Jurnal Ilmiah Informatika (JIF)
| ISSN (Print) 2337-8379 | ISSN (Online) 2615-1049 |
Jurnal online di akses di http://ejournal.upbatam.ac.id/index.php/jif

Pemanfaatan Metode DNA Kriptografi Dalam Meningkatkan Keamanan Citra Digital

Kharisma Mahesa [a], *Bambang Sugiantoro* [b], *Yudi Prayudi* [c]

[a,c] *Universitas Islam Indonesia, Yogyakarta, Indonesia*
[b] *Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia*

INFORMASI ARTIKEL

Sejarah Artikel:
Diterima Redaksi: 28 Agustus 2019
Revisi Akhir: 20 September 2019
Diterbitkan *Online*: 30 September 2019

KATA KUNCI

Digital image, cryptography, DNA cryptography

KORESPONDENSI

No HP: 0852 8959 8116
E-mail: 17917110@students.uii.ac.id

A B S T R A C T

There are many data transmitted on internet and certainly has positive and negative side. Negative side that perceived is the increase in cybercrime activities which is a threat to everyone. Securing confidential data is very necessary so that the data is not misused by others for individual or groups benefit. This research is developing an application that is able to secure data like digital images by applying cryptography. Cryptography is the most appropriate way to secure data like digital images. DNA cryptography is one of cryptography method. Beside to application of computing is very easy, this method has excess speed in processing, use minimal storage and power usage. The result from this research are application that are built can encrypt dan decrypt digital images which has a lot color distribution well. Application and method used will work well on image that have a lot or even distribution colors. But not in digital images that have 1 dominant or transparent color in that.

1. PENDAHULUAN

Meningkatnya penggunaan teknologi dalam kehidupan sehari – hari memiliki sisi positif yang dapat membantu memudahkan kegiatan manusia keseharian seperti komunikasi menggunakan telepon, mengirimkan pesan menggunakan aplikasi whatsapp, telegram, line dan lain sebagainya. Namun terdapat pula sisi negatif yang dapat merugikan pengguna teknologi tersebut, seperti manipulasi data, peretasan pada berbagas situs *web*, penyadapan terhadap data orang lain. Kejahatan seperti ini lebih dikenal dengan istilah *cybercrime*.

Terdapat berbagai macam jenis data yang ditransmisikan melalui jaringan *internet*. Seperti teks, gambar, suara, video dan lain sebagainya. Dan diantara data tersebut terdapat beberapa data yang perlu dirahasiakan. Sebagai contoh sebuah perusahaan ingin mengirimkan hasil desain dari sebuah arsitektur bangunan kepada pihak kliennya yang ingin membangun sebuah bangunan, namun pada saat pengiriman terdapat pihak ketiga yang mencoba untuk mengambil desain tersebut dan membuat desain tersebut seolah – olah adalah karya yang dibuatnya. Hal ini tentu menjadi sangat penting untuk mengamankan sebuah data sebelum ditransmisikan, sehingga tidak bisa digunakan begitu saja oleh orang lain tanpa seizin dari pemilik data tersebut.

Penelitian tentang pengamanan data berupa citra digital sebelumnya telah dilakukan oleh [1]. Penelitian tersebut melakukan enkripsi terhadap metadata yang merupakan informasi yang yang terdapat pada file citra digital dengan menggunakan metode *eXtended Tiny Encryption Algorithm* (XTEA). Namun visual dari citra digital tersebut tetap dapat dilihat oleh orang lain dan akan sangat memungkinkan pihak ketiga untuk menduplikasi atau memanipulasi citra tersebut dan membuat citra digital tersebut seolah – olah adalah hasil karyanya. Mengingat banyaknya aplikasi yang memungkinkan untuk menduplikasi dan memanipulasi citra digital serta metadata yang terdapat didalamnya. Dengan demikian perlu adanya penanganan dari masalah tersebut.

Kriptografi merupakan cara yang tepat untuk melakukan pengamanan terhadap visual dari citra digital, yang dimana enkripsi dan dekripsi menjadi fungsi dasar dari kriptografi [2] DNA kriptografi merupakan salah satu metode dari kriptografi. DNA kriptografi yang baru lahir muncul pada tahun 1994 dengan penelitian komputasi DNA. DNA Kriptografi memiliki kemampuan pemrosesan paralel dengan tingkat melekuler untuk memecahkan masalah komputasi yang kompleks. DNA Kriptografi dan ilmu informasi adalah aplikasi yang efektif

dalam desain, analisis dan penerapan kriptosistem DNA. Dan penelitian tentang Kriptografi DNA masih dalam tahap awal dan membutuhkan banyak penelitian di bidang ini. Pemilihan terhadap metode DNA Kriptografi selain penerapan kedalam komputasi yang sangat mudah, metode ini memiliki kelebihan yaitu memiliki kecepatan dalam pemrosesan, persyaratan daya yang minimal dan persyaratan penyimpanan yang minimal [3]–[5].

Dengan demikian didalam penelitian ini metode DNA Kriptografi dianggap metode yang tepat yang diharapkan mampu melakukan pengamanan terhadap citra digital yang bertujuan untuk menjaga citra digital tetap aman pada saat ditransmisikan.

2. TINJAUAN PUSTAKA

Citra Digital

Citra digital merupakan representasi dari gambar dua dimensi yang dibatasi oleh nilai digital atau lebih dikenal dengan elemen gambar atau piksel. Citra digital juga dapat direpresentasikan dalam sebuah matriks *f(x,y)* yang terdiri dari *M* kolom dan *N* baris, yang dimana perpotongan antara kolom dan baris bisa disebut dengan piksel *(pixel = picture element)* [6], [7].

$$f(x,y) \approx \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,M-1) \\ f(1,0) & f(1,1) & \dots & f(1,M-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(N-1,0) & f(N-1,1) & \cdots & f(N-1,M-1) \end{bmatrix} \quad (1)$$

a. Jenis Citra Digital

Pada umumnya citra digital menjadi 3 macam [7], diantaranya adalah:

1. *Binary Image* adalah jenis citra digital yang hanya terdiri dari warna hitam dan putih. Disebut *binary* karena hanya ada dua warna untuk setiap pikselnya, maka hanya perlu 1 *bit* untuk masing – masing pikselnya (0 dan 1).
2. *Black and White* atau citra hitam putih atau *grayscale* adalah citra dimana setiap pikselnya memiliki gradiasi mulai dari warna putih hingga hitam. Dengan demikian masing masing piksel dapat diwakili oleh 8 *bit* atau 1 *byte*.
3. *Color Image* atau RGB *(Red, Green, Blue)* atau citra berwarna yang dimana setiap piksel memiliki warna tertentu dimana warna tersebut merupkan representasi dari warna merah *(Red)*, hijau *(Green)*, biru *(Blue)*. Setiap masing masing warna tersebut memiliki *range* antara 0 - 255, dengan total yaitu 2553 = 16.581.375 variasi warna berbeda pada sebuah gambar. Pada dasarnya *color image* atau citra berwarna ini terdiri dari tiga buah matriks yang mewakili nilai R, G dan B atau merah, hijau dan biru untuk masing masing pikselnya.

b. Format Citra Digital

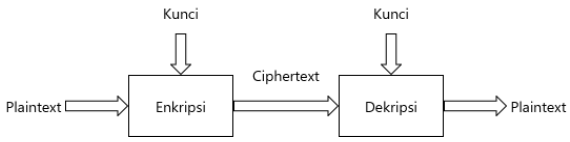
1. JPG *(Joint Photographic Group)* pada awalnya bukanlah sebuah *format file* atau gambar. JPEG merupakan sebuah algoritma yang dikembangkan oleh Joint Photographic Experts Group pada tahun 1990. JPEG atau JPG sangat cocok digunakan untuk penyimpanan gambar berwarna yang kompleks seperti foto. JPEG atau JPG adalah *format file* yang sangat tepat untuk diakses dalam penggunaan dan proses kompresi untuk transmisi *online* yang lebih cepat. JPEG merupakan nama lengkap dari JPG. Ekstensi tiga karakter yaitu JPG adalah *format file* yang paling sering digunakan [8], [9].
2. PNG *(Portable Network Graphics)* atau lebih dikenal dengan *format file* PNG dikembangkan oleh PNG Development Group pada tahun 1996. *Format file* ini mendukung kedalaman warna dari 1 *bit* hingga 48 *bit*. Gambar yang tersimpan selalu dalam keadaan terkompresi dengan algoritma *deflate* berbasis LZ77 *lossless* yang tidak dipatenkan. Oleh sebab itu bebas digunakan [8]. PNG merupakan generasi dari GIF dan merupakan standar *web* dan dengan cepat menjadi salah satu *format* gambar yang paling umum digunakan secara online [10].
3. BMP *(Bitmap)* dikembangkan oleh Microsoft sebagai *format vektor* asli sistem operasi Windows. Versi *format* ini rilis bertepatan dengan rilisnya Windows, dimana versi pertama muncul pada tahun 1985 dengan Windows 1.0. Versi tambahan kemudian dikembangkan untuk digunakan dengan sistem operasi IBM OS / 2. *Format* BMP mendukung kedalaman warna 1 *bit* hingga 32 *bit* dan memberikan kompresi optional *lossless* RLE. Namun, meskipun dipatenkan, *format* ini gratis untuk digunakan oleh siapapun karena hubungannya dengan Windows. Akan tetapi popularitas dari *format* ini menurun setelah muncul *format - format* baru [8].

Kriptografi

Kriptografi merupakan seni penulisan rahasia yang telah digunakan sejak zaman Romawi yang digunakan untuk menyembunyikan informasi atau mengamankan informasi. Metode yang banyak digunakan adalah enkripsi yaitu mengubah pesan sederhana *(plaintext)* menjadi pesan yang tidak dapat dibaca oleh orang lain *(ciphertext)*. Dan juga dekripsi untuk mengembalikan pesan rahasia *(ciphertext)* agar dapat dibaca kembali atau diubah kembali menjadi pesan asli *(plaintext)* [2]. [11] Tujuan dari kriptografi ialah memberikan keamanan dalam aspek-aspek diantaranya:

a. Kerahasiaan *(Confidentiality)* yang merupakan layanan untuk menjaga agar data tidak bisa dibaca oleh pihak – pihak yang tidak berhak. Terkecuali memiliki kunci untuk membuka atau mengakses informasi yang telah terkriptografi.
b. Integritas Data *(Data Integrity)* yang merupakan layanan yang dapat menjamin bahwa data yang diperoleh masih asli dan belum di manipulasi selama pengiriman.
c. Otentikasi *(Authentication)* yang merupakan identifikasi baik dari kedua belah pihak antara pengirim dan penerima maupun data itu sendiri.
d. *Non-repudiation* yang merupakan tindakan pencegahan pengirim ataupun penerima mengingkari bahwa mereka telah menerima ataupun mengirimkan sebuah data.

Berikut merupakan skema proses enkripsi dan dekripsi dalam pertukaran informasi:



Gambar 1. Skema Enkripsi dan Dekripsi

DNA Kriptografi

Salah satu teknik yang muncul di dunia kriptografi adalah DNA kriptografi yang bekerja pada konsep komputasi DNA. Dengan menggunakan struktur biologis DNA. Teknik baru yang digunakan untuk mengamankan data diperkenalkan dan disebut dengan komputasi DNA / komputasi biologis. Keuntungan dari komputasi DNA diantaranya adalah kecepatan, persyaratan daya yang minimal, persyaratan penyimpanan yang minimal. Satu gram DNA mengandung sekitar 1021 basis DNA atau sekitar 108 *tera-byte*. Dengan demikian beberapa gram DNA mungkin memiliki potensi untuk menyimpan semua data atau informasi yang ada didunia. Dengan demikian perkembangan kriptografi DNA mendapat manfaat dari kemajuan komputasi DNA atau bisa disebut dengan (komputasi molekuler atau komputasi biologis). Disisi lain pula, paling tidak kriptografi selalu memilki beberapa hubungan dengan model komputasi yang sesuai [4], [5]. Hubungan antara kriptografi dan biologi molekuler pada awalnya tidak relavan, akan tetapi dengan studi yang mendalam tentang *bioteknologi modern* dan komputasi DNA, kedua disiplin ilmu ini bekerja sama lebih erat. DNA Kriptografi adalah ilmu informasi yang lahir setelah penelitian dibidang komputasi DNA oleh Adlemen. DNA Kriptografi didasarkan pada masalah biologis. Secara teori, komputer DNA tidak hanya memiliki kekuatan komputasi yang sama dengan komputer *modern*, tetapi juga akan memiliki potensi dan fungsi yang tidak dapat ditandingi oleh komputer tradisional [12].
Komputasi DNA mengacu pada asam *nukleat De-Oxy Ribo* yang merupakan asam nukleat yang mengandung informasi genetik yang digunakan untuk pertumbuhan serta berfungsinya semua organisme hidup. Segmen didalam DNA yang menyimpan informasi genetik dikenal sebagai gen. Urutan tersebut digunakan untuk memodifikasi penggunaan informasi genetik seperti *string* atau *biner* yang dikodekan dengan 0 dan 1. Pengkodean untai DNA terdapat 4 baris yang diwakili oleh huruf A *(Adenine)*, T *(Timin)*, C *(Cytosine)*, dan G *(Guanin)* [13].

3. METODOLOGI

Tahapan ini merupakan tahapan bagaimana proses penelitian ini dilakukan yang dibuat dalam bentuk langkah – langkah kerja sebagai panduan menyelesaikan masalah yang ada.

Identifikasi Masalah

Tahapan ini merupakan tahapan awal dalam melakukan sebuah penelitian yang dimana pada tahapan ini akan ditentukan sebuah topik atau ide penelitian yang diperoleh dari permasalahan yang ada, informasi yang ada maupun berupa pengembangan dari penelitian yang telah dilakukan sebelumnya.

Studi Literatur

Tahapan ini merupakan tahapan untuk mengumpulkan toeri – teori terkait dengan topik penelitian agar penelitian menjadi lebih terarah. Setelah informasi diperoleh dari masing – masing literatur lalu dilakukan analisa – analisa untuk mengetahui kelemahan yang ada yang kemudian dilakukan perbaikan dengan pengembangan terhadap metode yang ada, untuk mendapatkan hasil yang lebih baik.

Desain dan Implementasi

Setalah selesai pada tahapan studi literatur, selanjutnya yaitu melakukan desain aplikasi yang dibangun dan mengimplementasi metode pada aplikasi tersebut. Dan berikut penerapan metode pada proses enkripsi dan dekripsi yang diterapkan diaplikasi yang dibangun:

a. Enkripsi

Proses ini merupakan proses untuk menyembunyikan citra digital dengan metode DNA kriptografi.

Gambar 2. Proses Enkripsi

1. Melakukan *input* data berupa citra digital yang kemudian diambil nilai desimal dari masing – masing R, G dan B pada citra digital tersebut.
2. Nilai desimal yang diperoleh dikonversikan ke bentuk *biner*.
3. Nilai *biner* kemudian dikonversikan kedalam bentuk kode DNA dengan ketentuan nilai *biner* dibagi menjadi 4 bagian, dan setiap bagian tersebut dimana setiap 00 diganti menjadi A, 01 menjadi T, 10 menjadi G dan 11 menjadi C.
4. Konversi kode DNA menjadi nilai desimal berdasarkan indeks dari pengacakan kode DNA pada Gambar 3.
5. Lakukan proses pada setiap piksel.
6. Nilai desimal yang diperoleh digunakan pada piksel untuk membuat citra baru yang merupakan citra terenkripsi.

1	AAAA	33	CAAA	65	GAAA	97	TAAA	129	AGAA	161	CGAA	193	GGAA	225	TGAA
2	AAAC	34	CAAC	66	GAAC	98	TAAC	130	AGAC	162	CGAC	194	GGAC	226	TGAC
3	AAAG	35	CAAG	67	GAAG	99	TAAG	131	AGAG	163	CGAG	195	GGAG	227	TGAG
4	AAAT	36	CAAT	68	GAAT	100	TAAT	132	AGAT	164	CGAT	196	GGAT	228	TGAT
5	AACA	37	CACA	69	GACA	101	TACA	133	AGCA	165	CGCA	197	GGCA	229	TGCA
6	AACC	38	CACC	70	GACC	102	TACC	134	AGCC	166	CGCC	198	GGCC	230	TGCC
7	AACG	39	CACG	71	GACG	103	TACG	135	AGCG	167	CGCG	199	GGCG	231	TGCG
8	AACT	40	CACT	72	GACT	104	TACT	136	AGCT	168	CGCT	200	GGCT	232	TGCT
9	AAGA	41	CAGA	73	GAGA	105	TAGA	137	AGGA	169	CGGA	201	GGGA	233	TGGA
10	AAGC	42	CAGC	74	GAGC	106	TAGC	138	AGGC	170	CGGC	202	GGGC	234	TGGC
11	AAGG	43	CAGG	75	GAGG	107	TAGG	139	AGGG	171	CGGG	203	GGGG	235	TGGG
12	AAGT	44	CAGT	76	GAGT	108	TAGT	140	AGGT	172	CGGT	204	GGGT	236	TGGT
13	AATA	45	CATA	77	GATA	109	TATA	141	AGTA	173	CGTA	205	GGTA	237	TGTA
14	AATC	46	CATC	78	GATC	110	TATC	142	AGTC	174	CGTC	206	GGTC	238	TGTC
15	AATG	47	CATG	79	GATG	111	TATG	143	AGTG	175	CGTG	207	GGTG	239	TGTG
16	AATT	48	CATT	80	GATT	112	TATT	144	AGTT	176	CGTT	208	GGTT	240	TGTT
17	ACAA	49	CCAA	81	GCAA	113	TCAA	145	ATAA	177	CTAA	209	GTAA	241	TTAA
18	ACAC	50	CCAC	82	GCAC	114	TCAC	146	ATAC	178	CTAC	210	GTAC	242	TTAC
19	ACAG	51	CCAG	83	GCAG	115	TCAG	147	ATAG	179	CTAG	211	GTAG	243	TTAG
20	ACAT	52	CCAT	84	GCAT	116	TCAT	148	ATAT	180	CTAT	212	GTAT	244	TTAT
21	ACCA	53	CCCA	85	GCCA	117	TCCA	149	ATCA	181	CTCA	213	GTCA	245	TTCA
22	ACCC	54	CCCC	86	GCCC	118	TCCC	150	ATCC	182	CTCC	214	GTCC	246	TTCC
23	ACCG	55	CCCG	87	GCCG	119	TCCG	151	ATCG	183	CTCG	215	GTCG	247	TTCG
24	ACCT	56	CCCT	88	GCCT	120	TCCT	152	ATCT	184	CTCT	216	GTCT	248	TTCT
25	ACGA	57	CCGA	89	GCGA	121	TCGA	153	ATGA	185	CTGA	217	GTGA	249	TTGA
26	ACGC	58	CCGC	90	GCGC	122	TCGC	154	ATGC	186	CTGC	218	GTGC	250	TTGC
27	ACGG	59	CCGG	91	GCGG	123	TCGG	155	ATGG	187	CTGG	219	GTGG	251	TTGG
28	ACGT	60	CCGT	92	GCGT	124	TCGT	156	ATGT	188	CTGT	220	GTGT	252	TTGT
29	ACTA	61	CCTA	93	GCTA	125	TCTA	157	ATTA	189	CTTA	221	GTTA	253	TTTA
30	ACTC	62	CCTC	94	GCTC	126	TCTC	158	ATTC	190	CTTC	222	GTTC	254	TTTC
31	ACTG	63	CCTG	95	GCTG	127	TCTG	159	ATTG	191	CTTG	223	GTTG	255	TTTG
32	ACTT	64	CCTT	96	GCTT	128	TCTT	160	ATTT	192	CTTT	224	GTTT	256	TTTT

Gambar 3. Pengacakan Kode DNA

b. Dekripsi

Dan berikut merupakan proses untuk mengembalikan citra digital yang terenkripsi menjadi semula dengan metode DNA kriptografi.

Gambar 4. Proses Dekripsi

1. Melakukan *input* data citra digital yang terenkripsi yang kemudian diambil nilai desimal dari masing – masing R, G dan B pada citra digital tersebut.
2. Nilai desimal yang diperoleh dikonversikan ke bentuk kode DNA berdasarkan indeks dari pengacakan kode DNA pada Gambar 3.
3. Kode DNA yang diperoleh dikonversikan menjadi nilai *biner* dengan ketentuan kode DNA dibagi menjadi 4 bagian, dan setiap karakter bernilai A akan menjadi 00, T menjadi 01, G menjadi 10 dan C menjadi 11.
4. Nilai *biner* di yang diperoleh dikonversikan menjadi nilai desimal.
5. Lakukan proses pada setiap piksel.

Nilai desimal yang diperoleh digunakan pada piksel untuk membuat citra baru yang merupakan citra terdekripsi.

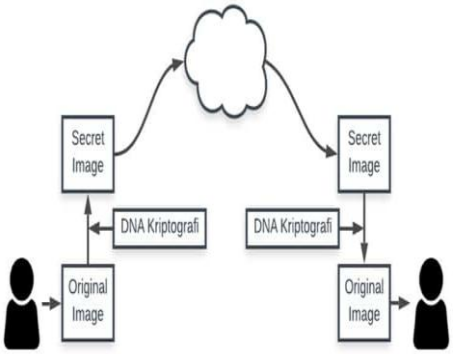
Pengujian dan Evaluasi

Tahapan ini merupakan tahapan pengujian terhadap aplikasi yang dibuat. Setelah dilakukan pengujian hasil dari sistem aplikasi tersebut, maka tahapan selanjutnya yaitu mengevaluasi hasil dari kinerja sistem aplikasi tersebut apakah sistem aplikasi yang telah dibuat berjalan dengan baik dan sesuai berdasarkan desain yang telah dibuat.

4. HASIL DAN PEMBAHASAN

Skenario Aplikasi

Bagian ini merupakan penjelasan dari alur sistem aplikasi yang akan dibuat. Berikut gambaran sistem tersebut:

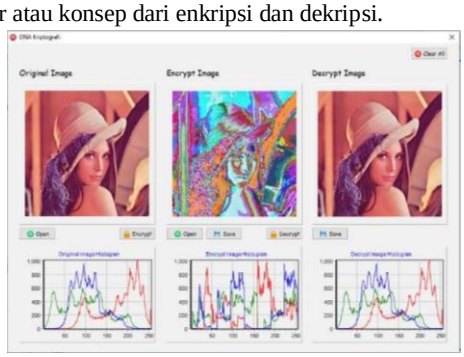


Gambar 5. Skenario Sistem Aplikasi

Dari gambaran yang ditunjukkan pada Gambar 5 tersebut, sebelum citra digital di transmisikan, pengirim terlebih dahulu mengenkripsi citra dengan menggunakan metode DNA kriptografi kemudian diperoleh secret image. Dan penerima hanya dapat melihat citra digital tersebut dengan melakukan dekripsi menggunakan metode DNA kriptografi.

Uji Coba Aplikasi

Uji coba aplikasi merupakan pengujian yang dilakukan untuk mengetahui apakah aplikasi yang dibuat sudah sesuai dengan prosedur atau konsep dari enkripsi dan dekripsi.



Gambar 6. Proses Enkripsi dan Dekripsi pada Aplikasi

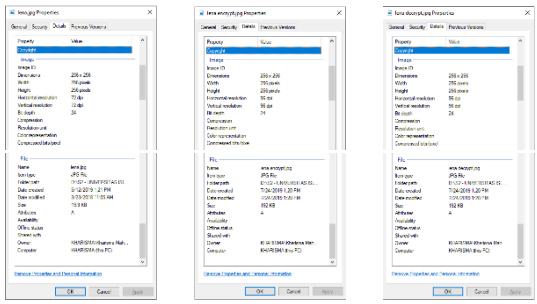
Secara keseluhan berdasarkan pengujian yang dilakukan, aplikasi yang dibuat telah sesuai dengan konsep kriptografi dengan adanya proses enkripsi dan dekripsi dengan menerapkan metode DNA kriptografi didalamnya.

Analisa Visual

Analisa visual merupakan analisa berdasarkan indera penglihatan manusia. Analisa ini berfungsi untuk melihat perubahan yang terjadi pada citra digital berdasarkan tampilan visual, metadata dan kapasitas dari citra sebelum dienkripsi, citra yang telah dienkripsi dan citra yang telah didekripsi.

(a) (b) (c)

Gambar 7. Tampilan Citra Hasil Proses Enkripsi dan Dekripsi



(a) (b) (c)

Gambar 8. Tampilan Metadata Citra Hasil Proses Enkripsi dan Dekripsi

Berdasarkan analisa yang dilakukan, citra yang terenkripsi akan tidak terlihat jelas seperti yang ditunjukkan pada Gambar 8 (b). sehingga penglihatan menusia tidak akan mengetahui maksud dari gambar tersebut. Dan berdasarkan metadata dari masing – masing citra original atau citra awal (ditunjukkan pada Gambar 9(a)) dan citra terenkripsi (ditunjukkan pada Gambar 9(b)) dan citra terdekripsi (ditunjukkan pada Gambar 9(c)). Tidak terjadi perubahan sama sekali pada *Dimensions* atau tinggi dan lebar

dari semua citra tersebut. Hanya saja kapasitas citra digital setelah dilakukan enkripsi menjadi bertambah.

Analisa Entropi dan PSNR

Entropi merupakan derajat ketidakpastian pada sebuah citra digital. Yang dimana nilai entropi berfungsi untuk mengetahui keacakan dari citra digital yang dienkripsi. Nilai entropi yang ideal adalah 8 atau mendekati [14]. Sedangkan PSNR atau *Peak Signal to Noise Ratio* merupakan nilai rasio antara citra digital sebelum dienkripsi dengan citra digital setelah dienkripsi. Nilai PSNR dinyatakan dalam *desibel* atau db. Jika pada Steganografi nilai yang dihasilkan harus > 30 db agar tidak dapat membedakan antara citra yang disisipi pesan dengan citra yang belum disisipi pesan, maka pada kriptografi nilai PSNR yang dihasilkan harus kecil.
Berikut merupakan tabel nilai entropi dan PSNR dari beberapa pengujian terhadap citra digital:

Tabel 1. Tabel Nilai Entropi dan PSNR

No	Nama dan Tipe Citra Digital	Nilai Entropi	Nilai PSNR
1	lena.jpg	7,7584	8,30 db
2	bird.jpg	7,2360	8,81 db
3	ant.jpg	1,8003	2,41 db
4	butterfly.jpg	7,3645	9,51 db
5	swan.jpg	6,6310	8,22 db
6	nemo.bmp	7,8882	8,18 db
7	saturn.bmp	7,1120	6,61 db
8	stonehenge.bmp	7,5788	8,40 db
9	penguin.bmp	7,4584	9,08 db
10	air.png	3,5462	15,02 db
11	google.png	2,5250	2,00 db

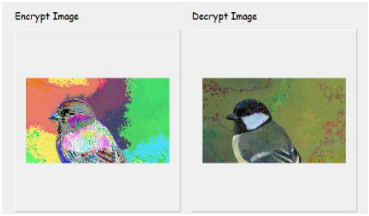
Dari analisa yang telah dilakukan, citra yang memiliki sebaran warna yang sedikit atau memiliki latar belakang 1 warna yang dominan atau bahkan terdapat piksel yang memiliki warna yang transparan, tidak dapat mempengaruhi nilai entropi yang digunakan untuk melihat tingkat keacakan dari enkripsi citra digital tersebut. Begitu juga nilai PSNR yang digunakan untuk melihat keidentikan antara citra digital sebelum diproses dengan citra digital setelah diproses. Terlihat seperti citra digital dengan nama citra digital **ant.jpg** yang terlihat nilai jauh berbeda dengan nilai dari *format file* JPG lainnya yang dimana hal ini disebabkan oleh adanya 1 warna yang dominan pada citra digital tersebut. Begitu juga citra digital dengan *format file* PNG yaitu dengan nama citra digital **air.png** dan **google.png**. Nilai yang dihasilkan memiliki ketimpangan antara kedua citra tersebut.

Uji Ketahanan Citra Digital

Bagian ini merupakan pengujian terhadap ketahanan citra yang telah terenkripsi terhadap manipulasi yang terjadi. Tujuan dari pengujian ini adalah untuk mengetahui apakah metode yang digunakan mampu mengembalikan atau mendekripsi citra yang terenkripsi yang kemudian di manipulasi kembali seperti semula. Berikut pengujian terhadap beberapa manipulasi pada citra digital, diantaranya:

a. *Cropping*

Cropping merupakan proses penghapusan bagian gambar untuk mengambil sebagai isi gambar guna memperoleh hasil yang diinginkan. Dan dalam pengujian ini, citra digital yang terenkripsi dihapus pada bagian tertentu dan kemudian dilakukan dekripsi pada citra digital terenkripsi yang dihapus tersebut.

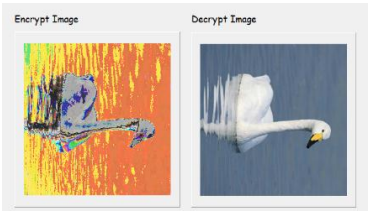


Gambar 9. Hasil Dekripsi Citra Digital *Cropping*

Pada proses pendekripsian citra digital terenkripsi yang telah dilakukan manipulasi, aplikasi yang dibuat hanya mampu mengembalikan sebagian citra digital yang telah dienkripsi. Hal ini dikarenakan sebagian dari citra digital tersebut telah dimanipulasi dengan cara dihapus sebagian dari citra digital sebelum didekripsi atau disebut dengan proses *cropping*. Oleh sebab itu pengembaliannya pun tidak akan mendapatkan hasil yang seutuhnya. Namun sebagian lain yang tidak dihapus dapat didekripsi dengan baik.

b. *Rotating*

Rotating merupakan proses memutar gambar sesuai derajat yang diinginkan. Pengujian ini diperlukan untuk melihat apakah citra digital terenkripsi yang kemudian dimanipulasi dengan cara merotasi citra tersebut akan dapat dekripsi. Pada pengujian ini citra digital terenkripsi akan dirotasi 90°.



Gambar 10. Hasil Dekripsi Citra Digital *Rotating*

Pada pengujian rotating, citra digital terenkripsi dapat dikembalikan secara keseluruhan tanpa ada bagian yang terpotong. Hanya saja citra digital yang telah didekripsi mengalami rotasi yang dimana hal ini disebabkan karena sebelum dilakukan proses dekripsi, citra yang terenkripsi di rotasi sebanyak 90°. Dengan demikian aplikasi akan mengembalikan citra digital sesuai dengan keadaan citra digital terenkripsi.

c. Kompresi

Kompresi merupakan proses memampatkan sebuah gambar yang berkapasitas besar menjadi lebih kecil yang berfungsi untuk mengurangi penggunaan ruang penyimpanan. Dalam pengujian ini, citra digital yang terenkripsi dilakukan proses kompresi terlebih dahulu sebelum didekripsi dengan hasil yang diharapkan setelah didekripsi citra digital tersebut dapat kembali seperti semula.

Gambar 11. Hasil Dekripsi Citra Digital Kompresi

Dari pengujian yang dilakukan, secara visual citra digital terenkripsi yang kemudian dikompresi tidak dapat dikembalikan secara utuh atau didekripsi kebentuk semula secara sempurna. Hal ini dipengaruhi oleh proses kompresi atau pemampatan pada citra digital yang dilakukan untuk mengurangi kapasitas pada citra digital tersebut yang tentu saja sangat berpengaruh pada kualitas dari citra digital.

5. KESIMPULAN DAN SARAN

Kesimpulan

1. Aplikasi yang dibuat dengan menggunakan Delphi 10.3 dengan menerapkan metode DNA kriptografi dalam meningkatkan keamanan citra digital berhasil melakukan proses enkripsi dan dekripsi terhadap citra digital.
2. Aplikasi yang dibuat jauh lebih baik bekerja pada *format citra* digital JPG dan BMP dibandingkan dengan *format* citra digital PNG.
3. Citra digital akan lebih aman jika sebaran warna yang terdapat pada citra digital sebelum dienkripsi lebih merata. Semakin berwarna citra digital tersebut, maka akan semakin lebih baik metode yang digunakan bekerja

Saran

1. Pada penelitian selanjutnya diharapkan dapat menambahkan kunci yang di gabungkan dengan konsep dari DNA kriptografi yang tentunya dapat lebih meningkatkan tingkat keamanan dari citra digital.
2. Diharapkan dapat dilakukan pengembangan pada tipe file yang sulit seperti video atau dengan format citra yang lain untuk melihat tingkat keamanan citra digital dari berbagai format citra digital

DAFTAR PUSTAKA

[1] H. Wijayanto, I. Riadi, and Y. Prayudi, "Encryption EXIF Metadata for Protection Photographic Image of Copyright Piracy," *Int. J. Res. Comput. Commun. Technol.*, vol. 5, no. 5, pp. 237–242, 2016.

[2] F. Maqsood, M. Ahmed, M. Mumtaz Ali, and M. Ali Shah, "Cryptography: A Comparative Analysis for Modern Techniques," *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 6, pp. 442–448, 2017.

[3] T. Anwar, S. Paul, and S. K. Singh, "Message transmission based on DNA cryptography: Review," *Int. J. Bio-Science Bio-Technology*, vol. 6, no. 5, pp. 215–222, 2014.

[4] X. Guozhen, L. Mingxin, Q. Lei, and L. Xuejia, "New field of cryptography: DNA cryptography," *Chinese Sci. Bull.*, vol. 51, no. 12, pp. 1413–1420, 2006.

[5] M. Rathi, S. Bhaskare, T. Kale, N. Shah, and N. Vaswani, "Data Security Using DNA Cryptography," *Int. J. Comput. Sci. Mob. Comput.*, vol. 5, no. 10, pp. 123–129, 2016.

[6] M. Bhat, "Digital Image Processing," *Int. J. Sci. Technol. Res.*, vol. 3, no. 1, pp. 272–276, 2014.

[7] R. Kusumanto and G. V. Tompunu, "PENGOLAHAN CITRA DIGITAL UNTUK MENDETEKSI OBYEK MENGGUNAKAN PENGOLAHAN WARNA MODEL NORMALISASI RGB," in *Seminar Nasional Teknologi Informasi & Komunikasi Terapan*, 2011.

[8] T. N. Archives, "Graphics File Formats," 2008. [Online]. Available: https://www.nationalarchives.gov.uk/documents/graphic-file-formats.pdf.

[9] N. Archives, "Digital File Types." [Online]. Available: https://www.archives.gov/preservation/products/definitions/filetypes.html.

[10] 99designs, "Image file formats: when to use each type of file." [Online]. Available: https://99designs.com/blog/tips/image-file-types/.

[11] F. N. Pabokory, I. F. Astuti, and A. H. Kridalaksana, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard," *Inform. Mulawarman*, vol. 10, no. 1, p. 20, 2015.

[12] Y. Zhang and L. H. Bochen Fu, "Research on DNA Cryptography," in *Applied Cryptography and Network Security*, 2012.

[13] B. B. Raj, J. Frank Vijay, and T. Mahalakshmi, "Secure Data Transfer through DNA Cryptography using Symmetric Algorithm," *Int. J. Comput. Appl.*, vol. 133, no. 2, pp. 19–23, 2016.

[14] R. Munir, "Analisis Keamanan Algoritma Enkripsi Citra Digital Menggunakan Kombinasi Dua Chaos Map," *J. Ilm. Teknol. Inf.*, vol. 10, no. 2, pp. 45–51, 2012.

BIODATA PENULIS

Kharisma Mahesa
Mahasiswa Pascasarjana di Jurusan Teknik Informatika Universitas Islam Indonesia. Minat penelitian meliputi citra digital, kriptografi, *watermarking* dan *steganography*.

Bambang Sugiantoro
Dosen senior di Jurusan Teknik Informatika Universitas Islam Negeri Sunan Kalijaga dan Universitas Islam Indonesia. Minat penelitian meliputi digital forensik, keamanan siber, dan kriptografi.

Yudi Prayudi
Dosen senior di Jurusan Teknik Informatika Universitas Islam Indonesia. Minat penelitian meliputi digital forensik, *cybercrime, watermarking, steganography,* analisa *malware* dan keamanan jaringan.