RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

Implementasi Metode MD2 Untuk Otentikasi Hasil Scan Citra Ijazah

Winda Wulan Sari[1*]

[1]Fakultas Ilmu Komputer dan Teknologi Informasi, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: [1*]windawulansari894@gmail.com

Abstrak−Ijazah menjadi salah satu syarat bagi seseorang yang hendak melamar pekerjaan, tetapi terkadang untuk mendapatkan hal tersebut, seseorang dapat melakukan kecurangan dengan memalsukan isi ijazahnya. Untuk itu diperlukan sebuah sistem yang dapat memberikan autentifikasi dari sebuah image ijazah. Dalam penelitian ini digunakan algoritma kriptografi yang akan di gabungkan dengan pengolahan citra untuk menjamin keamanan dari sebuah image atau ijazah. Dalam penelitian ini terdapat proses penyisipan dan proses keamanan yang menggunakan Metode MD2 sebagai media untuk penyelesaian pada implementasi Otentikasi hasil scan Citra Ijazah. Hasil penelitian ini menunjukkan bahwa aplikasi otentikasi dapat mendeteksi manipulasi ijazah

Kata Kunci: Ijazah, Kriptografi, Algortima MD2

Abstract−A diploma is one of the requirements for someone who wants to apply for a job, but sometimes to getthis, someone can commit fraud by falsifying the contents of the certificate. Forthat we need a system that can provide authentication of a diploma image. This research uses a cryptographic algorithm that will becombined with image processing to ensure the security of an image or certificate. In this study, there is an insertion process and a security process that uses the MD2 method as a medium for solving the implementation of the Authentication of the Ijazah image scan. The results of this study indicate that the authentication application can detect diploma manipulation

Keywords: Diploma, Cryptography, MD2 Algorithm.

1. PENDAHULUAN

Kriptografi merupakan penerapan yang dilakukan secara mendalam pada bidang akademis dengan menggunakan teknik matematis yang canggih, Kriptografi juga cabang dari ilmu matematika yang memiliki banyak fungsi dalam pengamanan data. Di dalam kriptografi, terdapat sebuah mekanisme yang bisa dipergunakan untuk mengamankan sistem dalam ke aslian untuk suatu file maupun data yang bersifat privasi, karena itu pada file dokumennya dienkripsikan untuk disembunyikan di sebuah file atau semua jenis file dapat dienkripsikan dan menggunakan jenis enkripsi berdasarkan fungsi yang akan diterapkan, seperti file citra dapat dienkripsi nilai pixelnya, digital signature atau penyisipan informasi rahasia.

Citra (gambar) digital dari ijazah hasil scan itu sendiri untuk mengetahui ke asliannya, di mana terdapat tampilan yang harus dikelola agar citra tersebut memenuhi tahapan-tahapan untuk melakukan sebuah penelitian yang menghasilkan ke aslian dari hasil scan ijazah tersebut, dalam citra digital terdapat proses perbaikan dan teknik pengolahan untuk memudahkan cara pengerjaan yang akan di lakukan untuk berbagai aktifitas online. Seperti lamaran kerja secara online dan pengiriman berkas secara online pada pelamaran tes CPNS, untuk itu perlu dilakukan langkah-langkah pada pendeteksian ke aslian scan citra dengan gabungan antara metode kriptografi dan pengolahan citra .

Otentikasi adalah suatu cara untuk memverifikasi apakah hal tersebut benar. Biasanya ini melibatkan metode yang menunjukan identitas sepeti kartu. Salah satu Metode yang berkaitan dengan otentikasi yaitu metode MD2 di mana di dalam pengerjaan metode tersebut terdapat beberapa aspek yang menghasilkan nilai hash yang berukurang 128-bit dan mampu menerima input dengan panjang yang tidak di tentukan. Otentikasi hasil scan cirta Ijazah merupakan suatu upaya untuk mengetahui adanya perubahan pada file citra ijazah dan MD2 digunakan sebagai fungsi keamanan dalam menyandingkan Biner file citra ijazah tersebut.

Algoritma Message-Digest atau yang di sebut MD2 dikembangkan pada tahun 1989 oleh Ron Rivest. spesifikasi aktual yang dapat ditemukan di RFC 1319 iyalah Algoritma yang memiliki kesamaan dengan MD4 dan Md5. MD2 adalah fungsi hash yang berorientasi byte. Memang semua intruksi untuk menangani 8 bit data itu sendiri dapat di lakukan dengan suatu intruksi yang berguna untuk arsitektur lama, Prosesor ini dapat memanipulasi kata-kata (setidaknya) 32 bit. Akibatnya semua hash modern menggunakan intruksi 32 bit[1].

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik matematis yang berhubungan dengan aspek keamanan informasi seperti tingkat keyakinan, integrasi data, autentikasi entitas dan autentikasi keaslian data. (*Menezes, Oorscho and Vanstonee, 1996*) Seni di defeniskan denga fakta sejarah bahwa setiap orang mempunyai cara masing – masing untuk mengamankan data, sehingga pesan memiliki nilai estetika tersendiri yang berhubungan dengan seni dan kebudayaan, jika di perhatikan secara mendalam *Gray* di dalam kriptografi memiliki makna sebuah seni. Keamanan juga membutuhkan teknik dan seni demikian pula dengan halnya keamanan pada data, kehandalan keamanan tergantung dari cara masing –masing dalam memahami penting dari data tersebut[2].

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

2.2 Citra Digital

Citra digital merupakan sebuah larik *(array)* yang berisi nilai-nilai real maupun komplek yang direpresentasikan dengan deretan bit tertentu. Citra yang disimpan dalam memori komputer hanyalah angka-angka yang menunjukkan besar intensitas pada masing-masing pixel tersebut. Sebuah citra digital dapat mewakili oleh sebuah matriks yang terdiri dari M kolom N baris, dimana perpotongan antara kolom dan baris disebut piksel (piksel = *picture element*) yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x,y) adalah f(x,y), yaitu besar intensitas atau warna dari piksel di titik [5].

2.3 Message Digest (MD2)

Message Digest 2 pertama kali dirancang pada tahun 1989 dan dirancang untuk komputer berbasiskan 8-bit. Detail tentang MD2 dapat dilihat di RFC 1319. Walaupun memiliki banyak flaw, sampai sekarang MD2 masih dipakai sebagai infrastruktur untuk sertifikat RSA. MD2 mengubah pesan string ke dalam kode heksadesimal 32 bit. Secara fisik, MD2 bekerja dengan mengkompresi 128 bit hash value dari pesan sembarang ke dalam blok-blok yang masing-masing berukuran 128 bit (16 byte) kemudian menambahkan sebuah checksum. Untuk kalkulasi yang sebenarnya, digunakan blok sebesar 48 byte dan tabel 256 byte yang dihasilkan secara tidak langsung. Apabila semua block dari pesan yang dipanjangkan telah diproses, fragmen pertama dari blok 48 byte menjadi hash value dari pesan[3].

Algortma MD2 dikembangkan oleh Ron Rivest pada tahun 1989. Algoritma ini dioptimasikan dengan menggunakan komputer 8-bit. MD2 sebenarnya dispesifikasikan dalam RFC 1319. Algoritma MD2 menghasilkan nilai hash yang berukuran 128-bit dan menerima input pesan dengan panjang yang tidak ditentukan. Pesan yang akan dijadikan input untuk fungsi hash ini akan terlebih dahulu akan dipadding. Untuk kalkulasi yang sebenarnya. Misalkan kita memiliki sejumlah b-byte pesan sebagai input, dan kita mengharapkan untuk dapat mendapatkan message digest dari pesan tersebut. Dalam hal ini, b merupakan suatu bilangan bulat sembarang yang bernilai positif, bisa juga nol, dan besarnya sembarang. Kita nyatakan bahwa byte dari pesan ditulis dalam bentuk. Di bawah ini akan dijelaskan 4 tahap proses untuk menghasilkan message digest untuk algoritma MD2.

1. Memasukkan Padding byte
   Pesan akan ditambahkan melalui proses padding sehingga panjang pesan tersebut kongruen dengan 0 modulo 16. Maka, pesan akan diperluas sehingga panjangnya merupakan kelipatan dari 16 byte. Proses padding ini selalu dilakukan meskipun panjang pesan awal sebelum dilakukan padding sudah kongruen dengan 0 modulo 16. Padding dilakukan dengan mengikuti : “i” byte dari nilai “i” akan ditambahkan pada pesan sehingga panjang pesan kongruen dengan 0 modulo 16. Maka ukuran padding byte paling sedikit 1 byte sampai 16 byte. Pada tahap ini pesan hasil padding memiliki panjang pesan kelipatan 16 byte. Kita bagi pesan menjadi M[0 . . . N-1] dimana N merupakan kelipatan 16.
2. Memasukkan Checksum
   Sebanyak 16 byte checksum dari pesan akan ditambahkan pada hasil dari tahap sebelumnya. Pada langkah ini digunakan sebuah 256-byte yang dibangkitkan secara acak yang dibuat dengan nilai digit dari pi. Jika S[i] menotasikan untuk elemen ke-i pada tabel.
3. Inisialisasi Penyangga MD
   Sebuah 48-byte penyangga X digunakan untuk menghasilkan message digest, nilai penyangga diinisialisasi dengan nol.
4. Proses pesan dalam blok 16-byte
   Langkah ini menggunakan angka hasil pemnbangkitan sebanya 256-byte yang sama yang dihasilkan pada proses 2.

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Analisa dilakukan untuk meneliti otentikasi hasil scan citra ijazah dengan menerapkan metode MD2. Adapun ijazah yang digunakan berjenis citra digital yang akan diberikan nilai hash MD2. Piksel citra ijazah diambil menggunakan aplikasi matlab dan dari piksel tersebut dilakukan encoding MD2, sehingga file citra ijazah memiliki identitas yang berfungsi sebagai autentikasi citra ijazah. Dengan demikian citra ijazah yang telah diberikan nilai hash MD2 pada saat mengalami perubahan oleh orang yang tidak bertanggung jawab dapat diketahui dengan cepat. Adapun proses yang terdapat pada pengerjaan metode MD2 tersebut melakuan sebanyak 5 kali step pengerjaan. Masalah dalam penerapan otentikasi MD2 pada citra digital ijazah yaitu, perubahan warna pada citra ijazah, akan tetapi dikarenakan data piksel warna yang digunakan untuk penempatan nilai hash MD2 hanya 16 Byte atau 3x4 pada area citra digital, perubahan tersebut dianggap tidak terlalu jelas atau signifikan. Untuk itu pengujian terhadap MD2 tentunya tidak mempersulit pemberian autentikasi citra ijazah hanya dikarenakan mengubah nilai citra digital ijazah tersebut.

3.1.1 Penerapan Algortima MD2

Pengerjaan yang pertama kali dilakukan adalah mengubah nilai RGB citra digital ijazah menjadi *grayscale* dan mendapatkan nilai pikselnya.

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

255	255	255
255	255	255
255	255	255
255	255	255

Berdasarkan pixel di atas diketahui nilai pixel yang terdapat pada citra tersebut diambil menggunakan aplikas matlab. Nilai-nilai pixel grascale iyalah nilai-nilai pixel yang akan diproses dengan menerapkan metode Message Digest Algorithm (MD2) untuk mengautentikasi hasil otentikasi terhadap citra ijazah itu sendiri. Demikian Nilai pixel diatas diproses sesuai dengan ketentuan dari metode Message Digest Algorithm (MD2).

1. Langkah 1 Memasukkan Padding byte :

Setelah nilai pixel didapat selanjutnya menambahkan 4 angka desimal dibelakang sehingga berjumlah menjadi 16 digit, seperti dibawah ini :

255	255	255	255	255	255	255	255	255	255	255	12	13	14	15
M_0	M_1	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}

Gambar 1. Pesan yang akan di enkrip

2. Langkah 2 Memasukkan Checksum :

Setelah dilakukannya penambahan angka desimal 12 13 14 15 selanjutnya dilakukan perhitungan sebanyak 16 kali perulangan, Seperti di bawah ini :

1. I= 0
   J=0
   L=0

Set C to M [i * 16+J]	Set C [j] to S [C XOR L]	Set L to C [J]
Set C to M [0*16+0]	Set C [0] to S [255 XOR 0]	Set L to [0]
Set C to M [0]	Set C [0] to S [255]	Set L to 20
Set C to 255	Set C [0] to 20	

2. I= 0
   J=1
   L=20

Set C to M [i * 16+J]	Set C [j] to S [C XOR L]	Set L to C [J]
Set C to M [0*16+1]	Set C [1] to S [255 XOR 20]	Set L to [1]
Set C to M [1]	Set C [1] to S [235]	Set L to 248
Set C to 255	Set C [1] to 248	

3. I= 0
   J=2
   L=248

Set C to M [i * 16+J]	Set C [j] to S [C XOR L]	Set L to C [J]
Set C to M [0*16+2]	Set C [3] to S [255 XOR 248]	Set L to [2]
Set C to M [2]	Set C [3] to S [7]	Set L to 1
Set C to 255	Set C [3] to 1	

4. I= 0
   J=3
   L=1

Set C to M [i * 16+J]	Set C [j] to S [C XOR L]	Set L to C [J]
Set C to M [0*16+3]	Set C [4] to S [255 XOR 1]	Set L to [4]
Set C to M [4]	Set C [4] to S [254]	Set L to 131
Set C to 255	Set C [4] to 131	

5. I= 0
   J=4
   L=131

Set C to M [i * 16+J]	Set C [j] to S [C XOR L]	Set L to C [J]
Set C to M [0*16+4]	Set C [5] to S [255 XOR 131]	Set L to [5]
Set C to M [4]	Set C [5] to S [124]	Set L to 156
Set C to 255	Set C [5] to156	

Untuk penyelesaian berikut tetap menggunakan cara yang sama dengan ketentuan perulangan dan hasil perulangan tersebut dapat dilihat dalam Tabel berikut.

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

M0	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15
20	248	1	131	156	179	11	143	79	44	139	150	97	172	163	186

3. Langkah 3 Inisialisasi Penyangga MD :

Untuk melakuan Inisialisasi Penyangga MD nilai pixel 3x4 di urutkan dengan menggabungkan perbaris. Hasil penggabungan tersebut dapat di lihat seperti tabel berikut ini

Tabel 1. Inisialisasi Penyangga MD

M_0	M_1	M_2	M_3	M_4	M_5	M_6	M_7
255	255	255	255	255	255	255	255
M_8	M_9	M_{10}	M_{11}	M_{12}	M_{13}	M_{14}	M_{15}
255	255	255	11	12	13	14	15
M_{16}	M_{17}	M_{18}	M_{19}	M_{20}	M_{21}	M_{22}	M_{23}
L	L	L	L	L	L	L	L
M_{24}	M_{25}	M_{26}	M_{27}	M_{28}	M_{29}	M_{30}	M_{31}
L	L	L	L	L	L	L	L

Initial MD Buffer

Buffer X = 00000000 00000000 00000000 00000000 00000000 00000000

Tabel 2. Initial MD buffer X

X0	X1	X2	X3	X4	X5	X6	X7
0	0	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
0	0	0	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	0	0	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

4. Langkah 4 Proses pesan dalam blok 16-byte :

Process message in 16 byte blocks

Copy blok i into x

For J = “0 To 15”

1. J = 0, i = 0

   Set x [16+ j] To M [i * 16 + j]

   Set x [16 + 0] To M [0 * 16 + 0]

   Set x [16] To M [0]

   Set x [16] To 255

   Set x [32 + j] To x [16 + j] xor x [j]

   Set x [32 + 0] To x [16 + 0] xor x [0]

   Set x [32] To x [16] xor x [0]

   Set x [32] To 0 xor 0

   Set x [32] To 0

   X = 00000000 00000000 2550000000 00000000 00000000 00000000

Tabel 3. Proses pesan dalam blok

X0	X1	X2	X3	X4	X5	X6	X7
0	0	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
255	0	0	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	0	0	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

2. J = 1, i = 0
   Set x [16 + 1] To M [i * 17 + j]
   Set x [16 + 1] To M [0 * 17 + 1]
   Set x [17] To M [1]
   Set x [17] To 255
   Set x [32 + j] To x [17 + j] xor x [j]
   Set x [32 + 1] To x [17 + 1] xor x [1]
   Set x [33] To x [18] xor x [1]
   Set x [33] To 19 xor 0
   Set x [33] To 19
   X = 00000000 00000000 255255000000 00000000 00000000 00000000

Tabel 4. Inisialisasi Penyangga MD

X0	X1	X2	X3	X4	X5	X6	X7
0	0	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
255	255	0	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	19	0	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

3. J = 2, i = 0
   Set x [16 + j] To M [i * 16 + j]
   Set x [16 + 2] To M [0 * 16 + 2]
   Set x [18] To M [2]
   Set x [18] To 255
   Set x [32 + j] To x [18 + j] xor x [j]
   Set x [32 + 2] To x [18 + 2] xor x [2]
   Set x [34] To x [20] xor x [2]
   Set x [34] To 22 xor 0
   Set x [34] To 22
   X = 00000000 00000000 25525525500000 00000000 00000000 00000000

Tabel 5. Inisialisasi Penyangga MD

X0	X1	X2	X3	X4	X5	X6	X7
0	0	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
255	255	255	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	19	22	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

4. J = 3, i = 0
   Set x [16+ j] To M [i * 16 + j]
   Set x [16 + 3] To M [0 * 16 + 3]
   Set x [19] To M [3]
   Set x [19] To 255
   Set x [32 + j] To x [19 + j] xor x [j]
   Set x [32 + 3] To x [19 + 3] xor x [3]
   Set x [35] To x [23] xor x [3]
   Set x [35] To 20 xor 0
   Set x [35] To 20
   X = 00000000 00000000 2552552552550000 00000000 00000000 00000000

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

Tabel 6. Inisialisasi Penyangga MD

X0	X1	X2	X3	X4	X5	X6	X7
0	0	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
255	255	255	255	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	19	22	20	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

5. J = 4, i = 0
   Set x [16+ j] To M [i * 16 + j]
   Set x [16 + 4] To M [0 * 16 + 4]
   Set x [20] To M [4]
   Set x [20] To 255
   Set x [32 + j] To x [20 + j] xor x [j]
   Set x [32 + 4] To x [20 + 4] xor x [4]
   Set x [36] To x [23] xor x [4]
   Set x [36] To 19 xor 0
   Set x [36] To 19
   X = 00000000 00000000 255255255255255000 00000000 00000000 00000000

Tabel 7. Inisialisasi Penyangga MD

X0	X1	X2	X3	X4	X5	X6	X7
0	0	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
255	255	255	255	255	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	19	22	20	19	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

Untuk penyelesaian berikut tetap menggunakan cara yang sama dengan ketentuan perulangan dan hasil perulangan tersebut dapat dilihat dalam Tabel berikut.

Tabel 8. Inisilaisasi Penyangga MD

X0	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Gambar 9. Inisialisasi Penyangga MD

X16	X17	X18	X19	X20	X21	X22	X23	X24	X25	X26	X27	X28	X29	X30	X31
255	255	255	255	255	255	255	255	255	255	255	255	12	13	14	15

Tabel 10. Hasil Inisialisasi Penyangga MD

X32	X33	X34	X35	X36	X37	X38	X39	X50	X41	X42	X43	X44	X45	X46	X47
0	19	22	20	19	31	26	25	40	43	41	45	36	39	34	33

Langkah 5 output:

1. K = 0 T = 0
   Set T and X [K] To x [K] xor S [T]
   Set T and X [0] To x [0] xor S [0]
   Set T and X [0] To 0 xor 41
   Set T and X [0] To 41
   T = 41

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

Tabel 11. output MD

X0	X1	X2	X3	X4	X5	X6	X7
41	0	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
0	0	0	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	0	0	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

2. K = 1 T = 41
   Set T and X [K] To x [K] xor S [T]
   Set T and X [1] To x [1] xor S [41]
   Set T and X [1] To 1 xor 41
   Set T and X [1] To 46
   T = 46

Tabel 12. output MD

X0	X1	X2	X3	X4	X5	X6	X7
41	46	0	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
0	0	0	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	0	0	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

3. K = 2 T = 46
   Set T and X [K] To x [K] xor S [T]
   Set T and X [2] To x [2] xor S [46]
   Set T and X [2] To 2 xor 46
   Set T and X [2] To 67
   T = 67

Tabel 13. output MD

X0	X1	X2	X3	X4	X5	X6	X7
41	46	67	0	0	0	0	0
X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	0	0	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

4. K = 3 T = 67
   Set T and X [K] To x [K] xor S [T]
   Set T and X [3] To x [3] xor S [67]
   Set T and X [3] To 3 xor 67
   Set T and X [3] To 201
   T = 201

Tabel 14. output MD

X0	X1	X2	X3	X4	X5	X6	X7
41	46	67	201	0	0	0	0

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

X8	X9	X10	X11	X12	X13	X14	X15
0	0	0	0	0	0	0	0
X16	X17	X18	X19	X20	X21	X22	X23
0	0	0	0	0	0	0	0
X24	X25	X26	X27	X28	X29	X30	X31
0	0	0	0	0	0	0	0
X32	X33	X34	X35	X36	X37	X38	X39
0	0	0	0	0	0	0	0
X40	X41	X42	X43	X44	X45	X46	X47
0	0	0	0	0	0	0	0

5. K = 4 T = 201
   Set T and X [K] To x [K] xor S [T]
   Set T and X [4] To x [4] xor S [201]
   Set T and X [4] To 4 xor 201
   Set T and X [4] To 162
   T = 1

Untuk penyelesaian berikut tetap menggunakan cara yang sama dengan ketentuan perulangan dan hasil perulangan tersebut dapat dilihat dalam Tabel berikut.

Tabel 15. hasil nilai X keseluruhan

X0	X1	X2	X3	X4	X5	X6	X7
41	46	67	201	162	216	124	1
X8	X9	X10	X11	X12	X13	X14	X15
61	54	84	161	236	240	6	19
X16	X17	X18	X19	X20	X21	X22	X23
98	167	5	243	192	199	115	140
X24	X25	X26	X27	X28	X29	X30	X31
152	147	43	217	188	76	130	202
X32	X33	X34	X35	X36	X37	X38	X39
30	155	87	60	253	212	224	22
X40	X41	X42	X43	X44	X45	X46	X47
103	66	111	24	138	23	229	18

Setelah nilai X nya didapat kita mengubah bilangan Desimalnya menjadi Biner sesuai dengan nilai X yang terdapat pada Tabel 15. yang tertera diatas, seperti dibawah ini :

Tabel 16. hasil nilai X diubah menjadi biner

X0	X1	X2	X3	X4	X5	X6	X7
101001	101110	1000011	11001001	10100010	11011000	1111100	1
X8	X9	X10	X11	X12	X13	X14	X15
111101	110110	10101100	10100001	11101100	1110000	110	10011
X16	X17	X18	X19	X20	X21	X22	X23
111101	110110	10101100	10100001	11101100	1110000	110	10011
X24	X25	X26	X27	X28	X29	X30	X31
10011000	10010011	101011	11011001	10111100	1001100	10000010	11001010
X32	X33	X34	X35	X36	X37	X38	X39
11110	10011011	1010111	111100	11111101	11010100	11100000	10110
X40	X41	X42	X43	X44	X45	X46	X47
1100111	1000010	1101111	11000	10001010	10111	11100101	10010

Nilai biner di atas di konversi ke hexsa dan hasil perubahannya menjadi message diges MD2 bawah ini:
292E43C9A2D87C13D36ACA1EC7061398932BD9BC4C82CA1E9B573CFDD4E01667426F188A17E512

3.2. Implementasi

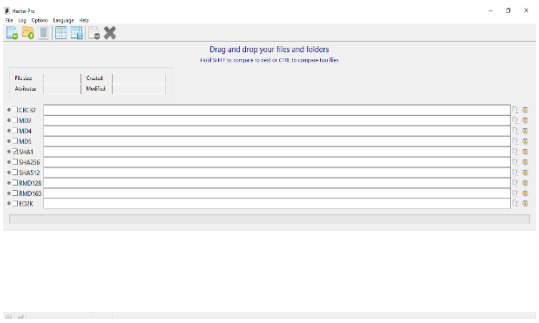
Implementasi MD2 untuk mendeteksi keaslian citra menggunakan HasherPro. Terdapat dua citra, yaitu satu citra yang asli dan satu yang palsu atau telah diubah. Pada citra yang dijadikan citra yang asli diberikan hasil encoding dari MD2 ke piksel citra asli tersebut dengan pengerjaan sebanyak 5 tahap. Tahapan implementasi terdari dari kebutuhan sistem computer yang digunakan dan hasil pengujian citra. Pengujian yang dilakukan menggunakan perangkat keras dengan perincian yang terdapat pada komputer Laptop Lenovo IdeaPad 300. Adapun spesifikasi computer yang digunakan, yaitu :

1. Perangkat Keras
   a. Prosesor : Intel Celeron N3150 1,6 Ghz 1,6 Ghz
   b. Memory : RAM 2 GB

c. Harddisk : Seagate 500 GB
d. Monitor : LCD 15 Inci

2. Perangkat Lunak
   a. Sistem Operasi : Microsoft Windows 7 32bit
   b. Aplikasi : Hasher Pro V3.2

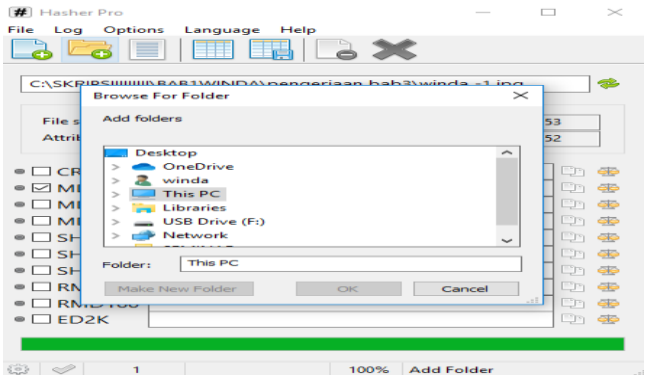
Aplikasi Pengujian implementasi metode MD2 untuk otentikasi hasil scan citra ijazah yang akan dilakukan pengujian hasil dari pembentukan kode fungsi Hash dengan menerapkan metode MD2 yang digunakan untuk hasil dari implementasi metode MD2 yang mendeteksi keaslian dengan menggunakan aplikasi Hasher Pro sebagai berikut :



Gambar 1. Aplikasi Hasher Pro

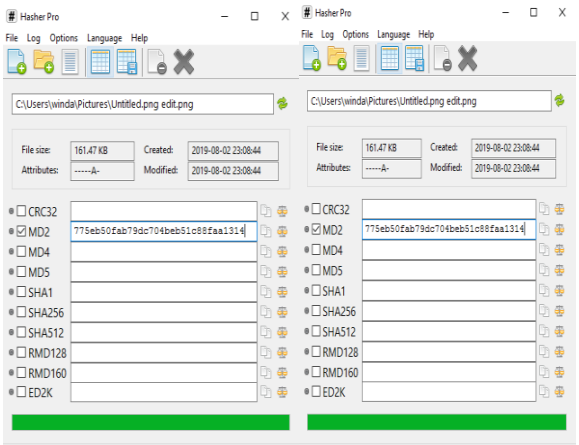
Pada Form yang digunakan Pada Aplikasi Hasher Pro tersebut terdapat beberapa langkah yang dapat dilakukan oleh user untuk menjalankan pengujian implementasi metode MD2 untuk mendeteksi file hasil scan citra ijazah di antara nya

1. Menginputkan File Citra ijazah
   Menginputkan file citra ijazah adalah proses dimana memanggil file dokumen yang akan di cari nilai MD2 seperti tampilan gambar 2.



Gambar 2. MengimputkanFile Awal

2. Memilih Metode MD2
   Memilih metode MD2 adalah proses dimana memilih metode yang digunakan untuk mendapatkan hasil dari metode MD2 ,berikut hasil dari pengujian aplikasi Hasher Pro yang asli maupun yang telah di edit.



Gambar 3. Memilih Metode MD2

ISSN 2745-7966 (Media Online)
Vol 1, No 5, Mei 2021
Hal 302-311
https://djournals.com/resolusi

4. KESIMPULAN

Berdasarkan pengembangan yang telah dilakukan selama proses implementasi. Hasil yang diperoleh dari penelitian yang dilakukan untuk otentikasi hasil scan citra ijazah mengunakan Metode MD2, maka dapat diambil kesimpulan Proses autentikasi citra ijazah dengan cara mendapatkan digital signature file citra ijazah yang berbentuk hash. Penerapan metode MD2 digunakan untuk encoding nilai piksel citra input ijazah dan menjadikan hasil hash sebagai nilai baru pada piksel citra ijazah. Metode MD2, hanya digunakan untuk keamanan citra digital tetapi tidak dapat melakukan otentikasi scan citra ijazah.

REFERENCES

[1] DCSSI Crypto Lab 51, Boulevard de Latour-Maubourg, 75700 Paris 07 SP France Frederic.Muller@sgdn.pm.gouv.fr
[2] Kriptografi untuk Keamanan Data/ oleh Harun Mukhtar.—Ed.1,Cet. 1- Yogyakarta: Deepublish, November 2018.
[3] N. Rogier, Fungsi Kompresi MD2 tidak bebas tabrakan,Wilayah yang dipilih dalam Kriptografi. Kanada, 1995.
[4] P. A. Md and D. A. N. Md, "Perbandingan algoritma md2, md4, dan md5," pp. 1–15.
[5] D. Nasution, Pengolahan Citra Digital. Darma Putra, 2010.
[6] P. N. Andono, Pengolahan Citra Digital. Yogyakarta: Andi, 2017.
[7] https://www.den4b.com/products/hasher/