Bulletin of Artificial Intelligence
Volume 1, No 1, April 2022 Page: 8−12
ISSN 2962-3944 (media online)
https://journal.grahamitra.id/index.php/buai

Analisa Dan Perbandingan Algoritma Whirpool dan Sha-512 Dalam Penyandian Data Gambar

Darwis Pardamean Purba

Fakultas, Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: darwis.p.purba@gmail.com

Abstrak−File gambar merupakan sebuah bentuk dari kolaborasi yang dimana berada diantara dari titik, garis, bidang dan juga warna yang merupakan akan sangat berguna untuk melakukan pencitraan terhadap sebuah hal, citra digital merupakan representasi dari fungsi intesitas cahaya dalam bentuk diskrit pada bidang dua dimensi. Sebuah file gambar dapat dikatakan asli atau orisinal apabila gambar tersebut tidak mengalami perubahan sedikitpun pada setiab struktur sebuah gambar. Manipulasi sebuah file sering terjadi dan dilakukan oleh orang yang tidak bertanggungjawab untuk memberikan keuntungan bagi orang tersebut maka perlu adanya sebuah teknik yang digunakan untuk menjaga orisinalitas sebuah file atau pun mendeteksi keaslian file gambar tersebut, dapat digunakan sebuah teknik yaitu teknik Kriptografi. Kriptografi merupakan suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetaplah aman saat dikirim, dari pengirim ke penerima tanpa mengalami gangguan apapun dari pihak-pihak yang tidak bertanggungjawab. Fungsi hash merupakan fungsi satu arah yang mengubah sekumpulan string menjadi sekumpulan string yang ukurannya lebih kecil daripada ukuran semula. Fungsi hash memiliki banyak kegunaan, seperti untuk menjaga integritas data, efisiensi waktu pengiriman, serta untuk meminimalisir panjang data yang beraneka ragam. Aplikasi pada dunia nyata dari fungsi hash bermacam-macam, seperti digunakan untuk mengecek suatu orisinalitas data, untuk menyimpan kata kunci pada basis data, dan masih banyak lagi. Pada penelitian ini akan dibahas mengenai 2 buah fungsi hash yang ada, yaitu fungsi hash SHA-512, serta fungsi hash whirlpool. SHA-512 merupakan varian dari SHA-2 yang didesain oleh National Security Agency (NSA), sedangkan algoritma hash Whirlpool dikembangkan oleh 2 orang, Vincent Rijmen dan Paulo S.L.M. Barreto. Kedua fungsi hash ini adalah fungsi hash yang dinilai memiliki keamanan yang tinggi. Pada kedua algoritma hash ini, masih belum ditemukannya adanya kolisi pada nilai hash. Penelitian ini akan membahas perbedaan dan persamaan dari kedua algoritma tersebut.

Kata Kunci : Kriptografi; File Gambar; Algoritma Whirlpool; Algoritma SHA-512

Abstract−Image file is a form of collaboration which is located between points, lines, fields and also colors which will be very useful for imaging something, digital images are representations of light intensity functions in discrete form on a two-dimensional plane. An image file can be said to be original or original if the image does not experience the slightest change in any structure of an image. Manipulation of a file often occurs and is carried out by irresponsible people to provide benefits for that person, it is necessary to have a technique used to maintain the originality of a file or detect the authenticity of the image file, a technique can be used, namely Cryptography techniques. Cryptography is a science that studies how to keep data or messages safe when sent, from sender to recipient without experiencing any interference from irresponsible parties. A hash function is a one-way function that converts a set of strings into a set of strings whose size is smaller than the original size. The hash function has many uses, such as to maintain data integrity, delivery time efficiency, and to minimize the length of diverse data. The real-world applications of hash functions vary, such as being used to check the originality of data, to store keywords in databases, and much more. In this study, 2 existing hash functions will be discussed, namely the SHA-512 hash function, and the whirlpool hash function. SHA-512 is a variant of SHA-2 designed by the National Security Agency (NSA), while the Whirlpool hash algorithm was developed by 2 people, Vincent Rijmen and Paulo S.L.M. Barreto. These two hash functions are hash functions that are considered to have high security. In these two hash algorithms, there is still no collision in the hash value. This study will discuss the differences and similarities of the two algorithms.

Keywords: Cryptography; Image Files; Whirlpool Algorithm; SHA-512 Algorithm

1. PENDAHULUAN

Salah satu teknik yang dapat dilakukan untuk mendeteksi keaslian orisinalitas data adalah dengan teknik kriptografi. Suatu data dapat dikatakan sebagai data asli bila tidak terjadi perubahan sedikitpun terhadap struktur pada data. Fungsi hash adalah fungsi yang menerima input berupa string sepanjang apapun lalu mengubahnya menjadi string dengan panjang output tetap. Fungsi hash sangat bermanfaat dalam mendukung mendeteksi orisinalitas data [1]. Dalam proses pendeteksian orisinalitas data ada beberapa algoritma yang dapat digunakan diantaranya Whirlpool dan SHA-512.

Algoritma Whirlpool memiliki kelebihan yaitu hasil hash yang di berikan lebih stabil namun juga memiliki kekurang yaitu membutuhkan ruang penyimpanan yang cukup banyak dan juga membutuhkan proses yang lebih rumit [2]. Sedangkan SHA-512 yang memiliki algoritma sederhana memiliki kelebihan yaitu memakai ruang penyimpanan yang lebih sedikit dan juga memiliki hasil nilai hash yang kuat tetapi terkadang nilai kata kunci yang diberikan sangat lemah walapun jumlah putaran yang dilakukan SHA-512 jauh lebih banyak dibandingkan dengan algoritma Whirlpool [3].

Algoritma Whirlpool merupakan salah satu fungsi hash yang bisa dijadikan sebuah aplikasi yang mampu mendeteksi orisinalitas sebuah file namun ditemukannya kelemahan pada diffusion matrix-nya juga dianggap membutuhkan ruang penyimpanan yang banyak, algoritma SHA-512 yang juga merupakan fungsi hash yang dapat dijadikan sebuah aplikasi untuk mendeteksi orisinalitas sebuah file namun nilai hash yang dihasilkan memiliki kemampuan sebagai kata kunci yang tidak stabil sehingga perlu di analisa dan dibandikan agar menjadi referensi dalam pembuatan sebuah aplikasi.

Bulletin of Artificial Intelligence
Volume 1, No 1, April 2022 Page: 8−12
ISSN 2962-3944 (media online)
https://journal.grahamitra.id/index.php/buai

2. METODOLOGI PENELITIAN

2.1 Algoritma Whirlpool

Algoritma Whirlpool adalah fungsi hash yang ditemukan oleh Vincent Rijmen dan Paulo S. L. M. Barreto yang beroperasi pada pesan yang memiliki ukuran tidak lebih dari 2 256 bit, dan menghasilkan message digest berukuran 512 bit. Whirlpool mempunyai 3 buah versi. Versi yang pertama, Whirlpool-0 diajukan ke proyek NESSIE. Versi kedua, yaitu Whirlpool-T, yang merupakan perbaikan dari versi pertama, dipilih sebagai portfolio NESSIE untuk primitive kriptografik. Kesalahan pada diffusion layer dikemukakan oleh Shirai dan Shibutani dan kemudian diperbaiki lagi, dan versi ketiga atau yang menjadi versi terakhirnya (yang disebut juga sebagai Whirlpool) diadopsi oleh International Organization for Standardization (ISO) pada standard ISO/IEC 10118-3:2004. Whirlpool memakai penguatan Merkle-Damgård dan skema hash Miyaguchi- Preenel dengan blok berukuran 512 bit yang disebut W.

2.2 Struktur Whirlpool

Whirlpool mempunayi 4 fungsi utama yang dapat digunakan untuk perhitungan nilai hash. Fungsi-fungsi tersebut terdiri dari SubByte, ShiftColumbus, MixRows, dan AddRoundkey. Fungsi Substitusi Byte (SubByte) Pada proses ini, algoritma akan memetakan setiap entri pada matrik CState ke sebuah table berukuran 16x16 yang disebut dengan S-Box. Proses ini merupakan pemetaan non-linier, yang nantinya akan mengubah Byte pada setiap entri matrik CState menjadi Byte-Byte baru. Setiap entri pada matrik input memiliki ukuran 8-bits (1-Byte). 4-bits yang berada di sebelah kiri akan dipandang sebagai baris pada kotak S-Box, sedangkan 4 bits yang berada di sebelah kanan akan dipandang sebagai kolom pada kotak S-box. Fungsi SubByte dapat ditulis sebagai suatu korespondensi antara Matrik input A dan Matrik Output B, yaitu :
$B = \text{SubByte}(A) \Leftrightarrow b_{i,j} = S[a_{i,j}], \ 0 \leq i, j \leq 7$

2.3 Algoritma SHA-512

Algoritma SHA-512 adalah algoritma yang menggunakan fungsi hash satu arah yang diciptakan oleh Ron Rivest. Algoritma SHA-512 merupakan pengembangan dari algoritma-algoritma sebelumnya yaitu algoritma SHA-0, SHA-1, SHA- 256 dan algoritma SHA-384[3]. Beberapa cara kerja kriptografi algoritma SHA-512 adalah menerima input berupa message dengan ukuran sembarang dan menghasilkan message diggest yang memiliki panjang 512 bit.

3. HASIL DAN PEMBAHASAN

3.1 Whirlpool

Analisa yang dilakukan dalam penelitian ini adalah untuk proses pengujian keaslian file gambar dengan software Matlab yang akan mengidentifikasikan dan mengevaluasi permasalahan hashing pada file gambar yang berekstensi jpg menggunakan algoritma whirlpool. Nilai pixel dari citra yang dirubah ke grayscale akan diambil sebanyak 5x5 dengan total 25 Pixel. File gambar yang akan diproses dapat dilihat pada gambar 1:

Gambar 1. Citra yang akan diproses

Pengerjaan contoh kasus berikut yang pertama kali dilakukan adalah mengubah nilai RGB citra digital menjadi grayscale dan mendapatkan nilai pixel- nya. Berikut ini adalah nilai RGB dari gambar 1 di atas yang mana diambil dari nilai 5x5 pixel diubah ke dalam bentuk nilai desimal untuk menentukan nilai dari RGB. Nilai pixel 5x5 yang akan diproses adalah pixel (x, y) berikut:
(350, 785), (350, 786),(350, 787),(350, 788),(350, 789),
(351, 785),(351, 786),(351, 787),(351, 788),(351, 789),
(352, 785), (352, 786), (352, 787), (352, 788), (352, 789),
(353, 785), (353, 786), (353, 787), (353, 788), (353, 789),
(354, 785), (354, 786), (354, 787), (354, 788), (354, 789),

Bulletin of Artificial Intelligence
Volume 1, No 1, April 2022 Page: 8−12
ISSN 2962-3944 (media online)
https://journal.grahamitra.id/index.php/buai

Adapun hasil dari pengujian menggunakan matlab, sebagai berikut:

Tabel 1. Tabel nilai RED

Pixel Y Pixel X	785	786	787	788	789
350	227	221	207	184	151
351	206	179	138	96	67
352	124	98	64	44	43
353	54	54	54	54	54
354	54	54	54	54	54

Tabel Nilai GREEN

Tabel 2. Tabel nilai Green

Pixel Y Pixel X	785	786	787	788	789
350	230	224	210	187	154
351	209	182	141	99	69
352	127	101	67	46	45
353	55	54	54	54	54
354	54	54	54	54	54

Tabel Nilai BLUE

Tabel 3. Tabel nilai Blue

Pixel Y Pixel X	785	786	787	788	789
350	221	215	203	180	147
351	202	175	134	92	64
352	120	94	60	41	40
353	50	52	52	52	52
354	52	52	52	52	52

Langkah pertama dalam Pengerjaan contoh kasus adalah mengubah nilai RGB citra digital menjadi grayscale dan mendapatkan nilai pixelnya. Perintah matlab untuk mengubah nilai RGB menjadi grayscale.

image1 = handles.data1; gray = rgb2gray(image1); axes(handles.axes2); imshow(gray); impixelregion

Tabel 4. Nilai Grayscale Citra Sampel 5 x 5

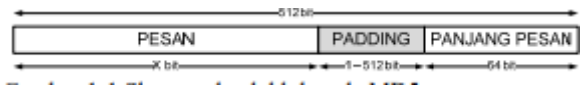
Pixel Y Pixel X	785	786	787	788	789
350	228	222	208	185	152
351	207	180	139	97	68
352	125	99	65	45	44
353	54	54	54	54	54
354	54	54	54	54	54

Setelah nilai desimal didapatkan maka nilai tersebut akan diubah ke dalam biner agar penambahan padding dapat dilakukan dengan menggunakan metode whirlpool. Nilai biner untuk pixel dapat dilihat pada tabel dibawah ini

Tabel 5. Nilai biner untuk pixel citra 5 x 5

1110 0100	1101 1110	1101 0000	1011 1001	1001 1000
1100 1111	1011 0100	1000 1011	0110 0001	0100 0100
0111 1101	0110 0011	0100 0001	0010 1101	0010 1100
0011 0110	0011 0110	0011 0110	0011 0110	0011 0110
0011 0110	0011 0110	0011 0110	0011 0110	0011 0110

Jumlah bit dalam citra sampel ini adalah sebanyak 200 bit dimana diperlukan 312 bit lagi agar genap menjadi kelipatan 512.



Gambar 2. Proses padding

Gambar sebuah blok pada Pengganjal yang diberikan pada pesan tersebut berupa kumpulan bit 1 dan bit 0 dengan urutan bit 1 diletakkan di awal dan bit 0 diletakkan di akhir hingga pesan mencapai panjang dengan kelipatan 512 bit kurang 64 bit.

4. KESIMPULAN

Berdasarkan analisa terhadap Algoritma Whirlpool dan Algoritma SHA- 512, maka didapatkan kesimpulan algoritma whirlpool dan SHA -512 menghasilkan perbedaan yang signifikan pada nilai hash nya walaupun perubahan yang terjadi pada pemindaian citra hanya perubahan arah. Algoritma whirlpool dan SHA-512 dapat mendeteksi perubahan yang terjadi pada pemindaian citra walaupun perubahan yang terjadi hanya perubahan arah. Perbedaan kecepatan antara algoritma Whirlpool dan SHA-512 dipengaruhi oleh jumlah putaran pada kedua algoritma tersebut dan kapasitas yang dipakai yaitu 700.000 byte untuk Whirlpool dan 601.000 untuk SHA-512.

REFERENCES

[1] Sulianto, “Perancangan Aplikasi Untuk Memeriksa Keaslian Data Yang Telah Didownload Menggunakan Algoritma Message Digest 5 (Md5),” Pelita Inform. Budi Darma, vol. 8, no. 3, pp. 172–177, 2014.
[2] T. S. Denis and S. Johnson, Cryptography for Developers. 2006.
[3] W. Setiawan, “Analisis dan Perbandingan Algoritma Whirlpool dan SHA- 512 sebagai Fungsi Hash,” Makal. IF3058 Kriptografi – Sem. II Tahun 2010/2011, 2011.
[4] Aris Kurniawan, (2020, Juli.24) PENGERTIAN Anal. CONTO, TAHAPAN SERTA TUJUAN MENURUT PARA AHLI https//pendidikan.co.id/pengertian- analisis.
[5] N. MARIANA, DEDE, YUNINGSIH, “Perbandingan Pemerintahan,”
Unversitas Terbuka, pp. 1–40, 2015.
[6] J. Maulana, “Teori perbandingan,” Surabaya, 2016.
[7] “Wikipedia (2020, September. 1) METODE PERBANDINGAN https://id.m.wikipedia.org/wiki/Metode_perbandingan.”
[8] M. Mufadhol, “KERAHASIAAN DAN KEUTUHAN KEAMANAN DATA DALAM MENJAGA INTEGRITAS DAN KEBERADAAN INFORMASI DATA,” J. Transform., vol. 6, no. 2, p. 78, 2009, doi: 10.26623/transformatika.v6i2.36.
[9] R. Munir, “Pengantar Kriptografi Bahan Kuliah IF4020 Kriptografi.”