Proteksi Data *X-Ray* Paru-Paru Pasien *COVID-19* menggunakan Algoritma *Rivest Shamir Adleman* dan Algoritma Enkripsi *Rubic Cube Principle*

Citra Nurina Prabiantissa[1], Gusti Eka Yuliastuti[2], Siti Agustini[3], Danang Haryo Sulaksono[4],

Program Studi Teknik Informatika, Fakultas Teknik Elektro dan Teknik Informasi, ITATS[1234]

e-mail: citranurina@gmail.com

ABSTRACT

The COVID-19 pandemic occurred in all countries of the world where all countries tried to find solutions to this pandemic problem. The number of victims who sick, causing the hospital was also overwhelmed with COVID-19 patients. This also results in an improved patient medical record, in which some patients have patches on the lungs and require Lung X-Ray. Therefore medical record security is needed so that this data can be kept confidential. In this study, the researchers wrote about data protection on X-Ray Lung data using 2 encryption methods, the RSA Algorithm (River Shamir Adleman) and the Rubik Cube Principle Encryption Algorithm. The research process consists of 3 processes, that is Pre-Processing of image data, application of methods, and testing using NPCR and UACI values. The results showed that the average value of UACI using the Rubic Cube algorithm was 29.87 whereas if using the RSA method was 30.99. From the average of the two values it can be concluded that the RSA method is better than the Rubic Cube method because it meets the UACI value provisions, which the number of values is more than 30. These values prove the input image is different from the encryption image so that the data can be protected properly.

Kata kunci: *COVID-19, Histogram Equalization, Encryption, River Shamir Adleman (RSA), Rubic Cube Principle*

ABSTRAK

Pandemi COVID-19 terjadi di seluruh negara di dunia dimana semua negara berusaha untuk mencari solusi dari masalah pandemi ini. Banyaknya korban yang sakit, menyebabkan rumah sakit juga kewalahan dengan pasien COVID-19. Hal tersebut juga berakibat pada hasil rekam medik pasien yang semakin bertambah, dimana beberapa pasien, memiliki flek pada paru – paru dan membutuhkan X-Ray Paru - Paru. Oleh sebab itu dibutuhkan keamanan rekam medik agar data ini dapat terjaga kerahasiaanya. Pada penelitian ini, peneliti menulis mengenai proteksi data pada data X-Ray Paru – Paru menggunakan 2 metode enkripsi yaitu Algoritma RSA (*River Shamir Adleman*) dan Algoritma Enkripsi Rubic Cube Principle. Proses penelitian terdiri dari 3 proses yaitu *Pre-Processing* data citra, penerapan metode, dan pengujian dengan menggunakan nilai NPCR dan UACI. Hasil penelitian menunjukkan bahwa rata – rata nilai UACI menggunakan algoritma Rubic Cube berjumlah 29.87 sedangkan jika menggunakan metode RSA berjumlah 30.99. Dari kedua rata – rata nilai dapat disimpulkan jika metode RSA lebih baik dari metode Rubic Cube karena memenuhi ketentuan nilai UACI yaitu jumlah nilai lebih dari 30. Nilai tersebut membuktikan citra input berbeda dengan citra enkripsi sehingga data dapat diproteksi dengan baik.

Kata kunci: *COVID-19, Histogram Equalization*, Enkripsi, *River Shamir Adleman (RSA), Rubic Cube Principle*

PENDAHULUAN

Pandemi yang terjadi di Indonesia dan negara lain ini menjadi perhatian banyak kalangan. Semua negara melakukan berbagai cara untuk menangani virus COVID-19. Jumlah pasien di rumah sakit meningkat dari waktu ke waktu menurut data pemerintah yang ditulis

melalui *website* resmi di Indonesia *covid19.go.id*. Meningkatnya jumlah pasien di rumah sakit menyebabkan data rekam medik pasien juga semakin bertambah, terutama data hasil rontgen (*X-Ray*) paru – paru karena penyakit ini memiliki dampak yang signifikan di beberapa organ paru – paru [1]. Data rekam medik ini membutuhkan keamanan data karena menurut undang – undang, rekam medik merupakan sebuah data yang wajib dijaga kerahasiaannya oleh dokter maupun tempat penyelenggaraan kesehatan atau rumah sakit [2].

Teknologi yang dapat membantu dalam pengamanan data adalah kriptografi. Kriptografi adalah sebuah teknik pengamanan data dimana isi data disembunyikan sehingga tidak dapat dibaca ataupun di mengerti maknanya oleh orang lain yang tidak berkepentingan. Algoritma chiper merupakan nama lain algoritma kriptografi [3]. Chiper merupakan persamaan matematika yang digunakan untuk enkripsi dan dekripsi, kedua persamaan tersebut memiliki hubungan matematis yang saling berkaitan satu dan yang lainnya [4].

Pada penelitian ini, akan dilakukan *pre-processing* dengan menggunakan histogram equalization yang diterapkan pada semua data citra, dimana histogram equalization digunakan untuk menghasilkan warna *grayscale* yang lebih akurat karena memiliki distribusi nilai yang lebih merata. Kemudian metode yang akan digunakan dalam penelitian adalah metode enkripsi dengan menggunakan metode *Rubic Cube Principle* dan RSA (*River Shamir Adleman)*. Menurut penelitian dari Deswanti et al [5], Algoritma *Rubic Cube* memiliki 100% performa yang baik, jika diterapkan langsung sebagai objek penelitian tanpa tambahan pengujian apapun. Sedangkan metode RSA memiliki kinerja yang baik karena keamanan algoritma ini terletak pada sulitnya memfaktorkan bilangan yang besar [6]. Dari hasil kedua algoritma tersebut, dilakukan analisis diferensial antara 2 buah citra dengan menggunakan NPCR (*Number of Changing Pixel Rate*) dan UACI (*Unified Averaged Changed Intensity*) [7]. Perbandingan ini yang menjadi tolak ukur algoritma manakah yang tepat digunakan untuk mengamankan atau proteksi data citra *X-Ray*.

TINJAUAN PUSTAKA

Algoritma *Rivest-Shamir-Adleman* (RSA)

Algoritma *Rivest-Shamir-Adleman* (RSA) adalah salah satu *public key* yang populer sebagai metode enkripsi [8]. Dalam penelitian tersebut menggambarkan cryptosystem kunci publik, termasuk generasi kunci dan sandi kunci publik, yang keamanannya dilakukan dengan memasukkan bilangan bulat sebagai faktor utama yang kemudian dikenal dengan nama *Cryptosystem* [9]. Berikut ini proses enkripsi dan dekripsi dari algoritma RSA :

1. Dua bilangan prima yang berbeda p dan q dan kemudian membentuk nilai modulus n = pq.
2. Pemilihan eksponen publik untuk menjadi bilangan koprima (p - 1) (q - 1), dengan 1 < e < (p - 1) (q - 1).
3. Pasangan (n, e) merupakan *public key*.
4. *Private Key* berupa integer unik dengan pengubahan nilai 1 <d <(p - 1) (q - 1) sehingga ed = 1 mod (p - 1) (q - 1).

Enkripsi: Pemisahan pesan M menjadi urutan blok M1, M2,. . . , Mt, di mana setiap Mi memenuhi 0 ≤ Mi <n. Kemudian mengenkripsi blok ini sebagai [10] :

$$C \equiv E(M) \equiv M^e \pmod{n}; \quad (1)$$

Dekripsi: Diberikan kunci pribadi d dan cipherteks C, fungsi dekripsi adalah:

$$D(C) \equiv CD \pmod{n}; \quad (2)$$

Algoritma Enkripsi *Rubic Cube Principle*

Penelitian ini menggunakan algoritma enkripsi berdasarkan prinsip kubus Rubik. Langkah pertama, untuk mengacak piksel gambar asli, hanya mengubah posisi piksel. Menggunakan dua kunci rahasia acak, bitwise XOR diterapkan ke baris dan kolom ganjil. Kemudian, bitwise XOR juga diterapkan pada baris dan kolom genap menggunakan kunci

rahasia yang dibalik. Langkah - langkah ini bisa diulang sementara jumlah iterasi tidak tercapai. Numerik simulasi telah dilakukan untuk menguji validitas dan keamanan algoritma enkripsi yang diusulkan [11]. Berikut ini merupakan proses enkripsi menggunakan algoritma rubik cube :

1. Dengan masing - masing panjang nilai M dan N, Dua kunci K_R dan K_C, dihasilkan secara acak. Setiap $K_R(i)$ dan $K_C(j)$ dapat mengambil nilai 0 hingga 255.
2. Operasi baris dari gambar input meliputi :
   a. Untuk setiap baris *i*, dilakukan penjumlahan dari semua elemen yang dilambangkan dengan $S_R(I)$.

$$S_R(i) = \sum_{j=1}^{n} I_0(i,j), \quad i = 1,2,3, \dots \dots, M \tag{3}$$

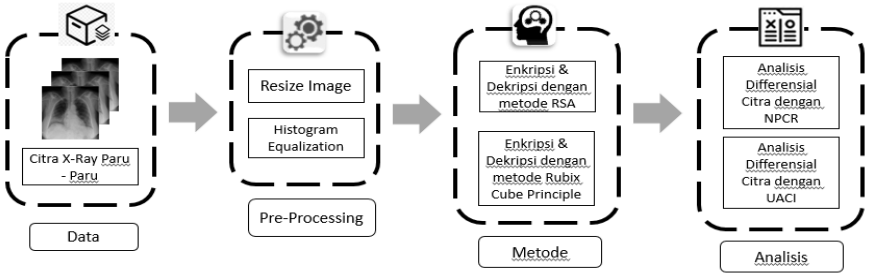
   b. Hitung modulus 2 dari $S_R(i)$, dilambangkan dengan $M_R(i)$.
   Menurut $M_R(i)$, baris *i* adalah kiri atau kanan yang digeser oleh posisi $K_R(i)$ sebagai berikut :
   Jika $M_R(i) = 0$ → right circular shift
   Jika tidak → left circular shift
3. Operasi kolom dari gambar input meliputi:
   Untuk setiap kolom *j* menghitung jumlah semua elemen dan dilambangkan dengan $S_C(j)$.

$$S_C(i) = \sum_{i=1}^{M} S_R(i,j), \quad j = 1,2,3, \dots \dots, N \tag{4}$$

   a. Hitung modulus 2 dari $S_C(j)$, dilambangkan dengan $M_C(j)$.
   b. Menurut $M_C(j)$, baris *i* adalah lingkaran kiri atau kanan digeser oleh posisi $K_C(j)$ sebagai berikut:
      Jika $M_C(j) = 0$ → up circular shift
      Jika tidak → down circular shift
   Setiap baris bitwise XOR untuk diedit dengan kunci K_C.
   $I_{XOR}(2i\text{-}1,j) = I_{SCR}(2i\text{-}1, j)$ XOR $K_C(j)$ & $I_{XOR}(2i, j) = I_{SCR}(2i, j)$ XOR rot180 ($K_C(j)$),
   Dimana rot 180 (K_C) mewakili pembalikan K_C dari kiri ke kanan [12].
4. Kemudian setiap kolom scrambled image I_{XOR} bitwise XOR dengan kunci acak K_R.
   $I_{ENC}(i, 2j - 1) = I_{XOR}(i, 2j\text{-}1)$ XOR $K_R(j)$ & $I_{ENC}(i, 2j) = I_{XOR}(i, 2j)$ XOR rot180($K_R(j)$),
   Dimana rot180(K_R) mewakili membalik K_R dari kiri ke kanan.
5. Lakukan perulangan hingga iterasi selesai.

METODE

Penelitian ini memiliki beberapa proses yaitu *pre-processing*, metode, dan analisis. Berikut ini merupakan gambar dari keseluruhan proses dari penelitian :



Gambar 1. Diagram Sistem Penelitian

Data Citra

Data citra yang digunakan pada penelitian ini adalah dengan menggunakan data citra *x-ray* paru-paru pada pasien covid-19. Ada 10 gambar yang dikumpulkan dengan dengan kondisi pasien yang berbeda. Kemudian di lakukan perubahan ukuran gambar (resize) agar keseluruhan gambar input memiliki ukuran yang sama yaitu 200 x 200 piksel.

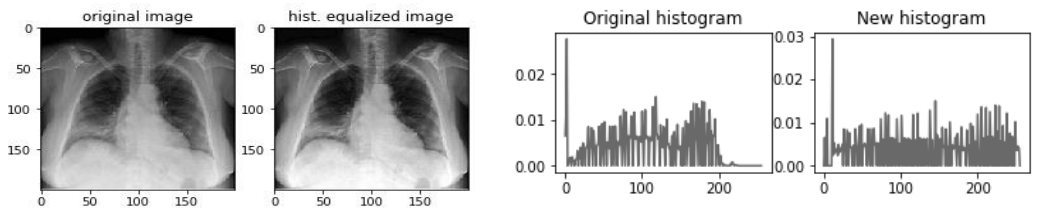
Penggunaan Metode Enkripsi dan Analisis Data

Data yang sudah di proses sebelumnya, kemudian akan melalui proses penerapan metode enkripsi dan dekripsi menggunakan metode enkripsi (RSA dan Rubic Cube). Proses ini mengubah citra menjadi bentuk citra abstrak sehingga informasi pada data rekam medik tidak dapat terbaca. Kemudian gambar tersebut di dekripsi menjadi citra input (citra awal). Penggunaan metode RSA dibandingkan dengan Rubic Cube untuk mengetahui metode mana yang baik untuk proteksi data citra *X-Ray* paru-paru dengan menggunakan NPCR dan UACI.

HASIL DAN PEMBAHASAN

Pre-Processing

Proses *Pre-processing* bertujuan untuk memperbaiki kualitas citra menggunakan sebuah histogram. Salah satu cara yang dapat digunakan untuk memodifikasi histogram citra adalah dengan melakukan *histogram equalization*. *Histogram equalization* (HE) adalah sebuah proses yang mengubah distribusi nilai derajat keabuan pada sebuah citra sehingga menjadi seragam. Tujuan dari HE adalah untuk memperoleh penyebaran histogram yang merata sehingga setiap derajat keabuan memiliki jumlah piksel yang relatif sama [13]. Secara teori HE mengubah distribusi nilai untuk meningkatkan kontras gambar hingga mencapai kinerja yang baik dengan kompleksitas komputasi yang rendah [14]. Hasil dari histogram equalization di visualisasikan pada gambar 2(a) dimana pada gambar tersebut gambar mengalami perubahan yang cukup signifikan. Gambar memiliki tingkat keabuan dari garis gambar yang lebih jelas dibandingkan dengan gambar aslinya. Hal tersebut dibuktikan pula dengan gambar histogram yang memiliki nilai derajat keabuan menjadi lebih rata. Distribusi merata yang terjadi memperbaiki citra input yang sebelumnya dominan pada angka 0-200 menjadi 0-255.

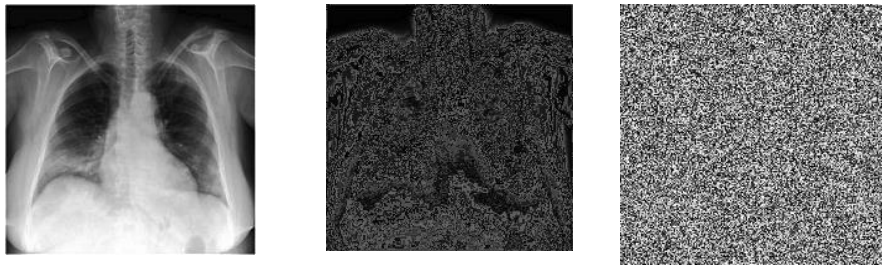


(a) (b)

Gambar 2. a) Data Citra Input, b) *Histogram Equalization*

Analisa dari Penerapan Metode

Penerapan kedua metode yang digunakan pada penelitian ini memiliki hasil yang berbeda. Algoritma Enkripsi dan Dekripsi RSA dan Rubic Cube Principle memiliki kemampuan yang berbeda dalam proteksi data. Hal ini terlihat pada hasil NPCR dan UACI dari kedua metode. Sebelum merujuk pada hasil analisa, pada awalnya dilakukan proses enkripsi menggunakan metode RSA dan dengan metode Rubic Cube Principle. Berikut ini hasil salah satu hasil data yang sudah terenkripsi secara visual setelah penerapan metode :



(a) (b) (c)

Gambar 3. a) Data Citra setelah *Pre-processing*, b) Hasil Enkripsi metode RSA, c) Hasil Enkripsi metode *Rubic Cube Principle*

Gambar 3(b) dan 3(c) menunjukkan data yang sudah terenkripsi menjadi bentuk gambar lain dimana untuk gambar dengan metode RSA masih sedikit terlihat kemiripan dengan data input, sedangkan untuk metode Rubic Cube gambar tampak buram secara keseluruhan. Setelah masing – masing gambar enkripsi sudah terbentuk, kemudian di analisa dengan menggunakan nilai NPCR dan UACI. Nilai NPCR merupakan nilai untuk menguji nilai statistik data citra dan data yang sudah di ekripsi. Suatu nilai NPCR jika mendekati 100% atau NPCR > 90 % dan nilai UACI > 30% dapat dikatakan bahwa keseluruhan piksel pada citra input berbeda dengan citra terenkripsi [15]. Berikut ini diagram hasil analisa :

Tabel 1. Data Analisa NPCR dan UACI

Data ke-	Algoritma Rubic Cube		Algoritma RSA	
	Nilai NPCR	Nilai UACI	Nilai NPCR	Nilai UACI
1	99.56	30.13	99.53	30.13
2	99.57	32.92	99.23	29.67
3	99.54	29.71	99.58	31.32
4	99.58	28.57	99.51	33.35
5	99.59	29.31	99.43	31.24
6	99.59	31.34	99.56	31.45
7	99.67	29.06	99.59	30.22
8	99.58	28.84	99.52	29.82
9	99.59	29.45	99.56	32.12
10	99.56	29.35	99.57	30.60
Rata - Rata	99.58	29.87	99.51	30.99

Data pada tabel 1 menunjukkan penerapan hasil NPCR dan UACI pada kedua metode. Pada metode Rubic Cube dan metode RSA, menurut angka NPCR, menunjukkan bahwa rata-rata nilai NPCR dari kedua metode adalah 99.58 dan 99.51 dimana jika nilai NPCR lebih dari 99 memiliki arti data input berbeda dengan data yang telah di enkripsi. Tetapi untuk data UACI kedua metode memiliki perbedaan hasil, dimana pada metode Rubic Cube, rata – rata nilai berjumlah 29.87 dan 30.99. Algoritma RSA lebih menunjukkan hasil yang baik jika

dibandingkan dengan metode Rubic Cube dimana nilai UACI melebihi angka 30. Jika melebihi dapat dikatakan image input berbeda dari image yang sudah di enkripsi.

KESIMPULAN

Pada penelitian ini telah dilakukan 3 proses dengan menggunakan citra input *X-Ray* dari pasien COVID-19, yaitu Pre-Processing dengan menggunakan histogram equalization, proses enkripsi data citra dengan algoritma RSA dan algoritma Rubic Cube, dan analisa data menggunakan nilai NPCR dan UACI. Salah satu indikator penguji algoritma yaitu nilai NPCR bernilai hampir sama antara kedua metode, maka analisa dapat menggunakan metode UACI yang memiliki hasil yang signifikan berbeda. Hasil analisa menunjukkan bahwa rata – rata nilai UACI menggunakan algoritma Rubic Cube berjumlah 29.87 sedangkan jika menggunakan metode RSA berjumlah 30.99. Dari kedua jumlah nilai dapat disimpulkan jika metode RSA lebih baik dari metode Rubic Cube karena memenuhi ketentuan nilai lebih dari 30. Jumlah nilai tersebut membuktikan citra input berbeda dengan citra enkripsi sehingga data dapat diproteksi dengan baik.

DAFTAR PUSTAKA

[1] C. D. Covid-, F. Pan, T. Ye, P. Sun, S. Gui, B. Liang, and L. Li, "Time Course of Lung Changes at Chest CT during Recovery," vol. 2019, 2020.

[2] A. Ampera, "Tanggung jawab rumah sakit terhadap pasien dalam pelaksanaan pelayanan ke-sehatan," vol. 20, no. 2, pp. 59–74, 2018.

[3] V. B. Liwandouw and A. D. Wowor, "Desain Algoritma Berbasis Kubus Rubik dalam Perancangan Kriptografi Simetris," *Semin. Tek. Inform. dan Sist. Inf.*, vol. 9, no. April 2015, 2015.

[4] A. T. Sholeh, E. Gunadhi, and A. D. Supriatna, "Mengamankan Skrip Pada Bahasa Pemrograman PHP Dengan Menggunakan Kriftografi Base64," *J. Algoritm.*, vol. 10, no. 1, pp. 30–38, 2013.

[5] F. M. Deswanti, H. Bambang, and A. Suci, "Steganografi Citra Digital Menggunakan Enkripsi Berdasarkan Prinsip Kubus Rubik Dan Kode BCH," *Univ. PGRI Yogyakarta*, no. 10, pp. 425–432, 2015.

[6] K. C. Puspita, "Implementasi Kriptografi Dengan Metode RSA Menggunakan Java," no. 1137050124, 2016.

[7] Y. A. Primadhana, R. A. Asmara, and A. R. T. Hayati Ririd, "Enkripsi Citra Menggunakan Algoritma Kubus Rubik Dengan Pembangkit Kunci Md5," *J. Inform. Polinema*, vol. 3, no. 1, p. 40, 2016.

[8] R. . Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[9] R. A. Molin, *Codes: The Guide to Secrecy from Ancient to Modern Times*. 2005.

[10] A. E. T. El Deen, E.-S. A. El-Badawy, and S. N. Gobran, "Digital Image Encryption Based on RSA Algorithm," *IOSR J. Electron. Commun. Eng.*, vol. 9, no. 1, pp. 69–73, 2014.

[11] K. Loukhaoukha, J. Y. Chouinard, and A. Berdai, "A secure image encryption algorithm based on Rubik's cube principle," *J. Electr. Comput. Eng.*, vol. 2012, 2012.

[12] K. A. Abitha and P. K. Bharathan, "Secure Communication Based on Rubik's Cube Algorithm and Chaotic Baker Map," *Procedia Technol.*, vol. 24, pp. 782–789, 2016.

[13] R. P. Singh and M. Dixit, "Histogram Equalization: A Strong Technique for Image Enhancement," *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol. 8, no. 8, pp. 345–352, 2015.

[14] R. K. Hapsari, M. I. Utoyo, R. Rulaningtyas, and H. Suprajitno, "Comparison of Histogram Based Image Enhancement Methods on Iris Images Comparison of Histogram Based Image Enhancement Methods on Iris Images," *Content from this Work may be used under terms theCreative Commons Attrib. 3.0 licence. Any Furth. Distrib. this Work must Maint. Attrib. to author(s) title Work. J. Cit. DOI.Published under licence*, 2019.

[15] A. Latifa, "Digital Repository Universitas Jember," vol. 02, no. 01, p. 27, 2015.

ISSN (print): 2686-0023
ISSN (online): 2685-6875