BAB II
LANDASAN TEORI

2.1 Identitas

Identitas merupakan ciri yang beraneka ragam dari seseorang seperti budaya, agama, etnis, jenis kelamin dan lainnya (Ting-Toomey, 2015). Mengutip dari Undang-Undang Republik Indonesia Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Pasal 1 ayat (14), Kartu Tanda Penduduk (KTP) merupakan identitas resmi penduduk sebagai bukti diri yang berlaku di seluruh wilayah Negara Kesatuan Republik Indonesia. Pada Pasal 1 ayat (2) dijelaskan bahwa penduduk adalah Warga Negara Indonesia (WNI) dan orang asing yang bertempat tinggal di Indonesia. Peraturan Presiden Republik Indonesa Nomor 26 Tahun 2009, Pasal 1 ayat 4, menyatakan bahwa penduduk yang telah berumur 17 tahun atau telah kawin atau pernah kawin secara sah, wajib memiliki KTP. Berdasarkan Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 tentang Perubahan atas Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan, Pasal 1 ayat (14), KTP untuk WNI memiliki masa berlaku seumur hidup sedangkan KTP untuk orang asing masa berlakunya sesuai dengan masa berlaku Izin Tinggal Tetap.

Berdasarkan Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 74 Tahun 2015 tentang Tata Cara Perubahan Elemen Data Penduduk dalam Kartu Tanda Penduduk Elektronik, Pasal 2 ayat (1), menyatakan bahwa data penduduk dalam KTP Elektronik adalah sebagai berikut.

1. Nomor Induk Kependudukan (NIK)
2. Nama

3. Tempat tanggal lahir
4. Laki-laki atau perempuan
5. Agama
6. Status perkawinan
7. Golongan darah
8. Alamat
9. Pekerjaan
10. Kewarganegaraan
11. Pas foto
12. Masa berlaku
13. Tempat dan tanggal dikeluarkan KTP
14. Tanda tangan pemilik KTP

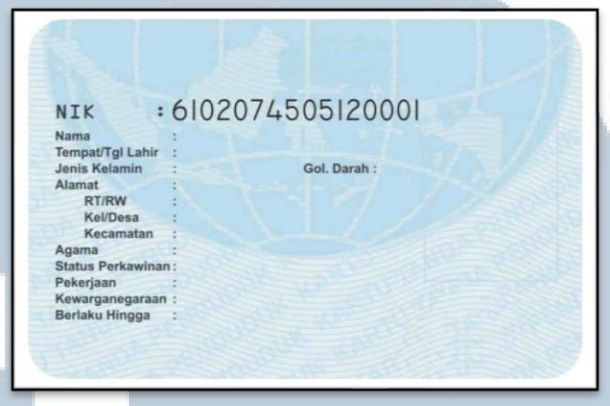
Dalam bagian penjelasan umum pada UU Nomor 23 Tahun 2006, dijelaskan bahwa Nomor Induk Kependudukan (NIK) yang terdiri dari 16 digit bersifat unik , tunggal, dan melekat pada seseorang. NIK juga merupakan kunci akses dalam verifikasi dan validasi data diri, karena seluruh Dokumen Kependudukan dikaitkan secara langsung oleh NIK.

Pengisian data diri dijelaskan dalam tata cara pengisian biodata pada Formulir Kependudukan dan Pencatatan Sipil dengan kode F-1.01. Formulir F-1.01 dapat dilihat pada Lampiran 1.

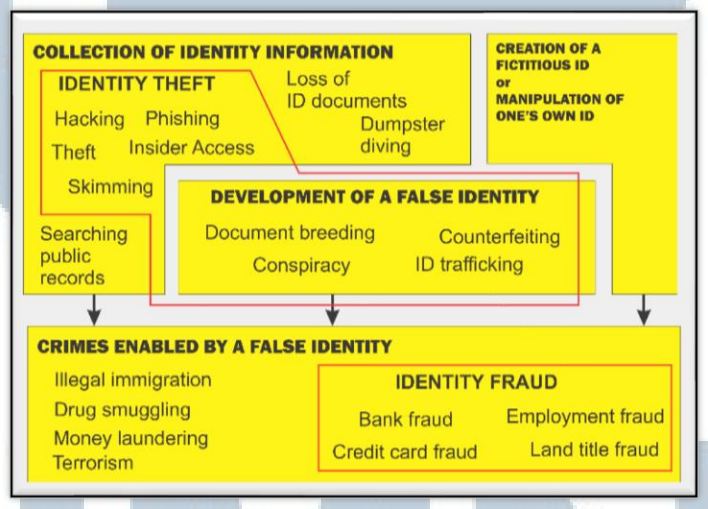
2.2 Pencurian Identitas

Suatu tindak kejahatan dapat dikatakan sebagai pencurian identitas saat identitas seorang individu disalahgunakan untuk mendapatkan keuntungan tertentu.

Identitas yang dicuri dapat berupa nomor, data diri pada Kartu Tanda Penduduk (KTP), nomor telepon, nama ibu kandung, *email*, dan lainnya (CIPPIC, 2017).



Gambar 2.1 *Field* pada Kartu Tanda Penduduk (KTP) Indonesia



Gambar 2.2 *Identity Theft Model* (CIPPIC, 2017)

Gambar 2.2 menjelaskan bahwa kejahatan *identity theft* terjadi melalui dua tahap yaitu sebagai berikut.

1. *Unauthorized collection*, adalah identitas yang diambil dapat berasal dari seseorang yang masih hidup maupun sudah meninggal, tanpa persetujuan dan sepengetahuan pihak terkait. Cara yang dapat digunakan dapat berupa pencurian, penipuan, dan lainnya. Identitas tersebut dapat segera digunakan atau disimpan untuk kejahatan di masa yang akan datang.

2. *Fraudulent use*, adalah saat identitas yang diambil disalahgunakan untuk melakukan tindak kejahatan. Pelaku akan berpura-pura sebagai korban untuk mendapatkan keuntungan yang dapat diklaim atas nama korban.

Identitas setiap orang bersifat unik dan pribadi, maka dari itu efek dari pencurian identitas lebih dari sekedar kerugian finansial. Korban dari tindak pencurian biasa dapat mengganti kerugian yang dialaminya, namun korban dari pencurian identitas dapat kehilangan reputasi dan kedudukan di masyarakat. Dibandingkan dengan pencurian biasa, membutuhkan waktu yang sangat lama untuk mengembalikan reputasi dan kedudukan (CIPPIC, 2007).

2.3 Kriptografi

Kriptografi merupakan suatu metode untuk menjaga kerahasiaan suatu informasi. Terdapat dua konsep utama yang ada dalam kriptografi yaitu enkripsi dan dekripsi. Konsep dari enkripsi adalah membuat informasi asli menjadi suatu karakter baru yang tidak dapat dipahami, sedangkan dekripsi adalah cara untuk mengubah karakter yang tidak dikenali tersebut menjadi informasi asli yang dapat dipahami (Romadhoni, dkk., 2014).

Kriptografi tradisional merupakan kriptografi yang menggunakan kunci untuk mengamankan data. Teknik dasar yang umum digunakan adalah subtitusi dan transposisi. Kriptografi modern menggunakan algoritma komputer yang kompleks untuk mengenkripsi datanya. Algoritma pada kriptografi modern adalah sebagai berikut (Marisman & Hidayati, 2015).

1. Algoritma simetris, menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Contoh algoritma kunci simetris adalah *Data Encryption Standard*

(DES), *Advance Encryption Standard* (AES), *International Data Encryption Algorithm* (IDEA), A5, RC4.

2. Algoritma asimetris, merupakan sepasang kunci untuk melakukan kriptografi. Kunci yang digunakan untuk melakukan proses enkripsi berbeda dengan kunci yang dilakukan untuk melakukan proses dekripsi. Contoh algoritma kunci asimetris adalah *Elliptical Curve Cryptography* (ECC), RSA.
3. Algoritma hibrida, memanfaatkan dua tingkatan kunci, yaitu kunci simetri atau kunci sesi (*session key*) untuk enkripsi data dan pasangan kunci rahasia dengan kunci publik untuk pemberian tanda tangan digital dan melindungi kunci simetri. Contoh dari algortima hibrida adalah *Cipher* aliran (*Stream Cipher*) dan *Cipher* blok (*Block Cipher*).

2.3.1 Kriptografi Kurva Eliptik

Kriptografi kurva eliptik merupakan algoritma kriptografi asimetris yang memanfaatkan persamaan kurva eliptik (Sibarani, dkk., 2017). Kurva elips yang digunakan merupakan kurva pada medan terbatas prima (Fp) (Arya, dkk., 2015). Kurva elips pada struktur Matematika didapatkan dari persamaan $y^2 = x^3 + ax + b$ (Padma, dkk., 2010).

Dalam menentukan kurva, terdapat suatu parameter yang mempengaruhi kekuatan kriptografi pada medan prima sebagai berikut (Standard for Efficient Cryptography (SEC), 2000).

Tabel 2.1 Tabel Domain Parameter

Parameter	Keterangan
p	Bilangan prima sebagai batas medan kurva
a, b	Koefisien persamaan kurva
P	Titik pada kurva
n	Titik nol atau titik tak hingga
h	Jumlah titik pada kurva

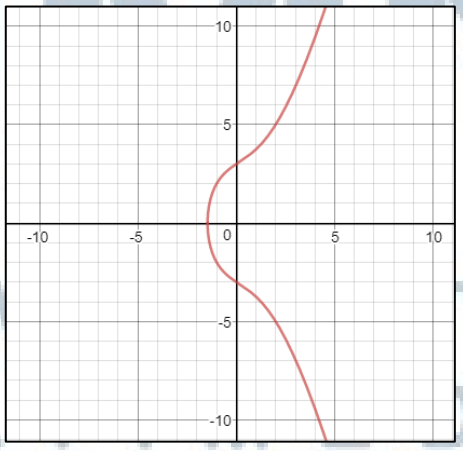
Bilangan prima (p) yang digunakan harus lebih besar dari tiga. Nilai a, b merupakan bilangan acak yang merupakan anggota himpunan bilangan prima $Fp = \{0, 1, 2, 3, \dots, p-1\}$. Nilai a, b juga harus memenuhi syarat Pertidaksamaan 2.1 (Romadhoni, dkk., 2014).

$$\boldsymbol{4a^3 + 27b^2 \neq 0 \ (mod\ p)} \quad \dots(2.1)$$

Untuk menentukan grup titik-titik yang membentuk kurva eliptik, terlebih dulu mencari *quadratic residue module* (QR_p) sebagai koordinat y dari hasil Rumus 2.2 untuk setiap anggota himpunan F_p (Sembiring, 2015).

$$\boldsymbol{y^2 \ (mod\ p)} \quad \dots(2.2)$$

Berikut adalah contoh untuk menentukan sebaran titik pada kurva elips dengan $\boldsymbol{p = 13}$, $\boldsymbol{a = 4}$, dan $\boldsymbol{b = 9}$.



Gambar 2.3 Kurva Eliptik untuk a=4, b=9 (Sembiring, 2015)

Gambar 2.3 merupakan gambar kurva elips dari persamaan $y^2 = x^3 + 4x + 9$, yang belum dibatasi oleh medan prima.

Tabel 2.2 Hasil Quadratic Residue Module

$y \in Fp$	$y^2 (mod\ p)$
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

Setelah mendapatkan hasil *quadratic residue*, kemudian dapat dicari grup titik-titik yang menentukan kurva eliptik untuk setiap $x \in F_p$ dengan Rumus 2.3 (Sembiring, 2015).

$$\boldsymbol{y^2 = x^3 + ax + b\ (mod\ p)} \qquad \text{...(2.3)}$$

Jika hasil y^2 memenuhi $y^2 \in QR_p$ maka x merupakan titik dalam kurva berpasangan dengan y himpunan F_p yang menghasilkan nilai QR_p ditambah 1 titik *infinity* dengan koordinat (∞, ∞).

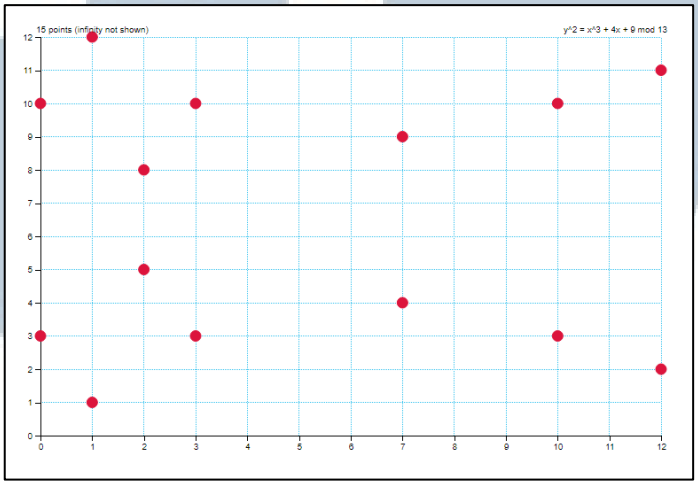
Tabel 2.3 Hasil Persamaan Kurva Eliptik

$x \in Fp$	$y^2 = x^3 + 4x + 9\ (mod 13)$	Titik kurva
0	9	(0, 1) dan (0, 10)
1	1	(1, 1) dan (1, 12)
2	12	(2, 5) dan (2, 8)
3	9	(3, 3) dan (3, 10)
4	11	-
5	11	-
6	2	-
7	3	(7, 4) dan (7, 9)
8	7	-
9	7	-

Tabel 2.3 Hasil Persamaan Kurva Eliptik (Lanjutan)

$x \in Fp$	$y^2 = x^3 + 4x + 9\ (mod 13)$	Titik kurva
10	9	(10, 3) dan (10, 10)
11	6	-
12	4	(12, 2) dan (12, 11)

Setelah didapatkan titik-titik, maka dapat digambarkan sebaran titik yang akan digunakan seperti pada Gambar 2.4. Jumlah titik yang didapatkan adalah 15 titik, 14 merupakan pasangan titik dan 1 titik *infinity*.



Gambar 2.4 Sebaran titik pada kurva dengan a = 4, b = 9, dan p = 13 (Sembiring, 2015)

Untuk setiap titik pada kurva mewakili setiap karakter yang akan dienkripsi. Kunci privat merupakan sebuah bilangan (d) yang dipilih dari anggota himpunan bilangan bulat $\{1, 2, \dots, p-1\}$. Kunci publik merupakan hasil kali d dengan titik (P) yang dipilih secara acak (Mohanta, 2014).

Proses enkripsi dan dekripsi dilakukan dengan menggunakan operasi aljabar yakni penjumlahan titik dan penggandaan titik, perhitungan dapat dilakukan menggunakan rumus sebagai berikut (Mohanta, 2014).

a. Penjumlahan titik

Jika diketahui titik $P(x_1, y_1)$ dan $Q(x_2, y_2)$, dimana $P \neq Q$, maka untuk mencari titik x digunakan Rumus 2.4

$$\boldsymbol{x_3 = [\lambda^2 - x_1 - x_2]\ mod\ p} \quad \ldots(2.4)$$

sedangkan untuk mencari titik y digunakan Rumus 2.5

$$\boldsymbol{y_3 = [\lambda(x_1 - x_3) - y_1]\ mod\ p} \quad \ldots(2.5)$$

dimana $\lambda = \left[\frac{y_2 - y_1}{x_2 - x_1}\right] mod\ p$

b. Penggandaan titik

Jika diketahui titik $P(x_1, y_1)$ dan $Q(x_2, y_2)$, dimana $P = Q$, maka untuk mencari titik x digunakan Rumus 2.6

$$\boldsymbol{x_3 = [\lambda^2 - x_1 - x_2]\ mod\ p} \quad \ldots(2.6)$$

dan untuk titik y digunakan Rumus 2.7

$$\boldsymbol{y_3 = [\lambda(x_1 - x_3) - y_1]\ mod\ p} \quad \ldots(2.7)$$

dimana $\lambda = \left[\frac{3{x_1}^2 + a}{2y_1}\right] mod\ p$

c. Perkalian titik

Operasi perkalian pada titik kurva menerapkan operasi penjumlahan yang berulang. Misalkan ada sebuah titik Q dikalikan dengan bilangan b maka, $bQ = Q + Q +$ ... sebanyak b kali.

d. Pengurangan titik

Operasi pengurangan dua titik dilakukan dengan cara menjumlahkan satu titik dengan nilai negatif dari titik lainnya. Jika diketahui titik $P(x_1, y_1)$ dan $Q(x_2, y_2)$. Titik $R(x_3, y_3)$ adalah hasil dari pengurangan $P - Q$, maka dapat dilakukan operasi $P + (-Q)$, dimana untuk setiap titik Q pada kurva memenuhi sifat $-Q(x_2, y_2) = Q(x_2, -y_2)$.

Untuk proses enkripsi, dibutuhkan sebuah bilangan k yang merupakan anggota himpunan bilangan bulat positif $\{1, 2, \ldots, p - 1\}$ yang dipilih secara acak,

$e1$ dan $e2$ yang merupakan titik dalam kurva. $e1$ dipilih secara acak dan $e2$ merupakan hasil kali dari $e1$ dengan d. Tiap titik yang merepresentasikan tiap karakter akan menghasilkan dua *cipher text* yaitu $c1$ dan $c2$ yang dapat dicari menggunakan Rumus 2.8

$$\boldsymbol{c1 = e1 \times k} \quad \ldots(2.8)$$

sedangkan untuk $c2$ dapat dicari menggunakan Rumus 2.9

$$\boldsymbol{c2 = P + e2 \times k} \quad \ldots(2.9)$$

Sehingga nantinya setiap karakter akan menghasilkan keluaran berupa teks $c1c2$ sebagai hasil enkripsi.

Untuk proses dekripsi, karakter asli (M) dapat diambil dengan melakukan pengurangan $c2$ terhadap hasil kali $c1$ dengan *private key* (d) yang telah ditentukan sebelumnya.

$$\boldsymbol{M = c2 - d \times c1} \quad \ldots(2.10)$$

2.4 Steganografi

Berbeda dari kriptografi yang merupakan ilmu untuk mengubah data sehingga tidak dipahami orang lain, steganografi berfokus pada keberadaan data rahasia tersebut, agar tidak disadari oleh orang lain. Penggunaan kriptografi dapat menimbulkan kecurigaan, oleh karena itu kecurigaan tersebut dapat dihilangkan dengan steganografi, sehingga orang lain tidak sadar akan keberadaan data rahasia (Ahmed & Khalifa, 2014).

Steganografi merupakan suatu teknik untuk memasukkan informasi rahasia ke dalam suatu media. Steganografi dapat digabungkan dengan kriptografi untuk menghasilkan suatu perlindungan yang lebih baik lagi bagi informasi tersebut.

Penyembunyian data menggunakan steganografi harus memperhatikan kriteria-kriteria sebagai berikut (Wijaya, dkk., 2012).

1. Ketepatan

   Media yang digunakan untuk menampung pesan rahasia tersebut, tidak boleh berbeda jauh dari kualitas aslinya. Perubahan yang terlalu mencolok dapat menimbulkan kecurigaan dari orang lain. Perubahan yang terjadi pada media penampung harus seminim mungkin agar tidak dapat dideteksi oleh indera manusia.

2. Ketahanan

   Data yang disembunyikan tidak boleh rusak saat terjadi perubahan pada media penampung.

3. Pemulihan

   Data yang telah disembunyikan, harus dapat dikembalikan ke data awal tanpa perubahan atau kerusakan.

Dilihat dari objek penampungnya, steganografi memiliki beberapa tipe yaitu *audio steganography*, *video steganography*, dan *image steganography*. Steganografi menggunakan gambar merupakan steganografi paling popular karena penyebaran gambar yang mudah melalui internet (Ahmed & Khalifa, 2014).

2.4.1 Least Significant Bit

Inti dari teknik Least Significant Bit adalah untuk menanamkan *bit* data rahasia ke nilai *bit* terkecil dari gambar yang dijadikan sebagai *cover image*. Perubahan pada *bit* terkecil tidak akan tampak oleh indra manusia karena perubahan yang dihasilkan kecil (Zin, 2013).

Untuk menyisipkan data pada gambar, dibutuhkan gambar yang layak. Teknik ini membutuhkan *bit* tiap *pixel* yang ada pada gambar, oleh karena itu gambar dengan kompresi *lossless* dibutuhkan, karena jika tidak, data yang disisipkan dapat rusak atau hilang saat dilakukan perubahan oleh algoritma (Zin, 2013).

Untuk melakukan steganografi, diperlukan *binary* dari *cover image* dan pesan yang ingin disembunyikan. Jika sebuah *image* 24-*bit color* memiliki resolusi 800×600 *pixel* dan tiap *pixel* dapat menyimpan 3-*bit* data maka total data yang dapat disembunyikan maksimal 800×600×3 = 1.440.000-*bit* atau 180.000 *bytes*.

Berikut adalah contoh penyisipan karakter pada 3 *pixel* dari gambar 24-*bit color* seperti pada Gambar 2.5.

00100111	11101001	11001000
00100111	11001000	11101000
11001000	00100111	11101001

Gambar 2.5 Contoh 3 *pixel* dari Gambar 24-*bit* color

Sebuah pesan yang ingin disisipkan, misal berupa karakter “A” dengan nilai biner 01000001, maka gambar yang baru akan memiliki nilai biner seperti Gambar 2.6.

00100110	11101001	11001000
00100110	11001000	11101000
11001000	00100111	11101001

Gambar 2.6 Hasil Penyisipan Karakter "A"

Dari Gambar 2.6 dapat dilihat bahwa perubahan pada gambar setelah menyisipkan karakter “A” hanya berubah dua *bit* saja. Perubahan dua *bit* dari total 24-*bit* tidak akan tampak jika dilihat menggunakan indra manusia. Lalu, untuk

mendapatkan kembali pesan yang disembunyikan, dapat dilakukan dengan mengekstrak *bit* terakhir dari masing-masing *pixel* secara berurutan (Irfan, 2013).

2.4.2 Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR) merupakan nilai yang digunakan untuk menentukan kualitas gambar setelah mengalami reskonstruksi (Munandar, dkk., 2011). PSNR biasa diukur dalam satuan *decibels* (dB). Nilai PSNR pada umumnya berkisar antara 20 dB hingga 40 dB (Saffor, dkk., 2001). Sebuah gambar yang sudah direkontruksi dikatakan memiliki kualitas tinggi jika memiliki nilai PSNR di atas 40 dB (Cheddad, dkk., 2010).

Untuk melakukan perhitungan PSNR, diperlukan nilai *Mean Squared Error* (MSE). Nilai PSNR digunakan untuk menentukan tingkat kemiripan dari dua gambar, sedangkan nilai MSE digunakan untuk mengukur perbedaan dari dua gambar (Almohammad & Ghinea, 2010).

Rumus yang digunakan untuk melakukan perhitungan adalah sebagai berikut (Almohammad & Ghinea, 2010).

$$\boldsymbol{MSE = \left(\frac{1}{MN}\right)\sum_{i=1}^{M}\sum_{j=1}^{N}\left(X_{ij} - \overline{X_{ij}}\right)^2} \quad \ldots(2.11)$$

Setelah mendapatkan nilai MSE maka, dapat dihitung nilai PSNR menggunakan rumus (Almohammad & Ghinea, 2010).

$$\boldsymbol{PSNR = 10.\log_{10}\frac{I^2}{MSE}\ db} \quad \ldots(2.12)$$

dimana:

M, N adalah tinggi dan lebar dari *image*,

X_{ij} adalah *pixel* baris ke-i dan kolom ke-j pada *image* asli,

$\overline{X_{ij}}$ adalah *pixel* baru ke-i dan kolom ke -j pada *stego-image*,

I adalah nilai maksimal yang dapat diterima oleh satu *pixel* (Almohammad & Ghinea, 2010).

Aplikasi PSNR 1.2 merupakan aplikasi untuk menghitung nilai PSNR dari dua gambar. Nilai PSNR akan muncul jika kedua gambar memiliki resolusi yang sama. Aplikasi ini dibuat oleh Pascal Bertolino, profesor universitas Grenoble departemen *Images and Signal*.

2.5 Portable Network Graphics

Media gambar dengan format *portable network graphics* (PNG) sudah sering digunakan oleh masyarakat luas, sehingga penggunaan gambar PNG untuk dijadikan tempat persembunyian bagi data rahasia tidak akan menimbulkan kecurigaan (Reddy, dkk., 2011). Kompresi format PNG juga merupakan yang terbaik karena dapat dilakukan tanpa kehilangan data gambar (*lossless compression).* Sejak 1995, format PNG sudah didukung oleh banyak *web browser* (Roelofs, 1999).

Sifat *lossless compression* yang dimiliki oleh format PNG membuat format ini dapat dijadikan alternatif dalam melakukan pengolahan citra. Format PNG tidak akan kehilangan bagian citranya dan juga tidak menurun kualitas gambarnya (Sari, dkk., 2012).

Dilihat dari sudut pandang steganografi, gambar dengan format PNG merupakan citra yang paling cocok untuk digunakan karena format PNG memiliki kemampuan untuk menyembunyikan informasi dalam jumlah banyak (Alqahtani, dkk., 2016).

Tidak seperti format *joint photographic expert group* (JPEG) yang meskipun memiliki resolusi gambar yang tinggi, namun masih bersifat *lossy compression*. Sifat tersebut membuat gambar akan kehilangan kualitasnya saat dilakukan kompresi, bahkan dapat kehilangan integritas gambarnya (Sinha, 2015).

Dibandingkan dengan format gambar lainnya seperti JPEG, GIF, dan TIFF, PNG memiliki kelebihan yang lebih baik. Seperti yang dapat dilihat pada Tabel 2.4 bahwa PNG memiliki kelebihan yang dimiliki oleh format lainnya (Alqahtani, dkk., 2016).

Tabel 2.4 Perbandingan Format Gambar (Alqahtani, dkk., 2016)

	JPEG	TIFF	GIF	PNG
Transparency			✓	✓
Palette Image		✓	✓	✓
Truecolor	✓	✓		✓
Best Compression				✓
Web Supporting	✓		✓	✓
Animation			✓	

2.6 Uji Korelasi

Korelasi adalah teknik statistik yang digunakan untuk menguji ada atau tidaknya hubungan dari dua variabel atau lebih. Nilai korelasi berkisar antara -1 hingga 1. Jika hasil uji menunjukkan nilai antara 0 hingga 1, maka variabel uji memiliki arah hubungan yang positif. Jika hasil uji menghasilkan nilai antara -1 hingga 0, maka variabel uji memiliki arah hubungan yang negative. Jika hasil uji menghasilkan nilai tepat 0, maka kedua variabel tidak memiliki hubungan (Hidayat, 2012).

Rumus perhitungan untuk melakukan uji korelasi adalah sebagai beirkut (Kho, 2017).

$$r_{xy} = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{n(\sum x^2) - (\sum x)^2} \times \sqrt{n(\sum y^2) - (\sum y)^2}} \quad \ldots(2.\ 13)$$

dimana,

n = banyaknya pasangan variabel

Σx = jumlah dari variabel x

Σy = jumlah dari variabel y

Σx^2 = jumlah kuadrat dari variabel x

Σy^2 = jumlah kuadrat dari variabel x

Σxy = jumlah perkalian dari variabel x dan y

Korelasi positif menunjukkan bahwa perubahan nilai suatu variabel diikuti perubahan nilai variabel yang lain secara teratur kea rah yang sama. Korelasi negatif menunjukkan bahwa perubahan satu nilai variabel diikuti dengan perubahan nilai variabel yang lain dengan arah yang berlawanan. Sedangkan untuk variabel yang tidak memiliki hubungan korelasi, perubahan suatu variabel terkadang mempengaruhi nilai variabel yang lainnya dengan arah yang serah atau berlawanan (Kho, 2017).