

Implementasi Metode MD2 Untuk Autentikasi Hasil Citra Rontgen (Ronsen)

Mahanum Harahap

Fakultas Ilmu Komputer dan Teknologi Informasi, Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: hanumharahap12@gmail.com

Abstrak-Implementasi dianggap sebagai wujud utama dan tahap yang sangat menentukan dalam proses kebijakan atau pelaksana rencana yang telah disusun secara cermat dan rinci bahwa tanpa implementasi yang efektif keputusan pembuat kebijakan tidak akan berhasil dilaksanakan, Implementasi juga dapat diartikan sebagai serangkaian tindakan yang dilakukan oleh berbagai aktor pelaksana kebijakan dengan sarana-sarana pendukung berdasarkan aturan-aturan yang telah ditetapkan untuk mencapai tujuan yang telah ditetapkan. Autentikasi juga dapat diartikan sebagai hal yang sangat penting dalam pengiriman informasi baik berbentuk data ataupun pesan teks. Hal ini dapat dikarenakan dibutuhkannya autentikasi terhadap suatu keaslian isi dari data tersebut, dengan adanya autentikasi tersebut penggunaan sistem autentikasi diharapkan dapat membentuk suatu sistem yang khusus pada bidang tersebut, salah satu contohnya adalah pada implementasi hasil citra rontgen yang mana keaslian dari data tersebut harus benar-benar real dengan hasil yang didiagnosa dokter terhadap pasien. Metode Message Digest Algorithm 2 (MD2) dapat diartikan sebagai fungsi hash cryptographic yang dikembangkan oleh Ron Rivest pada tahun 1989, algoritma ini dioptimalkan dengan menggunakan komputer 8-bit. MD2 sebenarnya dispesifikasikan dalam RFC 1319 Dan algoritma MD2 menghasilkan nilai hash yang berukuran 18-bit dan menerima input pesan dengan panjang yang tidak ditentukan. Dengan metode ini diharapkan mampu menyelesaikan masalah yang kerap terjadi pada hasil rontgen agar proses yang dilakukan untuk menerapkan hasil citra rontgen dengan diagnosa dokter teruji nilai kepalidasiannya berdasarkan dengan metode MD2, maka dibangun suatu aplikasi dengan menggunakan aplikasi "Hasher Lite" guna untuk membuktikan hasil dari keseluruhan tersebut.

Kata Kunci: Implementasi, Autentikasi, Metode Message Digest Algorithm 2 (MD2)

Abstract-Implementation is considered as the main form and a crucial stage in the policy-making process or the implementation of a carefully and detailed plan, that without effective implementation, policy decisions will not be successfully executed. Implementation can also be interpreted as a series of actions carried out by various policy implementers with supporting means based on established rules to achieve predetermined goals. Authentication can also be interpreted as a very important thing in delivering information, both in the form of data or text messages. This is because authentication is needed for the authenticity of the contents of the data, with the existence of authentication, the use of authentication systems is expected to form a specific system in that field, one example is the implementation of X-ray image results where the authenticity of the data must be truly real with the results diagnosed by the doctor on the patient. The Message Digest Algorithm 2 (MD2) method can be interpreted as a cryptographic hash function developed by Ron Rivest in 1989, this algorithm is optimized using an 8-bit computer. MD2 is actually specified in RFC 1319 and the MD2 algorithm produces a hash value that is 18 bits in size and accepts input messages with an unspecified length. With this method, it is expected to solve problems that often occur in X-ray results so that the process of applying X-ray image results with doctor's diagnosis is tested for its authenticity value based on the MD2 method, then an application is built using the "Hasher Lite" application to prove the results of the whole process.

Keywords: Implementation, Autentication, Message Digest Algorithm 2 Method (MD2)

1. PENDAHULUAN

Komputer merupakan perangkat teknologi yang sudah tidak asing lagi, baik di perusahaan, di lembaga pendidikan, di lembaga sosial, dan masyarakat maupun di rumah. Teknologi ini terus berkembang dari tahun ke tahun seiring dengan kemampuan dan kecepatannya dalam memproses data dan memberikan informasi kepada pengguna. Perkembangan teknologi komputer demikian pesatnya, yang memiliki fungsi awal sebagai alat bantu dalam menyelesaikan persoalan dan masalah dalam segala bidang kemudian memasuki fungsi sebagai penambahan ilmu pengetahuan. Hal ini ditandai dengan banyak produk-produk yang berbasis komputer dalam dunia teknologi.

Manusia pada umumnya menderita suatu penyakit yang berbeda-beda. Penyakit manusia timbul dari berbagai faktor yang berbeda-beda seperti pikiran, makanan, lingkungan sekitar dan lain sebagainya. Penyakit yang diderita akan di diagnosa oleh seorang dokter spesialis untuk mengetahui jenis penyakit yang diderita. Dalam memastikan hasil diagnosa tersebut maka perlu dilakukan rontgen. *Rontgen* merupakan tindakan menggunakan radiasi untuk mengambil gambar bagian dalam dari tubuh seseorang. *Rontgen* digunakan untuk pengecekan masalah kesehatan yang ditimbulkan oleh berbagai jenis penyakit yang diderita atau juga sebagai pemantauan kondisi kesehatan seseorang. Hasil *rontgen* terdapat berbagai jenis sesuai dengan penyakit yang dialami. Hasil diagnosa dengan hasil *rontgen* terkadang tidak sesuai, maka perlu dilakukan autentikasi kebenaran dari hasil diagnosa dengan hasil *rontgen*.

Permasalahan mengenai keamanan hasil citra *rontgen* yang kerap terjadi di beberapa rumah sakit yaitu diantaranya terkadang hasil *rontgen* tidak sesuai harapan akan kebenaran yang didapat, mengambil citra *rontgen* adalah proses mendiagnosa penyakit yang diderita manusia. Sebuah rumah sakit yang mempunyai alat yang digunakan untuk mengambil citra *rontgen* tentunya memiliki banyak *file* hasil citra *rontgen*. Untuk mengamankan citra *rontgen* dan melakukan autentikasi maka perlu suatu metode yang membantu dalam melihat keaslian *file* citra *rontgen*. Dalam melakukan autentikasi hasil diagnosa dengan hasil *rontgen* perlu menggunakan metode penyelesaian. Metode yang

digunakan dalam mengautentikasi hasil diagnosa dengan hasil *rontgen* yaitu metode Message Digest Algorithm 2 (MD2). Dimana metode Message Digest Algorithm 2 (MD2) merupakan salah satu dari fungsi hash.

Metode Message Digest Algorithm 2 ini yaitu, fungsi hash cryptographic yang di kembangkan oleh Ron Rivest pada tahun 1989, algoritma ini dioptimalkan dengan menggunakan Komputer 8-bit. MD2 sebenarnya dispesifikasikan dalam RFC 1319. Algoritma MD2 menghasilkan nilai Hash yang berukuran 18-bit dan menerima input pesan dengan panjang yang tidak ditentukan[1].

Metode MD2 juga dapat diartikan sebagai algoritma yang termasuk ke dalam keluarga algoritma bersama dengan MD4 dan MD5. dan memiliki fungsi, Dikembangkan oleh Ron Rivest, untuk keamanan RSA. Bagaimana, di bandingkan dengan yang lain algoritma keluarga, (dan fungsi hash yang paling aktual). MD2 juga dapat menghasilkan pesan dari 128 bit[2].

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. keamanan informasi[2] Berikut ini adalah rangkuman beberapa mekanisme yang berkembang pada kriptografi modern :

- Fungsi *Hash*, fungsi Hash adalah fungsi yang melakukan pemetaan pesan dengan panjang sembarangan ke sebuah teks khusus yang disebut *message digest* dengan panjang tetap. Fungsi *hash* umumnya dipakai sebagai nilai uji (*check value*) pada mekanisme keutuhan data.
- Penyandian dengan kunci asimetrik (*Asymmetric key encipherment*). Penyandian dengan kunci simetrik adalah penyandian yang kunci enkripsi dan kunci dekripsi bernilai sama. Kunci pada penyandian simetrik diasumsikan bersifat rahasia hanya pihak yang melakukan enkripsi dan dekripsi yang mengetahui niainya. Oleh karena itu penyandian dengan kunci simetrik disebut juga penyandian dengan kunci rahasia *secret key encipherment*.
- Penyandian dengan kunci asimetrik (*Asymmetric key encipherment*). Penyandian dengan kunci asimetrik atau sering juga disebut dengan penyandian kunci publik (*public key*) adalah penyandian dengan kunci enkripsi dan dekripsi berbeda nilai. Kunci enkripsi yang juga disebut dengan kunci publik (*public key*) bersifat terbuka. Sedangkan, kunci dekripsi yang juga disebut kunci privat (*private key*) bersifat tertutup/rahasia.

2.2 Citra Digital

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman pada data yang bersifat optik berupa foto, bersifat analog berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang dapat langsung disimpan pada suatu media penyimpanan. Citra juga memiliki kombinasi antara titik, garis, bidang, dan warna untuk menciptakan suatu imitasi dari suatu objek biasanya objek fisik atau manusia. Citra bisa berwujud gambar (picture) dua dimensi, seperti lukisan, foto, dan berwujud tiga dimensi, seperti patung[6].

Citra digital adalah gambar dua dimensi yang bisa ditampilkan pada layar komputer sebagai nilai digital yang disebut dengan pixel. Sebuah citra grayscale ukuran 150 x 150 piksel (elemen terkecil dari sebuah citra) diambil sebagian (kotal kecil) berukuran 9 x 9 piksel. Maka, monitor akan menampilkan sebuah kotak kecil. Namun, yang disimpan dalam memori komputer hanyalah angka-angka yang menunjukkan besar intensitas pada masing-masing piksel tersebut[6]. Ada banyak cara untuk menyimpan citra digital didalam memori. Cara penyimpanan menentukan jenis citra digital yang terbentuk. Beberapa jenis citra digital yang sering digunakan adalah citra biner, citra grayscale, dan citra warna.

2.3 Message Digest Algorithm 2 (MD2)

Metode Message Digest Algorithm 2 adalah fungsi hash cryptographic yang dikembangkan oleh Ron Rivest pada tahun 1989, algoritma ini dioptimalkan dengan menggunakan komputer 8-bit. MD2 sebenarnya dispesifikasikan dalam RFC 1319. Algoritma MD2 menghasilkan nilai Hash yang berukuran 18-bit dan menerima input pesan dengan panjang yang tidak ditentukan. Metode MD2 juga termasuk kedalam algoritma bersama dengan MD4 dan MD5, dan memiliki fungsi untuk keamanan RSA (fungsi hash yang paling aktual) MD2 juga dapat menghasilkan pesan dari 128 bit[5].

2.4 Rontgen

Rontgen adalah bagian dari penerapan ilmu radiologi, ilmu radiologi adalah ilmu yang mencakup dua bidang penting yaitu radiodiagnostik dan radioterapi. Makna radioterapi adalah pengobatan penyakit dengan menggunakan radiasi. Sedangkan radiodiagnostik adalah diagnosis menggunakan sinar pengion. Pemeriksaan radiodiagnostik secara umum menggunakan sinar-X. Pada proses *capture* atau pengambilan foto rontgen sering terdapat *noise* dan membuat informasi yang ditampilkan tidak jelas atau rancu. Proses peningkatan kualitas dilakukan dengan cara melakukan peralatan *pixel* ketetapan, dengan maksud meratakan setiap *pixelnoise* dengan *pixel* citra dan menghilangkan *noise*. Proses komputasi dimensi marik yang besar membutuhkan waktu proses yang lama sehingga diperlukan reduksi dimensi matrik untuk meminimalisir waktu proses[8].

Rontgen juga dapat diartikan sebagai sebuah foto dari bayangan. Pemeriksaan diagnostic dengan sinar pengion (foto rontgen dan juga pemeriksaan dengan isotop radioaktif), mempertinggi kemungkinan terkena kanker tertentu. Pada pembuatan foto rontgen digunakan dasar bahwa organ-organ menahan lebih banyak sinar atau lebih sedikit yang lewat. Sebuah foto rontgen adalah sebuah foto dari bayangan beraneka struktur yang letaknya satu menumpuk diatas yang lain. Oleh karena itu foto rontgen selalu berupa foto negatif dan hitam-abu-putih.

3. HASIL DAN PEMBAHASAN

3.1 Analisa

Analisa dilakukan untuk meneliti Autentikasi hasil citra rontgen dengan menerapkan metode MD2. Adapun hasil rontgen yang digunakan berjenis citra digital yang akan diberikan nilai hash MD2. Pixel citra rontgen diambil menggunakan aplikasi matlab dan dari pixel tersebut dilakukan encoding MD2, sehingga file citra rontgen memiliki identitas yang berfungsi sebagai autentikasi citra rontgen. Dengan demikian citra rontgen yang telah diberikan nilai hash MD2 pada saat mengalami perubahan oleh orang yang tidak bertanggung jawab dan sehingga hasil citra rontgen dengan hasil yang didiagnosa dokter terhadap pasien dapat diuji kepalidasiannya secara terperinci.

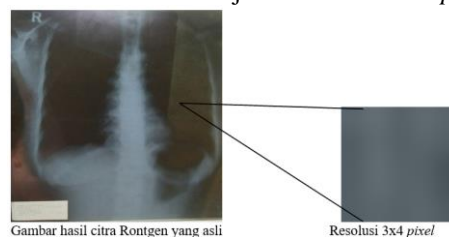
Gambar yang dianalisa adalah gambar dari sebuah hasil rontgen, dan dari gambar tersebut peneliti dapat mengetahui hasil dari diagnosa dokter dengan hasil rontgen tersebut apakah benar-benar sama keefesiensinya, setiap manusia pasti pernah mengalami yang namanya sakit, dan tergantung sakit yang diderita oleh pasien apakah perlu dilakukan rontgen atau tidak itu tergantung kepada dokter yang menanganinya, disebahagian rumah sakit pasti pernah mengalami kendala dalam menangani pasien termasuk dalam mendiagnosa penyakit pasien, salah satu contoh terjadinya kendala adalah berkas riwayat penyakit pasien dengan berkas riwayat penyakit pasien yang riwayat penyakitnya berbeda tertukar atau salah menempatkan, Maka dari itu peneliti melakukan penguraian dari masalah yang terurai diatas guna untuk mencegah terjadinya hal yang tidak diinginkan dalam melakukan sebuah rontgen terhadap orang yang sedang mengalami sakit atau perlunya dilakukan rontgen terhadap pasien tersebut.

Berdasarkan dari gambaran diatas dapat disimpulkan tahapan kerja dalam file memiliki proses berupa data masukan, proses utama dan keluaran yang diuraikan sebagai berikut :

- Data yang dimasukkan berupa file berekstensi JPG.
- Proses pertama bagaimana cara pengerjaan metode MD2.
- Hasil yang akan dikeluarkan (output) berupa file dengan bentuk huruf hexadesimal.

3.2 Contoh Kasus

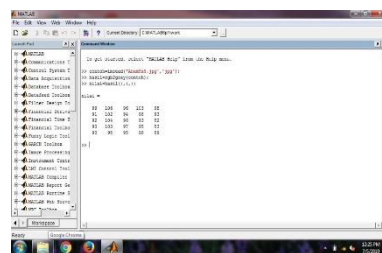
Berikut adalah gambar hasil citra rontgen Gambar tersebut diambil dari sebuah hasil rontgen yang aslinya, Gambar dibawah ini merupakan gambar berukuran dan diubah menjadi berukuran 3×4 pixel.



Gambar 1. Pengambilan Nilai Pixel Yang Akan Diproses

Adapun langkah-langkah untuk mengambil nilai-nilai *pixel* citra rontgen dengan matlab adalah :

- Buka aplikasi MATLAB.
- Siapkan gambar grayscale bertipe JPEG dan simpan direktori.
- Langkah selanjutnya tuliskan listing program.
- Selanjutnya akan ditampilkan nilai *pixel* yang berisikan nilai berikut ini :



Gambar 2. Citra Grayscale dengan Pixel 3x4

Berdasarkan *pixel* diatas diketahui nilai *pixel* citra tersebut diambil menggunakan aplikasi matlab. Dimana nilai-nilai *pixel* grayscale nilai-nilai *pixel* tersebut akan diproses dengan menerapkan metode Message Digest Algorithm 2

(MD2) untuk mengautentikasi hasil rontgen tersebut. Nilai *pixel* diatas diproses sesuai dengan ketentuan dari metode Message Digest Algorithm 2 (MD2).

Tabel 1. Nilai *Pixel* 3x4

99	106	96
91	102	94
92	104	96
93	103	97

Langkah 1 :

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

99	106	96
91	102	94
92	104	96
93	103	97

99	106	96	102	94	92	104	96	93	103	97	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

Langkah 2 :

Setelah dilakukannya penambahan angka desimal 12 13 14 15, Seperti dibawah ini :

1. I = 0
- J = 0
- L = 179
- Set C To M [i x 16 + J]
- Set C To M [0 x 16 + 0]
- Set C To M [0]
- Set C To 99
- Set C [J] To S [C xor L]
- Set C [0] To S [99 xor 0]
- Set C [0] To S [99]
- Set C [0] To 179
- Set L To C [J]
- Set L To C [0]
- Set L To 179

Langkah 2 dapat dilakukan sampai 16 kali atau sampai perhitungan ke 16 perulangan, setelah melakukan perulangan sampai 16 maka akan dilakukan langkah 3 dibawah ini.

Langkah 3 :

M ₀	M ₁	M ₂	M ₃	M ₄	M ₅	M ₆	M ₇	M ₈	M ₉	M ₁₀
99	106	96	91	102	94	92	104	96	93	103
M ₁₁	M ₁₂	M ₁₃	M ₁₄	M ₁₅	M ₁₆	M ₁₇	M ₁₈	M ₁₉	M ₂₀	
11	12	13	14	15	L	L	L	L	L	
M ₂₁	M ₂₂	M ₂₃	M ₂₄	M ₂₅	M ₂₆	M ₂₇	M ₂₈	M ₂₉	M ₃₀	M ₃₁
L	L	L	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

Langkah 4 :

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 99

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 99000000 00000000 00000000 00000000

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
99	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

Langkah 4 dapat dilakukan sampai 16 kali perulangan, setelah melakukan perulangan sampai 16 maka akan dilakukan langkah 5 dibawah ini.

Langkah 5 :

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

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

Langkah 5 dapat dilakukan sampai 47 kali perulangan, setelah melakukan perulangan sampai 47 maka akan didapat bilangan desimal menjadi biner sesuai dengan nilai X yang terdapat pada tabel 2, seperti dibawah ini.

Tabel 3. 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
1100010	10100111	101	11110011	11000000	11000111	1110011	10001100
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


Berdasarkan pengujian yang dilakukan metode MD2 maka pada tabel 2 menghasilkan nilai desimal dari keseluruhan perhitungan, dan pada tabel 3 nilai yang tadinya berbentuk desimal diubah menjadi nilai biner yang terdapat pada tabel 3. Nilai biner tersebut dikonversi ke hexa dan hasil perubahannya menjadi message digest MD2 dibawah ini : 292E43C9A2D87C13D3654A1ECF061362A75F3C0C7738C98932BD9BC4C82CA1E9B573CFDD4E01667426F188A17E512. Sehingga hasil dari Autentikasi dengan metode MD2 pada citra rontgen yaitu : 24 Byte 12 Karakter, Seperti dibawah ini :

292E43C9 A2D87C13 D3654A1E CF061362 A75F3C0C 7738C989 32BD9BC4 C82CA1E9 B573CFDD 4E016674 26F188A1 7E512000.

3.3 Pengujian Sistem

Aplikasi Hasher untuk melakukan pengujian menggunakan metode MD2 untuk proses pengujian autentikasi hasil citra rontgen. Dengan tujuan untuk meningkatkan keamanan hasil dari rontgen tersebut. Berikut ini implementasi dari aplikasi yang digunakan.

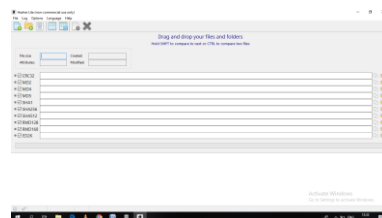
Tabel 4. Hasil Nilai Hash

Citra hasil Rontgen	Nilai Hash
	8db4147d50e bccedd03fe230324aaa4f

Adapun parameter yang digunakan sebagai perbandingan terhadap nilai hash citra hasil rontgen yang asli dengan yang editan yaitu sebagai berikut :

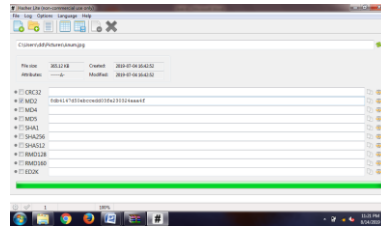
1. Aplikasi Hasher

Menjelaskan beberapa langkah yang dapat dilakukan oleh *user* untuk menampilkan menu lembar kerja pada pengujian autentikasi hasil citra rontgen. Gambar dibawah ini tampilan menu lembar kerja yang dapat dilihat pada gambar dibawah ini :



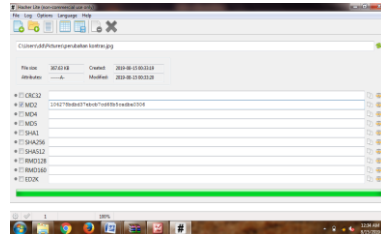
Gambar 3. Tampilan Kerja Hasher

2. Proses Aplikasi Hasher



Gambar 4. Tampilan Pembuktian Hasil Rontgen Yang Asli

3. Tampilan Rontgen yang Editan



Gambar 5. Tampilan Pembuktian Hasil Rontgen Yang Editan

Perbandingan nilai hash antara citra asli dengan citra editan dapat dilihat pada tabel berikut :

Tabel 5. Perubahan Nilai Hash

Parameter	Citra Awal	Citra Editan	Nilai Hash Citra Awal	Nilai hash Citra Editan
Perbedaan antara Rontgen yang asli dengan editan			8db4147d50e bccedd03fe230324aaa4f	104278bdbc37ebcb7 cd68b5cadba0306

Dari hasil penerapan yang dilakukan citra hasil Rontgen yang asli dengan editan dapat dilihat dari hasil nilai hash yang berbeda menggunakan aplikasi hasher tersebut. Berdasarkan data hasil pengujian pada tabel 5 diatas maka dapat diperoleh hasil dari autentikasi citra Rontgen menggunakan aplikasi hasher bahwa sekecil apapun perubahan pada citra rontgen tersebut sangat mempengaruhi keaslian hasil dari Rontgen tersebut berdasarkan dari nilai hash yang diperoleh.

4. KESIMPULAN

Berdasarkan hasil dari penelitian yang penulis lakukan mengenai autentikasi hasil citra Rontgen dengan menggunakan metode MD2 dapat diuji dengan aplikasi yang sudah ada yaitu Hasher, penulis dapat menarik kesimpulan bahwa cara analisa autentikasi citra Rontgen dilakukan dengan mengetahui citra digital terhadap suatu autentikasi hasil Rontgen yang teridentifikasi pada citra tersebut, hasil citra Rontgen bertujuan untuk mengautentikasi hasil dari kebenaran terhadap suatu hasil citra Rontgen tersebut, dan juga dapat melakukan perubahan atau menganalisa suatu keaslian pada sebuah file citra, sekecil apapun perubahan tersebut dapat mempengaruhi suatu keaslian dari citra tersebut. Penerapan Metode MD2 pada hasil citra Rontgen dilakukan dengan menggunakan aplikasi matlab versi 6.1 untuk mencari nilai pixel yang terdapat pada citra Rontgen itu tersendiri, sehingga mendapatkan nilai pixel yang berukuran 3x4 pixel, dan mencari nilai hash menggunakan metode MD2 sehingga autentikasi dari rontgen tersebut menghasilkan 24 byte 12 karakter. Proses Autentikasi menggunakan aplikasi hasher versi 3.4, Selain dengan aplikasi hasher aplikasi yang lain juga diharapkan mampu dapat mengautentikasi citra dari hasil tersebut.

REFERENSI

[1] P. A. Md and D. A. N. Md, "Perbandingan algoritma md2, md4, dan md5," *perbandingan algoritma MD2, MD4, dan MD5*, pp. 1–15.

[2] F. Muller, "The MD2 Hash Function Is Not One-Way," *The MD2 Hash function is Not One-Way*, pp. 214–229, 2010.

[3] B. A. B. Ii, A. K. Implementasi, and P. Implementasi, "No Title," pp. 12–75, 1990.

[4] R. Sadikin, "kriptografi untuk keamanan jaringan," in *kriptografi untuk keamanan jaringan*, T. A. Prabawati, Ed. Yogyakarta: C.V ANDI OFFSET, 2012.

[5] M. K. Emy Setyaningsih,S.Si., "Kriptografi dan implementasi menggunakan matlab," in *Kriptografi dan implementasi menggunakan matlab*, Nikodemus WK, Ed. Yogyakarta, 2015, p. 3.

- [6] M. ir.yusuf kurniawan, *Kriptografi keamanan internet dan jaringan telekomunikasi*. bandung: informatika bandung, 2004.
- [7] M. K. T.Sutoyo, S.Si., "Teori pengolahan citra digital," in *Teori pengolahan citra digital*, Benedicta Rini W, Ed. Yogyakarta: Andi Offset, 2009, p. 9.
- [8] Darma Putra, *Pengolahan Citra Digital*. Yogyakarta, 2010.
- [9] F. Sidik and H. Sunandar, "Perancangan Aplikasi Pengolahan Citra Meningkatkan Kualitas Foto Rontgen Menggunakan Metode Median Filtering," *JURIKOM (Jurnal Riset Komputer)*, vol. 3, no. 6, pp. 38–41, 2016.
- [10] Yusufzal, "Kode Autentikasi Hash pada Pesan Teks Berbasis Android," *Kode Autentikasi Hash pada Pesan Teks Berbasis Android*, pp. 1–9, 2018.