Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dengan berkembangnya pertumbuhan dari aplikasi multimedia, keamanan merupakan salah satu isu penting dalam komunikasi dan penyimpanan media seperti gambar (Patel & Belani, 2011). Pada tahun 2013 terjadi kebocoran informasi dari National Security Agency (NSA) Amerika Serikat. Banyak dokumen-dokumen penting seperti prosedur rahasia dalam bentuk gambar digital yang dicuri oleh Edward Snowden yang kemudian disebarluaskan kepada masyarakat umum (Harding, 2014). Berbagai macam informasi penting lain mengenai pemerintahan, militer, perbankan, maupun dokumen-dokumen terdapat dalam sebuah gambar digital (Khizrai & Bodkhe, 2014). Banyak cara yang sudah dilakukan salah satunya termasuk *watermark* digital yang disisipkan ke dalam image dan juga kriptografi (Loukhaoukha, Chouinard, & Berdai, 2012). *Watermark* digital lebih sering digunakan sebagai tanda hak cipta untuk gambar tersebut (Sencar & Memon, 2005). Di sisi lain, kriptografi digunakan untuk melindungi gambar. Kriptografi terdiri dari enkripsi dan dekripsi. Enkripsi merupakan suatu proses untuk mengubah bentuk suatu informasi dari *plaintext* menjadi *ciphertext* agar tidak dapat dipahami apabila tidak didekripsi terlebih dahulu (Chhabra & Sundaram, 2016).

Enkripsi gambar digunakan untuk mengubah gambar asli menjadi suatu gambar lain yang sulit dimengerti orang lain. Dengan kata lain, tidak ada yang dapat mengetahui isi dari gambar tanpa *key* untuk dekripsi (Patel & Belani, 2011). Enkripsi gambar dapat diklasifikasi menjadi 3 grup besar, yaitu algoritma berdasarkan permutasi, algoritma berdasarkan 11perubahan *value*, dan algoritma berdasarkan

Implementasi Algoritma Enkripsi..., Kenny Wantara, FTI UMN, 2018

perubahan visual (Pakshwar dkk., 2013). Beberapa skema enkripsi berdasarkan permutasi sudah ditemukan tidak aman melawan serangan *ciphertext-only* dan *known-plaintext*/*chosen-plaintext* karena redundansi informasi tinggi dan juga permutasi rahasia didapatkan dengan membandingkan *plaintext* dan *ciphertext* yang dipermutasi. Secara umum, algoritma enkripsi gambar berdasarkan perubahan visual lebih banyak digunakan daripada yang lain (Loukhaoukha, Chouinard, & Berdai, 2012).

Berbagai macam algoritma enkripsi gambar telah diusulkan seperti algoritma berdasarkan perubahan visual dengan memanfaatkan sebuah peta *chaotic cat* untuk mengacak posisi dan *value* dari gambar (Chen dkk., 2004), algoritma berdasarkan perubahan transformasi dari setiap blok gambar yang dibagi lalu dienkripsi memakai algoritma *blowfish* pada setiap blok (Pakshwar dkk., 2013), dan juga algoritma enkripsi baru yang menggabungkan permutasi dan difusi dari setiap 4 x 4 *pixel* yang kemudian dienkripsi dengan algoritma RijnDael (Wang dkk., 2011). Loukhaoukha dkk. (2012) mengusung sebuah algoritma enkripsi baru berdasarkan prinsip dari Rubik's cube yang diimplementasikan pada *software* MATLAB. Pengujian dilakukan dengan menghitung besar persentase *Number Pixel Change Rate* (NPCR) dan *Unified Average Changing Intensity* (UACI) pada 4 gambar *grayscale* 8 bit dari *Standard Test Images* dengan ukuran yang sama yaitu 256 x 256 *pixel* dengan menggunakan iterasi satu kali.

Rubik's cube merupakan salah satu permainan yang popular. Peraturan permainan dari Rubik's cube digunakan secara sukses dalam tahap perancangan pada enkripsi gambar digital (IONESCU & DIACONU, 2015). Algoritma enkripsi gambar berbasis Rubik's cube memiliki kemampuan untuk melakukan enkripsi atau dekripsi berdasarkan jumlah iterasi yang ingin dilakukan. Proses enkripsi dan dekripsi akan semakin cepat apabila menggunakan jumlah iterasi yang kecil, tetapi semakin besar

Implementasi Algoritma Enkripsi..., Kenny Wantara, FTI UMN, 2018

jumlah iterasi yang digunakan maka proses pengacakan akan semakin banyak sehingga membuat proses enkripsi lebih aman (Loukhaoukha, Chouinard, & Berdai, 2012).

Berdasarkan latar belakang permasalahan di atas, maka diperlukan penelitian untuk mengimplementasikan algoritma enkripsi berbasis Rubik's cube pada aplikasi enkripsi citra digital berbasis web untuk melindungi gambar digital.

1.2 Rumusan Masalah

Berdasarkan latar belakang permasasalahan yang sudah dijelaskan sebelumnya, masalah yang dirumuskan adalah sebagai berikut.

a. Bagaimana mengimplementasikan algoritma enkripsi berbasis Rubik's cube pada proses enkripsi dan dekprisi citra digital dalam aplikasi enkripsi berbasis web?
b. Bagaimana tingkat NPCR dan UACI dari aplikasi enkripsi citra digital berdasarkan jumlah iterasi yang digunakan ?

1.3 Batasan Masalah

Terdapat tujuh batasan yang didefinisikan, yaitu sebagai berikut.

a. Gambar yang dienkripsi hanya sebatas 512 x 512 *pixel*.
b. Gambar yang dienkripsi hanya berbentuk persegi.
c. Gambar yang dienkripsi merupakan gambar 8-bit.
d. Gambar yang diuji diambil dari Testimages (Asuni & Giachetti, 2015) .
e. Gambar yang diuji menggunakan tiga gambar (Loukhaoukha, Chouinard, & Berdai, 2012)
f. Jumlah iterasi yang digunakan adalah 1, 2, 3, 4, 5, 6, 7, 8, 9, dan 10 (Diyachenko, 2015)
g. Gambar yang dienkripsi hanya sebatas format *Portable Network Graphics* (PNG) (Sinha, 2013).

Implementasi Algoritma Enkripsi..., Kenny Wantara, FTI UMN, 2018

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, tujuan penelitian ini adalah sebagai berikut.

a. Mengimplementasikan algoritma berbasis Rubik's cube untuk melakukan enkripsi dan dekripsi citra digital pada aplikasi berbasis web.
b. Mengukur tingkat NPCR dan UACI dari hasil enkripsi gambar berdasarkan jumlah iterasi yang digunakan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari implementasi algoritma Rubik's cube pada aplikasi enkripsi citra digital berbasis web adalah memberikan keamanan pada citra digital.

1.6 Sistematika Penulisan

Sistematika penulisan skripsi ini terdiri dari lima bab, yaitu sebagai berikut.

1. BAB I PENDAHULUAN

Bab ini terdiri atas latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

2. BAB II LANDASAN TEORI

Bab ini menjelaskan landasan teori dari penelitian yang dilakukan, seperti enkripsi, enkripsi gambar, algoritma berbasis Rubik's cube, dan analisis keamanan enkripsi gambar.

3. BAB III METODOLOGI DAN PERANCANGAN PROGRAM

Bab ini berisikan metode penelitian yang digunakan dan perancangan. Perancangan program yang dimaksud, yaitu perancangan *application model, flowchart,* dan desain antarmuka.

Implementasi Algoritma Enkripsi..., Kenny Wantara, FTI UMN, 2018

4. BAB IV IMPLEMENTASI DAN UJI COBA

Bab ini berisi implementasi dan hasil dari uji coba program yang telah dibangun.

5. BAB V KESIMPULAN DAN SARAN

Bab ini terdiri atas simpulan dari hasil pengujian program dan saran untuk pengembangan program di kemudian hari.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA