is encrypted. In cryptography there are many methods and algorithms that can be used, one of which is the Fletcher checksum algorithm. The aim of Fletcher is to provide error detection properties that approximate cyclic redundancy checking but with lower computational effort associated with the summation technique. So that digital certificates that have changed will be detected as authentic.

Keywords: Cryptography; Checksum; Fletcher-32

1. PENDAHULUAN

Rumah atau tempat tinggal adalah sebuah bangunan yang di huni seseorang ataupun keluarga di dalamnya, yang berfungsi sebagai tempat beristirahat serta tempat pulang seseorang dari berpergian. Bisa juga di multifungsikan menjadi tempat usaha dalam mencari nafkah. Selain menjadi salah satu kebutuhan primer manusia, rumah juga menjadi tolak ukur untuk mengetahui bagaimana kondisi ekonomi kehidupan seseorang. Perekonomian yang sulit terkadang memaksa seseorang menjadikan sertifikat rumah sebagai jaminan untuk meminjam uang ataupun modal usaha bagi mereka. Ditambah lagi seiring jumlah penduduk yang meningkat, membuat harga rumah menjadi mahal, tak terkecuali harga sewa rumah juga ikut naik. Hal ini juga mendorong seseorang menyalahgunakan kesempatan tersebut dengan cara yang tidak halal. Seperti memanipulasi sertifikat tersebut untuk menipu calon korbannya.

Di era sekarang ini, pembaharuan terus dilakukan demi mencapai integritas yang lebih baik. Penerbitan sertifikat yang biasa di cetak dalam bentuk kertas, dianggap masih rawan akan rusak dan hilang. Seiring perkembangan zaman, kini sertifikat juga diterbitkan dalam bentuk digital. Kriptografi merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi, dan ketiadaan penyangkalan [1]. Sertifikat digital sangat cocok di imlementasikan dalam kasus yang diangkat dalam penelitian kali ini.

Dalam kriptografi ada banyak metode dan algoritma yang bisa digunakan salah satunnya yaitu algoritma fletcher checksum. Fletcher adalah algoritma untuk menghitung checksum tergantung posisi, tujuan dari fletcher yaitu untuk menyediakan sifat deteksi kesalahan yang mendekati pemeriksaan redudansi siklik tetapi dengan upaya komputansi yang lebih rendah terkait dengan teknik penjumlahan. Sehingga sertifikat digital yang mengalami perubahan akan terdeteksi keasliannya. Terdapat sebuah penelitian oleh Muhammad Dhito Prihardanto dengan topik "Studi Perbandingan Beberapa Fungsi Hash dalam Melakukan Checksum Berkas" Checksum atau hash sum adalah suatu data dengan ukuran tetap (fixed-size datum) yang dihitung dari suatu blok data digital dengan tujuan untuk mendeteksi yang mungkin terjadi saat proses transmisi atau penyimpanan. Integritas data dapat diperiksa pada langkah selanjutnya dengan menghitung pula checksum dan membandingkannya dengan data yang satunya (data sumber/asli). Jika checksum tidak sama, maka hampir dipastikan bahwa data tersebut telah berubah, baik disengaja maupun tidak disengaja [2].

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (cryptography) berasal dari bahasa Yunani, yaitu dari kata crypto dan graphia yang berarti 'penulisan rahasia'.

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 1-6
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3123
Website https://ejurnal.seminar-id.com/index.php/jussi

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, auntentikasi, dan ketiadaan penyangkalan. Algoritma kriptografi merupakan fungsi matematis yang digunakan untuk proses enkripsi yaitu proses untuk menyandikan pesan atau informasi (menjadi bentuk *chipertext)*, dan proses deskripsi yaitu proses untuk membuka suatu pesan tersandi menjadi pesan semula (*plaintext)* [1].

2.2 Fungsi Hash

Fungsi Hash merupakan fungsi yang menerima masukan string yang panjangnya sembarangan dan mengkonversinya menjadi suatu string keluaran yang panjangnya tetap (biasanya ukuran string keluaran jauh lebih kecil daripada ukuran semula). Persamaan fungsi hash adalah sebagai berikut.

$$\text{Hash} = \text{func (message)} \quad (1)$$

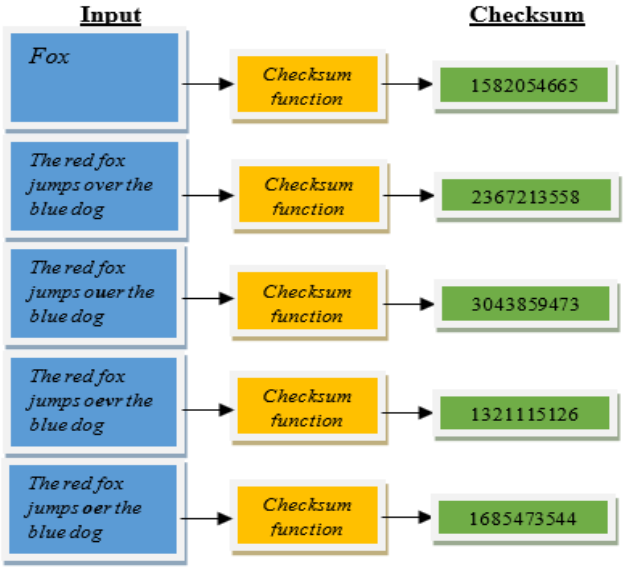
Keluaran fungsi hash biasa disebut dengan nilai hash (hash values), kode hash (hash codes), has sums, checksum, hashes, atau pesan-ringkas (massage digest). Saat ini fungsi hash masih memungkinkan untuk memetakan dua pesan yang berbeda tetapi menghasilkan nilai hash yang sama. Hal itu disebut dengan kolisi (collision). Fungsi hash sering dikaitkan (dan sering juga campur aduk) dengan istilah checksum, check digit, fingerprints, randomizing functions, error correcting codes, dan fungsi hash kriptografi. Meskipun semuanya berkaitan, tetapi pada dasarnya setiap istilah tersebut memiliki kegunaan dan kebutuhan masing-masing yang dirancang dan digunakan untuk hal yang berbeda [3].

Fungsi hash akan mengembalilkan hash value yang panjangnya jauh lebih pendek dibandingkan dengan panjang string masukan. Sebagai contoh, pesan yang ingin dicari nilai hash-nya hanya memiliki ukuran sebesar 1 Mb, maka hash value yang dihasilkan hanya 128 bit. Kebanyakan fungsi hash yang ada saat ini berupa fugsi hash satu arah. Artinya, pesan yang sudah diubah menjadi massage digest tidak dapat dikembalikan lagi menjadi pesan semula (irreversible). Selain itu, fungsi hash satu arah mempunyai sifat sebagai berikut [4]:

a. Fungsi H dapat diterapkan pada blok data berukuran berapa saja.
b. H menghasilkan nilai (h) dengan panjang tetap (fixet length output).
c. H (x) mudah dihitung untuk setiap nilai x yang diberikan.
d. Untuk setiap h yang dihasilkan, tidak mungkin dikembalikan nilai x sedemikian sehingga H(x) = h.
e. Untuk setiap x yang diberikan, tidak mungkin dicari $y \neq x$ sedemikian sehingga H(y) = H(x).
f. Tidak mungkin dicari pasangan x dan y sedemikian sehingga H(x) = H(y).

2.3 Cheksum

Checksum adalah teknologi untuk menandai sebuah file, dimana setiap file yang sama harus memilki checksum yang sama, dan bila nilai checksumnya meskipun berbeda satu bit saja, maka file tersebut merupakan file yang berbeda walaupun memiliki nama file yang sama. Checksum digunakan untuk verifikasi suatu data yang disimpan atau yang dikirim dan diterima. Setiap kali terjadi proses pengiriman data, checksum akan mengenali file tersebut untuk melihat apakah data yang diterima sudah sesuai dengan data yang dikirimkan. Fungsi inilah yang menjadikan checksum sangat efektif untuk melakukan pengecekan terhadap proses transfer suatu data. Checksum akan membaca ulang, menghitung dan membandingkan file yang diterima dengan file yang ditransfer. Bila ada perbedaan nilai, maka checksum akan menganggap bahwa telah terjadi kesalahan, distori atau korupsi selama penyimpanan atau pengiriman. Fungsi checksum akan selalu menghasilkan checksum dengan panjang yang tetap dan cukup identik satu sama lain. Dengan kata lain, bila pesan yang dimasukan berbeda maka checksum-nya juga akan berbeda [5].



Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 1-6
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3123
Website https://ejurnal.seminar-id.com/index.php/jussi

Gambar 1. Mekanisme Checksum

2.4 Algortima Fletcher-32

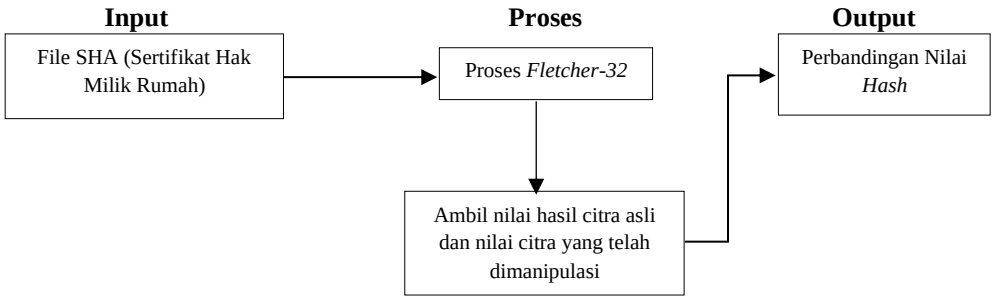
Flecher checksum adalah algoritma untuk memnghitung checksum tergantung posisi. Dibuat oleh John G. Fletcher (1934-2012) di Lawrence Livermore Labs pada akhir 1970-an. Tujuan dari checksum fletcher adalah untuk menyediakan properti deteksi kesalahan yang mendekati pemeriksaan redundansi siklik tetapi dengan upaya komputensi yang lebih rendah terkait dengan teknik penjumlahan [6].

Ketika data word dibagi menjadi blok 16-bit, dua jumlah hasil 16-bit dan digabung ke dalam checksum fletcher32-bit. Biasanya, jumlah kedua akan dikalikan dengan 216 dan ditambahkan ke checksum sederhana, secara efektif menumpuk jumlah berdampingan dalam kata 32-bit dengan checksum sederhana pada akhiryang paling tidak signifikan. Algoritma ini kemudian disebut sebagai fletcher-32 checksum. Pengggunaan modulus 216-1=65.535 juga umumnya tersirat. Alasan unttuk pilihan ini sama dengan fletcher-16.
Algoritma fletcher dapat dirumuskan sebagai berikut:
$A = 1 + D1 + D2 + \ldots + Dn \pmod{65535}$
$B = (1 + D1) + (1 + D1 + D2) + \ldots + (1 + D1 + D2 + \ldots + Dn) \pmod{65535}$
$= n \times D1 + (n - 1) \times D2 + (n - 2) \times D3 + \ldots + Dn + n \pmod{65535}$
Fletcher-32 (D) $= B \times 65536 + A$

3. HASIL DAN PEMBAHASAN

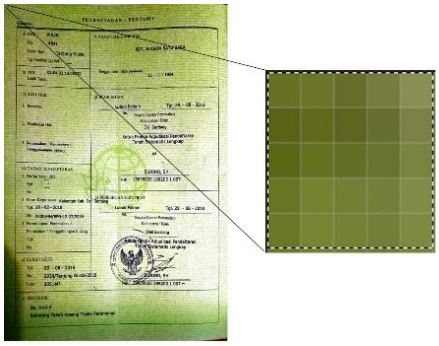
3.1 Analisa Algortima Fletcher-32

Proses pendeteksian dilakukan dengan menggunakan file citra sertifikat tanah dengan format JPEG dan resolusi 902 x 1280 pixel. Langkah yang dilakukan yaitu mencari pixel warna RGB dari hasil scan citra SHM (Sertifikat Hak Milik Rumah) yang dikonversi menjadi nilai grayscale menggunakan aplilkasi Matlab. Kemudian nilai pixel grayscale akan dihitung dengan menerapkan algoritma fletcher-32. Sehingga menghasilkan nilai hash melalui pixel grayscale dengan metode fletcher-32. Dari nilai hash tesebut yang akan menjadi kode identitas keaslian pada sertifikat, yang kemudian menjadi perbandingan pada sertifikat yang telah di duplikat. Adapun gambaran proses pendeteksian keaslian sertifikat menggunakan algoritma fletcher-32 seperti dibawah ini:



Gambar 2. Alur Analisa Penelitian

Analisa pada penelitian kali ini, dengan menggunakan sampel file citra sertifikat rumah dengan format JPEG. Mempunyai resolusi sebenarnya 902 x 1280 piksel, untuk mempermudah analisa maka sampel yang diambil pada sertifikat rumah yaitu ukuran 5 x 5 piksel. Hasil scan sertifikat rumah kemudian dikonversi ke RGB, yang merupakan nilai intensitas dari tiga kombinasi warna yang terdiri dari Red (Merah), Green (Hijau), Blue (Biru). Warna dasar ini kemudian dijumlahkan kemudian dibagi tiga untuk mendapatkan nilai rata-rata. Sehingga menghasilkan nilai tunggal pada kanal. Di mana dalam proses ini citra RGB telah dikonversi menjadi citra greyscale. File sertifikat yang digunakan dapat dilihat pada gambar di bawah ini.



Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 1-6
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3123
Website https://ejurnal.seminar-id.com/index.php/jussi

Gambar 3. File Citra Sertifikat Tanah

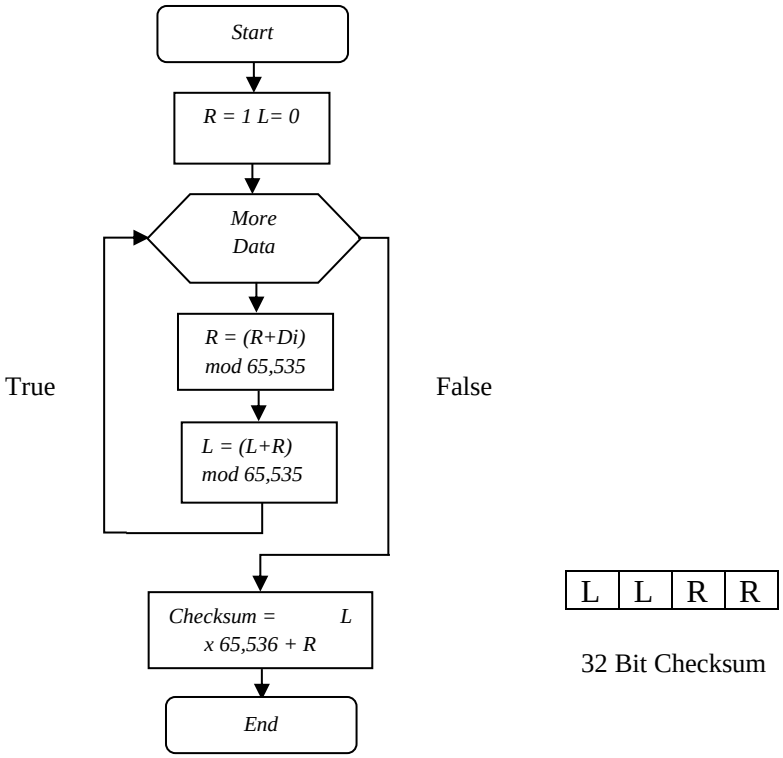
3.2 Pembahasan

Di bawah ini adalah tabel nilai *grayscale* dari citra sertifikat rumah yang telah diubah menjadi resolusi 5 x 5 piksel.

Tabel 1. Nilai grayscale dari citra sertifikat rumah

155	147	156	162	152
135	133	144	148	137
160	158	164	156	148
155	159	167	159	149
157	161	168	160	150

Berdasarkan tabel nilai grayscale yang di dapat, maka nilai inilah yang akan digunakan sebagai data untuk mencari nilai fletcher-32 selanjutnya. Alur pehitungan mencari nilai fletcher-32 dapat dilihat pada proses yang ditampilkan pada flowchart di bawah ini:



Gambar 4. Flowchart Fletcher-32

Keterangan:
L = Left 16-bit checksum
R = Right 16-bit checksum
Di = Next 16-bit data item

Data yang digunakan untuk menghitung Algoritma fletchert-32 yaitu berdasarkan nilai piksel grayscale yang telah didapat sebelumnya. Proses perhitungan bisa dilihat pada tabel di bawah ini:

Tabel 2. Proses Perhitunga *Fletchert-32*

No	Data	C1		C2	
1	155	1	+ 155 = 156	0	+ 156 = 156
2	147	156	+ 147 = 303	156	+ 303 = 459
3	156	303	+ 156 = 459	459	+ 459 = 918
4	162	459	+ 162 = 621	918	+ 621 = 1539
5	152	621	+ 152 = 773	1539	+ 773 = 2312
6	135	773	+ 135 = 908	2312	+ 908 = 3220
7	133	908	+ 133 = 1041	3220	+ 1041 = 4261
8	144	1041	+ 144 = 1185	4261	+ 1185 = 5446
9	148	1185	+ 148 = 1333	5446	+ 1333 = 6779
10	137	1333	+ 137 = 1470	6779	+ 1470 = 8249
11	160	1470	+ 160 = 1630	8249	+ 1630 = 9879

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 1-6
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3123
Website https://ejurnal.seminar-id.com/index.php/jussi

12	158	1630 + 158 = 1788	9879 + 1788 = 11667
13	164	1788 + 164 = 1952	11667 + 1952 = 13619
14	158	1952 + 158 = 2110	13619 + 2110 = 15729
15	148	2110 + 148 = 2258	15729 + 2258 = 17987
16	155	2258 + 155 = 2413	17987 + 2413 = 20400
17	159	2413 + 159 = 2572	20400 + 2572 = 22972
18	167	2572 + 167 = 2739	22972 + 2739 = 25711
19	159	2739 + 159 = 2898	25711 + 2898 = 28609
20	149	2898 + 149 = 3047	28609 + 3047 = 31656
21	157	3047 + 157 = 3204	31656 + 3204 = 34860
22	161	3204 + 161 = 3365	34860 + 3365 = 38225
23	168	3365 + 168 = 3533	38225 + 3533 = 41758
24	160	3533 + 160 = 3693	41758 + 3693 = 45451
25	150	3693 + 150 = 3843	45451 + 3843 = 49294

Checksum 1 (C1) = 3843 % mod fletcher-32
= 3843 % 65535
= 3843
= F03 hex (base 16)
Checksum 2 (C2) = 49294 % mod fletcher-32
= 49294 % mod 65535
= 49294
= C08E hex (base 16)
Output = 49,294 x 65,536 + 3,843
= 3230535427 (decimal)
= C08E0F03 (hexadecimal)

Jadi, nilai checksum yang didapat dari tabel di atas adalah 3230535427 dengan nilai hexadecimal yaitu C08E0F03. Hasil penjumlahan checksum 1 dan checksum 2 yang di dapat, sebelumnya telah dimodulus 216-1 atau 65.535. Proses di atas menunjukan dua hasil penjumlahan 16-bit. Di mana hasil dari C1 = F03 dan C2 = C08E. Ketika kedua hasil penjumlahan 16-bit digabungkan, maka akan menghasilkan nilai fletcher checksum-32 bit.

Selanjutnya, hasil perhitungan dengan metode fletcher-32 di atas akan dilakukan sedikit modifikasi atau perubahan pada nilai pixel yang asli atau sebelumnya. Hal ini untuk membuktikan fungsi dari checksum atau hash. Perubahan pada hash hanya dapat dideteksi oleh program komputer. Di bawah ini adalah tabel yang sudah mengalami modifikasi pada nilai grayscale dari hasil nilai grayscale yang asli.

Tabel 3. Nilai *Grayscale* proses modifikasi

155	147	156	162	152
135	133	144	148	137
160	158	164	156	148
155	159	167	159	149
157	105	166	160	150

Tabel 4. Proses Perhitungan modifikasi

No	Data	C1	C2
1	155	1 + 155 = 156	0 + 156 = 156
2	147	156 + 147 = 303	156 + 303 = 459
3	156	303 + 156 = 459	459 + 459 = 918
4	162	459 + 162 = 621	918 + 621 = 1539
5	152	621 + 152 = 773	1539 + 773 = 2312
6	135	773 + 135 = 908	2312 + 908 = 3220
7	133	908 + 133 = 1041	3220 + 1041 = 4261
8	144	1041 + 144 = 1185	4261 + 1185 = 5446
9	148	1185 + 148 = 1333	5446 + 1333 = 6779
10	137	1333 + 137 = 1470	6779 + 1470 = 8249
11	160	1470 + 160 = 1630	8249 + 1630 = 9879
12	158	1630 + 158 = 1788	9879 + 1788 = 11667
13	164	1788 + 164 = 1952	11667 + 1952 = 13619
14	158	1952 + 158 = 2110	13619 + 2110 = 15729
15	148	2110 + 148 = 2258	15729 + 2258 = 17987
16	155	2258 + 155 = 2413	17987 + 2413 = 20400
17	159	2413 + 159 = 2572	20400 + 2572 = 22972
18	167	2572 + 167 = 2739	22972 + 2739 = 25711
19	159	2739 + 159 = 2898	25711 + 2898 = 28609

Jurnal Sains Dan Teknologi Informasi
Vol 2, No 1, Desember 2022, Hal 1-6
ISSN 2809-610X (Media Online)
DOI 10.47065/jussi.v2i1.3123
Website https://ejurnal.seminar-id.com/index.php/jussi

20	149	2898 + 149 = 3047	28609 + 3047 = 31656
21	157	3047 + 157 = 3204	31656 + 3204 = 34860
22	105	3204 + 105 = 3309	34860 + 3309 = 38169
23	166	3309 + 166 = 3475	38169 + 3475 = 41644
24	160	3475 + 160 = 3635	41644 + 3635 = 45279
25	150	3635 + 150 = 3785	45279 + 3785 = 49064

Checksum 1 (C1) = 3785 % mod fletcher-32
= 3785 % 65535
= 3785
= EC9 hex (base 16)
Checksum 2 (C2) = 49064 % mod fletcher-32
= 49064 % mod 65535
= 49064
= BFA8 hex (base 16)
Output = 49,064 x 65,536 + 3,785
= 3215462089 (decimal)
= BFA80EC9 (hexadecimal)

Dari proses modifikasi pada table 4 hasil yang di dapat yaitu checksum 1 = EC9 hex dan checksum 2 = BFA8 hex, dengan hasil output yang di dapat yaitu BFA80EC9. Hasil yang di dapat berbeda dari pengujian sebelumnya dengan output yaitu C08E0F03. Checksum akan mendeteksi perubahan sekecil apapun pada nilai piksel dengan menggunakan algoritma fletchert-32. Dengan begitu keaslian sertifikat rumah akan terdeteksi. Tabel perbedaan nilai checksum pada sertifikat rumah dapat dilihat pada tabel di bawah ini:

Tabel 5. Perbedaan nilai *checksum* citra awal dan manipulasi

Citra		Nilai *Checksum*
Citra Awal		C08E0F03
Citra Manipulasi		BFA80EC9

4. KESIMPULAN

Dari hasil penelitian yang penulis lakukan, maka kesimpulan dapat di uraikan yaitu mendeteksi keaslian sertifikat rumah berhasil dilakukan dengan algoritma fletcher-32. Proses yang dilakukan untuk membedakan citra asli dan citra modifikasi yaitu dengan melakukan perhitungan menggunakan algoritma fletcher-32, sehingga menghasilkan nilai checksum yang berbeda pada setiap sertifikat. Pendeteksian dengan algoritma fletcher-32 dilakukan dengan menggunakan aplikasi Matlab, Keaslian sertifikat akan terlihat berdasarkan nilai checksum sebagai output pada sistem. Apabila nilai checksum berbeda dengan yang asli maka dapat dipastikan bahwa sertifikat tersebut telah mengalami modifikasi.

REFERENCES

[1] B. Schneier, Apply Cryptography, Electr Eng, 1996.
[2] M. D. Prihardhanto, "Studi Perbandingan Beberapa Fungsi Hash dalam Melakukan Checksum Berkas".
[3] Sumandri, "Studi Model Algoritma Kriptografi Klasik dan Modern," Semin. Mat. dan Pendidik. Mat. UNY, 2017.
[4] R. Munir, Pengolahan Citra Digital dengan Pendekatan Algoritmik, Bandung Informatika, 2004.
[5] M. K. E. S. S.Si, Kriptografi & Implementasinya Menggunakan MATLAB, CV ANDI OFFSET (Andi Yogyakarta), 2015.
[6] Wijayanto, Penggunaan CRC32 Dalam Integritas Data, 2006.