KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 2, No 1, Agustus 2021
Hal 28-34
https://djournals.com/klik

Analisa Metode SHA224 Untuk Mendeteksi Orisinalitas Citra Digital

Rusman Halawa

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: rusmanhal14@gmail.com

Abstrak− Dalam sebuah citra digital sangatlah penting yang namanya keaslian sebuah data, mengingat data yang terkandung di dalamnya sangatlah penting dan sangat dirahasikan dari pihak-pihak yang tidak berkewajiban yang ingin merusak dan mengubah informasi yang terkandung didalamanya sehingga tidak sesuai dengan yang diharapakan. Maka, perlu diterapkan yang namanya keamanan data yang dapat menjaga data tersebut agar tidak dapat di manipulasi ataupun merusak segala informasi yang ada didalam data tersebut. Kriptografi Beberapa permasalahan diatas yang perlu diperhatikan dan dipahami agar sistem yang di terapkan sesuai dengan apa yang diingikan oleh semua pihak. Pada citra digital hal utama yang harus diamati untuk menjaga keaslian citra digital dan memperbaiki permasalahan kualitas citra digital yang ingin dimanipulasi. Dengan adanya penelitian ini dapat mengatasi segalah masalah yang terjadi tentang memanipulasi data dari piha-pihak yang tak berkewajiban terhadap data tersebut Dari penelitian diatas tujuan dari SHA224 adalah mengamankan bentuk citra digital yang masih asli yang ingin di manipulasi oleh pihak-pihak lain. Citra dapat dilihat ataupun di manipulasi suapapun baik yang memiliki hak atau kawajiban didalam data maupun yang tidak memiliki kewajiban sama sekali, namun ketika dilakukan pengamanan data dengan mengunakan metode SHA224 maka data-data yang hasil dari manipulasi maupun data asli akan terdeteksi dan akan terlihat hasil yang sebenarnya. Dengan adanya metode SHA224 dapat menjaga keamanan maupun keaslian citra digital. Pada mengujian ini dapat dilakukan dengan metode SHA224 yang mengunakan aplikasi MATLAB.

Kata Kunci: Kriptografi, Fungsi Hash, SHA-224, Citra Digital.

Abstract− In a digital image it is very important that the name of the authenticity of the data, given the data contained in it is very important and very confidential from parties who are not obliged to want to damage and change the information contained therein so it does not match what is expected. So, it is necessary to apply data security that can protect the data so that it cannot be manipulated or damaged any information contained in the data. Cryptography is the study of mathematical techniques related to aspects of information security such as data confidentiality, data integrity of data integrity, and data authentication. But not all aspects of information security can be solved by cryptography. Cryptography can also be interpreted as a science or an art to maintain message security. Some of the problems above that need to be considered and understood so that the system applied in accordance with what is desired by all parties. In digital images, the main thing that must be observed is to maintain the authenticity of digital images and improve the quality problems of digital images that you want to manipulate. With this research can overcome all the problems that occur about manipulating data from parties who are not obliged to the data From the above research the purpose of SHA224 is to secure a form of digital images that are still original that want to be manipulated by other parties. The image can be seen or manipulated anyone who has rights or obligations in the data or has no obligation at all, but when securing data using the SHA224 method, the data resulting from manipulation and original data will be detected and the results will be seen in fact. With the SHA224 method it can maintain the security and authenticity of digital images. In testing this can be done with the SHA224 method using the MATLAB application.

Keywords: Cryptography, Hash Function, SHA-224, Digital Image.

1. PENDAHULUAN

Citra adalah suatu gambar atau kemiripan dari suatu objek. Citra analog tidak dapat dipresentasikan kedalam komputer, sehingga tidak bisa diproses oleh komputer secara lagsung. Tentu agar bisa diproses di komputer, cintra analog harus di konversi menjadi citra digital. Citra digital adalah citra yang dapat diolah oleh komputer dan dihasilkan dari peralatan digital (citra digital) kemudian diolah oleh komputer[1].

Dalam sebuah citra digital sangatlah penting yang namanya keaslian sebuah data, mengingat data yang terkandung di dalamnya sangatlah penting dan sangat dirahasiakan dari pihak-pihak yang tidak berkewajiban yang ingin merusak dan mengubah informasi yang terkandung didalamanya sehingga tidak sesuai dengan yang diharapakan. Maka, perlu diterapkan yang namanya keamanan data yang dapat menjaga data tersebut agar tidak dapat di manipulasi ataupun merusak segala informasi yang ada didalam data tersebut. Teknik keamanan data agar terjaga keaslianya dengan mengunakan teknik kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan[2]. Dengan mengamankan data dapat menghidari kejadian-kejadian yang tidak diharapkan seperti, pambajakan, dan pemalsuan data. Kemudahan dalam merubah citra digital dapat merusak hasil dari keaslian citra digital dalam berbagai bentuk. Sehingga jarang digunakan dalam tindakan kejahatan, dengan kriptografi dengan melakukan keamanan jarang ditemukan pemalsuan sebab informasi yang dikirim atau disampaikan menjadi beda dengan yang sebelumnya.

Beberapa permasalahan diatas yang perlu diperhatikan dan dipahami agar sistem yang di terapkan sesuai dengan apa yang diingikan oleh semua pihak. Pada citra digital hal utama yang harus diamati untuk menjaga keaslian citra digital dan memperbaiki permasalahan kualitas citra digital yang ingin dimanipulasi. Dengan adanya penelitian ini dapat mengatasi segalah masalah yang terjadi tentang memanipulasi data dari piha-pihak yang tak berkewajiban terhadap data tersebut.

SHA224 merupakan singkatan dari *Secure Hash Algaritma* 224, diumumkan oleh NIST pada tahun 2004. SHA224 juga memiliki data input maksimum panjangnya 64-bit. Nilai hash tetap atau intisari 224 bit adalah dikeluarkan dari

algoritma. SHA224 juga diproses input dalam blok 512-bit yang selanjutnya di bagi menjadi sub-blok divisi masing-masing dengan panjang 32 bit. SHA224 melakukan 64 langkah-langkah dalam perhitungan nilai hash akhir[3].

Dalam penelitian sebelumnya SHA224 diterapakan oleh Jinita Jose, Nandakumar R, Nisha J.S kriptografi dapat diringkas secara sederhana sebagai ilmu menulis dalam kode rahasia ini tentang komunikasi di hadapan musuh. Ini tentang komunikasi dihadapan dari musuh, hari ini orang-orang terutama bergantung pada Email, Perbankan Internet, Belanja Online, dan Dgital sensitif lainya komunikasi. Fungsi hash adalah fungsi satu arah dan memberikan integtritas, sebuah keluaran algoritma dirancang oleh Institut NasionalStandar dan Teknologi (NIST) dan diterbitkan sebagai Federal Information of Processing Standars (FIPS)[4].

Dalam penelitian sebelumnya metode SHA224 diterapkan oleh Hendry Nunoo-Mensah keamanan dalam jaringan sensor nirkabel (WSN) telah menjadi meningkatnya kebutuhan karena area aplikasi yang beragam diimplementasikan. Ontentikasi simpul adalah teknik yang cocok terhadap gangguan simpul dan pengenalan node palsu, cara ontentikasi node adalah dengan mengunakan *Masssage Authenyication Code* (MAC), merupakan implementasi mengunakan fungsi Hash. Dalam makala ini, analisis komperatif dari fungsi Hash (MD-5, SHA-1, SHA-224, SHA-256, SHA-384 dan SHA-512). Namun, dari beberepa fungsi hash hasil analisi menunjukan SHA224 sebagai fungsi hash terbaik untuk digunakan saat mendesain WSN yang aman dan sadar energi, jaringan sensor nirkabel, keamanan dan fungsi hash[3].

Dari penelitian diatas tujuan dari SHA224 adalah mengamankan bentuk citra digital yang masih asli yang ingin di manipulasi oleh pihak-pihak lain. Citra dapat dilihat ataupun di manipulasi suapapun baik yang memiliki hak atau kawajiban didalam data maupun yang tidak memiliki kewajiban sama sekali, namun ketika dilakukan pengamanan data dengan mengunakan metode SHA224 maka data-data yang hasil dari manipulasi maupun data asli akan terdeteksi dan akan terlihat hasil yang sebenarnya. Dengan adanya metode SHA224 dapat menjaga keamanan maupun keaslian citra digital. Pada mengujian ini dapat dilakukan dengan metode SHA224 yang mengunakan aplikasi MATLAB.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik metematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan [2] [5].

2.2 Citra Digital

Citra digital adalah repsesentasi numerik dari citra dua dimensi. Nilai numerik yang direpresentasekan umumnya adalah nilai biner 8 bit. Nilai biner ini disimpan pada elemen citra yang sering disebut sebagai pixel. Citra digital berisi piksel yang jumlah baris dan kolomnya tetap. Pixel adalah elemen gambar terkecil dari citra digital [6].

2.3 SHA224 (Secure hash Algoritma 224)

SHA224 merupakan singkatan dari *Secure Hash Algaritma* 224, diumumkan oleh NIST pada tahun 2004. SHA224 juga memiliki data input maksimum panjangnya 64-bit. Nilai hash tetap atau intisari 224 bit adalah dikeluarkan dari algoritma. SHA224 juga diproses input dalam blok 512-bit yang selanjutnya di bagi menjadi sub-blok divisi masing-masing dengan panjang 32 bit. SHA224 melakukan 64 langkah-langkah dalam perhitungan nilai hash akhir. Pada algorima SHA224 terdapat beberapa tahap[1].

Preprocessing terdiri dari tiga langkah yaitu mengisi pesan, parsing pesan kedalam blok pesan dan mengatur inisial nilai hash.

1. *Padding the massage*
   Tujuan dari pudding the masage utnutk memastikan bahwa pesan yang empuk adalah kelipatan 512 bit. Misalkan panjang M adalah 512 bit tambahkan "1" ke akhir pesan yang diikuti oleh "K" nol bit diman K adalah solusi kecil non-negatif persamaan *1*+1+K= 448 mod 512. Kemudian tambahkan blok 64 bit itu sama dengan angka 1 yang mnggunakan representasi biner.
   Keterangan :
   1 = panjang pesan
   K = banyak bit 0 yang ditambahkan sebagai panjang
2. Pebambahan Panjang Append
   Penambahan panajang append dilakukan dengan menambahkan panjang pesan sebanyak 64 bit dengan panjang pesan dari sebuah citra
3. Parsing pesan
   Pesan empuk diuraikan menjadi N blok 512 setiap blok terdiri dari enam belas kata 32 bit
4. Mengatur nilai hash
   Nilai hash awal terdiri dari urutan delapan kata 32 bit yang diperoleh dengan mengambil tiga puluh hingga enam puluh empat bit dari bagian dari pencahan dari akar kuadrat dari kesembilan melalui dari bilangan prima keenam belas tesebut.
5. Koefisien SHA-224

Koefisien ini merupakan hasil nilai yang telah ditetapkan oleh standart SHA sebagai nilai ketetapan

6. Langkah ini diawali dengan mengubah setiap blok pesan menjadi bilangan heksadesimal untuk penjadwalan pesan ke 16 sampai ke 64 kali putaran

Hash Computation yaitu Pesan M memiliki panjang 1 bit diman $0 \leq 1 < 264$ bisa hash menggunakan algoritma SHA224. Algoritma terdiri enam puluh empat kata 32 bit (W0, W1……...W63) delapan variabel yang bekerja (a,b,c,d,e,f,g,h) masing-masing 32 bit dan nilai hash 224 bit dan nilai hash 224 bit. Setiap blok preprocessed sebagai berikut i = 1 ke N, langkah-langkah sebagai berikut[1] :

1. Jadwal pesan mengambil pesan asli 512-bit memblokir dan memperluas enam belas kata 32-bit ini menjadi 64 kata, satu kata untuk setiap putaran fungsi kompresi kata-kata dari jadwal pesan diberi variabel $W_{0,}W_{1,}$……..$W_{63.}$

$$W_t = \begin{cases} M_t^{(t)} & 0 \leq t \leq 15 \\ \{\sum_{O1}^{224}(w_{i-2}) + (w_{i-7}) + w_{i-7} + O_0^{224}(w_{i-15}) + w_{i-16} & 16 \leq t \leq 63 \end{cases}$$

Dimana :

$O_1^{224}(w_{i-2}) = ((w_{i-2})ROTR\ 17) \oplus ((w_{i-2})RORT\ 19) \oplus ((w_{i-2})SHR10)$

$O_0^{224}(w_{i-2}) = ((w_{i-15})ROTR\ 7) \oplus ((w_{i-15})RORT\ 18) \oplus ((w_{i-15})SHR3)$

Keterangan :

$\sum$ = sigma (penjumlahan)
W_t = Blok pesan yang baru
M_t = Blok pesan yang lama
W_{i-2} = Blok pesan dari W ke i-2
W_{i-15} = Blok pesan dari W ke i-15
RORT = *RotateRight*(operasi geser kiri)
SHR = *ShiftRight*
$\oplus$ = Operator *XOR*

2. Delapan variabel kerja a,b,c,d,e,f,g,h dan h , dimuat dengan nilai hash awal untuk setiap iterasi pertama atau sebelumnya nilai hash (i-1).

For T_0 to T63
{
$T_1 = h + \sum_1^{224}(e) + ch(e,f,g) + K_1^{224} + W_t$
$T_2 = \sum_0^{224}(a) + Maj(a,b,c)$
$H = g$
$G = f$
$F = e$
$E = d + T_1$
$D = c$
$C = b$
$A = T_1 + T_2$
}

Dimana :

$ch(e,f,g) = (e \wedge f) \oplus (\sim e \wedge g)$
$Maj(a,b,c) = (a \wedge b) \oplus (a \wedge c) \oplus (c \wedge b)$
A,b,c,d,e,f,g,h = variabel yang berisi pesan heksadesimal
K_1^{224} = konstanta SHA224
ROTR = rotateright
$\oplus$ = operator xor
$\wedge$ = operator and
K_1 = Nilai ketetapan konstanta

Tabel 1. kosntanta

428A2F98	71374491	B5C0FBCF	E9B5DBA5
3956C25B	59F111F1	923F82A4	AB1C5ED5
D807AA98	12836B01	243185BE	550C7DC3
72BE5D74	80DEB1FE	9BDC06A7	C19BF174
E49B69C1	EFBE4786	DFC19DC6	240CA1CC
2DE92C6F	4A7484AA	5CB0A9DC	76F988DA
983E5152	A831C66D	B00327C8	BF597FC7
C6E00BF3	D5A79147	06CA6351	14292967
27B70A85	2E1B2138	4D2C6DFC	53380D13
650A7354	766A0ABB	81C2C92E	92722C85
A2BFE8A1	A81A564B	C24B8B70	C76C51A3
D192E819	D6990624	F40E3585	106AA070
19A4C116	1E376C08	2748774C	34BDBCB5

391C0CB3	4ED8AA4A	5B9CCA4F	682E6FF3
748F82EE	78A5626F	84C87814	8CC70208
90BEFFFA	A4506CEB	BEF9A3F7	C67178F2

3. Tiap kata dari ekspansi(perluasan) pesan kemudian diteruskan ke fungsi kompresi SHA. Ini bermanfaat delapan 32-variabel kerja bit enam puluh empat iterasi komnpresi fungsi kemudian di lakukan. Setelah semua blok pesan di proses final 224 di bentuk dengan nilai
$H0^{(N)}$, $H1^{(N)}$, $H2^{(N)}$, $H3^{(N)}$, $H4^{(N)}$, $H5^{(N)}$, $H6^{(N)}$, $H7^{(N)}$

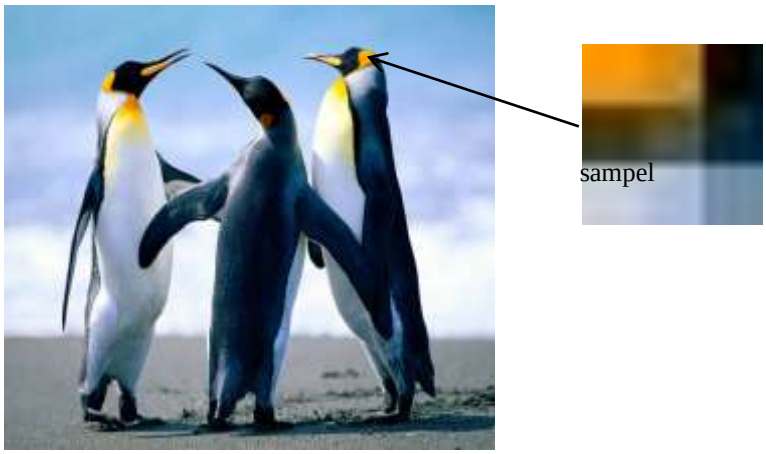
3. HASIL DAN PEMBAHASAN

Permasalahan yang dianalisis pada penelitian ini difokuskan pada poin-poin masalah yang telah dirumuskan pada bagian pendahuluan yaitu masalah pendekteksian citra digital dengan menerapkan teknik kriptografi dengan tujuan agar mencegah atau membatasi sebah pemalsuan data citra digita yang bersifat rahasia.

Masalah keamanan data hingga saat ini memang masih menjadi salah satu hal yang di anggap sangat di utamakan dan diperhatikan dalam penjagaan data-data rahasia terhadap tindakan-tindakan pemalsuan dan memanipulasi data asli dengan data yang tidak asli yang dapat saja dilakukan oleh pihak-pihak yang tak memiliki kewenangan dan hak atas segala data tersebut. Namun tidak diherankan juga bahwa tindakan-tindakan pemalsuan data asli sering terjadi di era saat ini untuk kepentingan pribadi. Sehingga kejadian-kejadian ini sangat merugikan pihak-pihak yang bertanggung jawab atas data tersebut maupun pihak yang akan menerima data dari si pengirim.

Pemanfaatan teknik pengamanan data asli atau data yang masih orisinalitas hasilnya juga masih kurang efesien dalam meyakinkan pihak pengirim dan penerima akan keamanan data milik mereka. Berdasarkan permasalahan tersebut maka pada penelitian ini, mencoba memberikan salah satu solusi dalam menyelesaiakan suatu masalah tersebut dengan menerapkan teknik sebuah pengamanan data yakni teknik kriptografi dalam mendetekni orisinalitas citra digital.
SHA224 merupakan singkatan dari *Secure Hash Algaritma* 224, diumumkan oleh NIST pada tahun 2004. SHA224 juga memiliki data input maksimum panjangnya 63-bit. Nilai hash tetap atau intisari 224 bit adalah dikeluarkan dari algoritma. SHA224 juga diproses input dalam blok 512-bit yang selanjutnya di bagi menjadi sub-blok divisi masing-masing dengan panjang 32 bit. SHA224 melakukan 64 langkah-langkah dalam perhitungan nilai hash akhir.

Yang menjadi objek pada penelitian ini adalah citra digital. Dalam hasil citra digital pemindaian ini berformat jpg gambar 3.1, sehingga untuk mempermudah proses analisa maka diambil sampel dari hasil citra tersebut berukuran 3 x 3 piksel pada kanal merah saja tabel 1. dan nilai piksel tersebut diambil mengunakan aplikasi Matlab 6.1



Gambar 1. Citra Grayscale

Tabel 2. nilai piksel citra sampel

166	166	165
165	166	165
165	166	166

Berikut ini yang merupakan langkah-langkah penerapan algoritma SHA224 untuk mendeteksi orisinalitas citra digital pada hasil pemindaian gambar jpg. Sebelum menerapkan algoritma SHA224 dilakukan terlebih dahulu penyesuaian *input* berupa bilangan biner. Untuk itu nilai piksel dari citra input diubah kedalam biner yaitu sebagai berikut

Tabel 3. Nilai input biner

10100110	10100110	10100101
10100101	10100110	10100101
10100101	10100110	10100110

1. Penambahan padding bit

   Pada penambahan panjang M=72 bit. Proses berikutnya adalah dengan menambahkan padding bit 1 dan sisanya 0 sejumlah k, dengan persamaan sebagai berikut:
   K = L+ 1 = 448 mod 512
   K = 72 + 1 = 448 mod 512
   K = 448 – 73
   K = 375
   Makan banyak padding bit 0 yang ditambahkan tabel 4. dari hasil perhitungan diatas adalah sebagai berikut :

Tabel 4. penambahan padding bit

10100110	10100110	10100101	10100101	10100110	10100101	10100101	10100110
10100110	10000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000

2. Penambahan panjang append

   Penambahan panjang append dilakukan dengan menambahkan panjang pesan sebanyak 64 bit di akhir tabel 5 Panjang pesan adalah 72 bit sehing ditambahkan panjang append sebagai berikut :

Tabel 5. penambahan panjang append

10100110	10100110	10100101	10100101	10100110	10100101	10100101	10100110
10100110	10000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
00000000	**00000000**	**00000000**	**00000000**	**00000000**	**00000000**	**00000000**	**0000000**

3. Parsing pesan

   Pada kasusu ini panjang pesan tidak boleh lebih dari 512 sehingga hanya menghasilkan 1 blok 512 bit yaitu $M^{(0)}$ tabel 6. Tahap selanjutnya adalah melakukan parsing pesan dengan membagi setiap blok 512 bit menjadi 16 blok berukuran 32 bit

Tabel 6. parsing pesan

$M_0^{(0)}$	10100110 10100110 10100101 10100101
$M_1^{(0)}$	10100110 10100101 10100101 10100110
$M_2^{(0)}$	10100110 10000000 00000000 00000000
$M_3^{(0)}$	00000000 00000000 00000000 00000000
$M_4^{(0)}$	00000000 00000000 00000000 00000000
$M_5^{(0)}$	00000000 00000000 00000000 00000000
$M_6^{(0)}$	00000000 00000000 00000000 00000000
$M_7^{(0)}$	00000000 00000000 00000000 00000000
$M_8^{(0)}$	00000000 00000000 00000000 00000000
$M_9^{(0)}$	00000000 00000000 00000000 00000000
$M_{10}^{(0)}$	00000000 00000000 00000000 00000000
$M_{11}^{(0)}$	00000000 00000000 00000000 00000000
$M_{12}^{(0)}$	00000000 00000000 00000000 00000000
$M_{13}^{(0)}$	00000000 00000000 00000000 00000000
$M_{14}^{(0)}$	00000000 00000000 00000000 00000000
$M_{15}^{(0)}$	00000000 00000000 00000000 00000000

4. Ini sialisasi nilai Hash

   Setelah proses pasing pesan maka langkah selanjutnya adalah inisialisasi hash di mana nilai merupakan sebuah ketentuan yaitu:

Tabel 7. InitialHashValue

Variabel	HashValue

$H_0^{(0)}$	6A09E667
$H_1^{(0)}$	BB67EA85
$H_2^{(0)}$	3C6EF372
$H_3^{(0)}$	A54FF53A
$H_4^{(0)}$	510E527F
$H_5^{(0)}$	9B05688C
$H_6^{(0)}$	1F83D9AB
$H_7^{(0)}$	5BE0CD19

5. Koesfisien SHA-224
Kemudian dilakukan peng-koefisien, yang sudah ditetapkan pada standar SHA-2 yakni adalah sebagai berikut:

Tabel 8. koefisien SHA

428A2F98	71374491	B5C0FBCF	E9B5DBA5
3956C25B	59F111F1	923F82A4	AB1C5ED5
D807AA98	12836B01	243185BE	550C7DC3
72BE5D74	80DEB1FE	9BDC06A7	C19BF174
E49B69C1	EFBE4786	DFC19DC6	240CA1CC
2DE92C6F	4A7484AA	5CB0A9DC	76F988DA
983E5152	A831C66D	B00327C8	BF597FC7
C6E00BF3	D5A79147	06CA6351	14292967
27B70A85	2E1B2138	4D2C6DFC	53380D13
650A7354	766A0ABB	81C2C92E	92722C85
A2BFE8A1	A81A564B	C24B8B70	C76C51A3
D192E819	D6990624	F40E3585	106AA070
19A4C116	1E376C08	2748774C	34BDBCB5
391C0CB3	4ED8AA4A	5B9CCA4F	682E6FF3
748F82EE	78A5626F	84C87814	8CC70208
90BEFFFA	A4506CEB	BEF9A3F7	C67178F2

Pada penelitian ini dilakukan beberapa pengujian pada objek penelitian yaitu citra. Pengujian ini dilakukan beberapa manipulasi pada pemindaian citra dan melihat apakah perubahan yang dilakukan pada citra tersebut juga mengubah nilai *hash* yang dihasilkan. Apa bila nilai *hash* yang dihasilkan berubah berarti manipulasi yang dilakukan pada citra adalah sebagai berikut :

Tabel 8. hasil pengujian

Parameter	Citra Awal	Citra Manipulasi	Nilai *hash* citra awal	Nilai *hash* citra manipulasi	hasil
Merubah nilai satu *pixel*			CE50B9B7110CEA1055176F547A45BC456B1F87FE8AF39448688D57068B0334D5	791A52C7F74DBFB7119E56f803206ACAD47C911AD8009DB1A6EC5A5D	Terdeteksi
Melakukan *rotasi* citra			CE50B9B7110CEA1055176F547A45BC456B1F87FE8AF39448688D57068B0334D5	69438F6A51E28B798627A7F8CAFF8E34CD084A773BEFE6585776473C	Terdeteksi
Melakukan *crop* pada citra			CE50B9B7110CEA1055176F547A45BC456B1F87FE8AF39448688D57068B0334D5	2D79022C5DF708726F0E8570449C90764BBF3F753E85393318C03B6D	Terdeteksi

Melakukan *filter* pada citra			CE50B9B711 0CEA1055176 F547A45BC4 56B1F87FE8 AF39448688D 5706 8B0334D5	8F73639C06 417709E43C D559140133 8350231C4 AEFEA11C 391EED62	Terdeteksi

Berdasarkan hasil pengujian yang dilakukan pada tabel 4.2 diatas membuktikan bahwa algoritma SHA-224 berhasil mendeteksi perubahan yang terjadi pada pemindaian citra dengan presentase hingga 100%, semua perubahan dapat dideteksi oleh algoritma SHA-224 bahkan perubahan pada satu nilai piksel memberikan perubahan pada nilai *hash*nya.

4. KESIMPULAN

Dari hasil penelitian yang telah dilakukan oleh penulis dapat mengambil sebuah kesimpulan dari hasil proses penelitian atau dengan isi penelitian itu sendiri. Citra dapat terdeteksi dengan perbandingan hasil dari citra asli dan hasil citra manipulasi yang telah terdeteksi. Metode SHA-224 dapat mendeteksi perubahan yang terjadi pada citra digital walaupun hanya satu piksel saja dan penerapan metode SHA-224 dapat di uji dengan mengunakan aplikasi matlab R2013a untuk mendeteksi orisinalitas citra digital.

REFERENCES

[1] Pulung Nurtatian Andono, pengolahan citra digital. Yogyakarta, 2017.
[2] renaldi, "pengertian dan contoh kriptografi dengan proses enkripsi dan deskripsi," ondigiitalforensics.weebly.com, 2016. [Online]. Available: http://ondigitalforensics.weebly.com/cryptography/pengertian-dan-contoh-kriptografi-dengan-proses-enkripsi-dan-dekripsi#.XRTEI45R3Dc. [Accessed: 27-Jun-2019].
[3] K.-G. K. O. Henry NuNoo-Mansah, "Analisis Komparatif Penggunaan Energi Hash Fungsi dalam Jaringan Sensor Nirkabel Aman," J. Int. Apl. Komput. (0975 - 8887), vol. 109, p. 1, 2015.
[4] N. J. S. Jinita jose, nanda kumar, "Desain & Validasi SHA 224 IP Core," IJCST, vol. vol.5, no. 0976–8491, p. 2, 2014.
[5] S. Aripin dan M. Syahrizal, "Pengaman File Video Menggunakan Algoritma Merkle Hellman Knapsack," J. MEDIA Inform. BUDIDARMA, vol. 4, no. April, hal. 461–465, 2020, doi: 10.30865/mib.v4i2.2039.

.