BAB II
TINJAUAN PUSTAKA

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu dari dua suku kata *Crypto* dan *Graphia*. *Crypt* artinya menyembunyikan, sedangkan graphia artinya ilmu. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data, yang dilakukan oleh seorang Kriptographer. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1) Kerahasiaan (*Confidentiality*)
2) Integritas Data (*Data Integrity*)
3) Otentikasi (*Autentication*)
4) Ketiadaan Peyangkalan (*Nonrepudiation*)

Kriptografi sebagai bidang ilmu tentu saja memiliki beberapa istilah tersendiri yang harus diketahui, beberapa istilah yang sering digunakan dalam kriptografi adalah :

1) *Plaintext* : *Plaintext* merupakan pesan asli yang ingin dikirimkan dan dijaga keamananya. Pesan ini tidak lain dari informasi tersebut.
2) *Ciphertext* : *Ciphertext* merupakan pesan yang telah dikodekan (disandikan).
3) *Cipher* : *Cipher* merupakan algoritma matematis yang digunakan untuk proses peyandian plaintextmenjadi *ciphertext*.
4) Enkripsi : Enkripsi (*encryption*) merupakan proses yang dilakukan untuk meyandikan *plaintext* sehingga menjadi *ciphertext*.
5) Dekripsi : Dekripsi (decryption) merupakan proses yang dilakukan untuk memperoleh kembali *plaintext* dari *ciphertext*.
6) Kriptanalisis : Ilmu dan seni untuk membuka suatu *chipertext* secara ilegal.
7) Kriptografi : Ilmu matematika yang mendasari ilmu kriptografi dan kriptanalisis.

Keamanan adalah keadaan bebas dari bahaya. Istilah ini dapat digunakan

dengan hubungan kepada kejahatan, dan segala bentuk kecelakaan. Keamanan merupakan topik yang luas termasuk keamanan nasional terhadap seorang teroris, keamanan komputer terhadap *hacker*, keamanan rumah terhadap maling dan penyusup lainnya, keamanan *financial* terhadap kehancuran ekonomi dan banyak situasi berhubungan lainnya. *Host* Kompuer yang terhubung ke *network*, mempunyai ancaman keamanan lebih besar daripada *host* yang tidak berhubungan kemana-mana. Dengan mengendalikan *network security* resiko tersebut dapat dikurangi. (Santoso & Fakhriza, 2018)

Algoritma kriptografi adalah fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Algoritma kriptografi semakin kuat jika waktu untuk proses pemecahan sandi semakin lama. Dengan begitu algoritma tersebut semakin aman untuk digunakan. Untuk mengenkripsi dan mendekripsi data kriptografi menggunakan suatu algoritma (*cipher*) dan kunci (*key*). Algoritma kriptografi modern tidak lagi mengandalkan keamannya pada kerahasian algoritma tetapi kerahasiaan kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula. Dengan demikian algoritma kriptografi dapat bersifat umum dan boleh diketahui siapa saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat dipecahkan. Sistem kriptografi adalah sebuah kunci algoritma kriptografi ditambah semua kemungkinan *plaintext*, *ciphertext* dan kunci. (Megantara & Rafrastara, 2019)

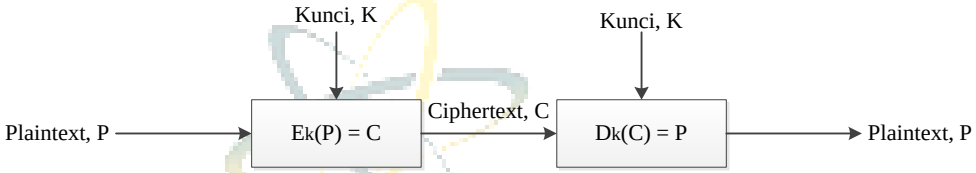
2.1.1 Jenis Kriptografi

Algoritma kriptografi terbagi menjadi dua jenis berdasarkan kunci yang digunakan, yaitu Algoritma Simetri dan Algoritma Asimetri.

1. Algoritma Simetri

   Sistem kriptografi kunci simetri disingkat menjadi “kunci simetri”, mengasumsikan pengirim dan penerima pesan sudah menerima kunci yang sama sebelum bertukar pesan. Keamanan algoritma kriptografi simetri terletak pada kerahasiaan kuncinya. Biasanya, cipher yang termasuk kriptografi simetri diproses dalam mode blok (block cipher), yaitu setiap

kali proses enkripsi/dekripsi dilakukan pada satu blok data, atau diproses dalam aliran penyandian (stream cipher), yaitu pada setiap proses enkripsi/dekripsi dilakukan terhadap satu bit atau byte data. Pada aplikasi kriptografi simetri yang menjadi utama adalah melindungi kerahasiaan data yang dikirim melalui saluran yang tidak aman dan melindungi kerahasiaan data yang disimpan pada media penyimpanan yang tidak aman. Skema proses dari kriptografi simetri dapat dilihat pada Gambar 2.1. (Basim & Painem, 2020)

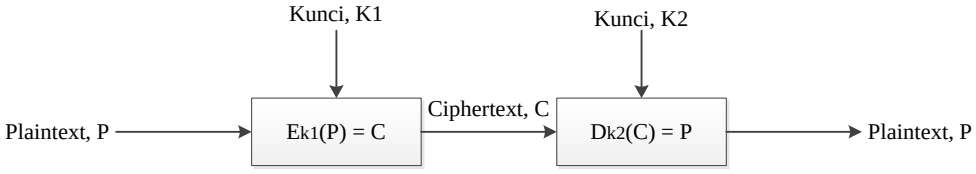


Gambar 2.1. Algoritma Kriptografi Simetri
(Sumber : Basim & Painem, 2020)

Beberapa contoh dari algoritma simetri adalah Data Encryption Standard (DES), Advance Encryption System (AES), International Data Encryption Algorithm (IDEA) dan RC4.

2. Algoritma Asimetri

Pada kriptografi asimetri, kunci/key untuk enkripsi bersifat tidak rahasia dan dapat diketahui/digunakan oleh siapapun (publik), sementara kunci/key untuk dekripsi bersifat rahasia/privasi yang hanya diketahui oleh penerima pesan. Pada kriptografi asimetri, setiap orang yang menggunakan aplikasi mempunyai sepasang kunci, yaitu kunci rahasia dan kunci publik. Pengirim men-enkripsi pesan dengan menggunakan kunci publik si penerima pesan (receiver). Hanya penerima pesan yang dapat men-dekripsi pesan karena hanya ia yang mengetahui kunci rahasianya sendiri. Skema kriptografi dapat dilihat pada Gambar 2.2. (Basim & Painem, 2020)



Gambar 2.2. Algoritma Kriptografi Asimetri
(Sumber : Basim & Painem, 2020)

Beberapa contoh dari algoritma simetri adalah Rivest Shamir Adleman (RSA), Diffie Hellman, Digital Secure Algorithm (DSA), XTR, Elliptic Curve Cryptography (ECC), dan Elgamal Encryption System (ESS).

2.1.2 Komponen Kriptografi

Didalam kriptografi terdiri dari komponen yang disebut plainteks, cipherteks, kunci dan algoritma. Plaintext (plainteks), yaitu informasi awal sebelum pesan dikirim, sehingga pesan ini masih dapat dibaca dan pahami maksud dan tujuannya. Ciphertext (cipherteks), yaitu pesan tersandikan, dimana pesan ini tidak lagi dapat dipahami isi dan maksudnya. Key (kunci), yaitu sebuah parameter untuk proses enkripsi dan dekripsi. Algorithm (algoritma), yaitu cara yang digunakan untuk proses enkripsi dan dekripsi. Istilah pemrosesan kriptografi disebut enkripsi dan dekripsi.

1. Encryption (enkripsi) yaitu cara merubah pesan yang dapat dibaca (plainteks) menjadi pesan yang tidak dapat dibaca. Hasil dari proses ini disebut ciphertext(cipherteks).
2. Decryption (dekripsi) yaitu proses mengembalikan pesan tidak bisa dibaca (ciphtertext) menjadi bisa terbaca (plaintext). (Syaifuddin et al., 2021)

2.2 Algoritma RSA

Dari sekian banyak algoritma kriptografi kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar. Oleh karena alasan tersebut RSA dianggap aman. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu : Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Kekuatan algoritma RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor bilangan primanya, sehingga semakin besar bilangan prima yang digunakan semakin baik atau aman. Dalam kriptografi menggunakan algoritma RSA terdapat tiga proses yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi, dan proses dekripsi

Adapun langkah-langkah pada proses pembangkitan kunci publik dan kunci privat pada algoritma RSA adalah sebagai berikut :

1. Pilih 2 bilangan prima yang berbeda p dan q secara acak dan p ≠ q, semakin besar semakin baik. Kedua bilangan prima ini, p dan q bersifat rahasia.
2. Hitung n = p * q dimana nilai n digunakan untuk modulus pada kunci publik dan kunci privat. Nilai n tidak rahasia, orang lain dapat mengetahuinya.
3. Hitung φ(n) = (p – 1) * (q – 1) digunakan untuk pencarian kunci privat. Nilai φ(n) bersifat rahasia.
4. Hitung nilai e dengan cara memilih bilangan bulat sedemikian rupa sehingga 1 < e < φ(n) dan GCD(φ(n), e) = 1, nilai e bersifat tidak rahasia.
5. Pilih nilai d yang merupakan bilangan bulat dengan syarat nilai d memenuhi (d * e) mod φ(n) = 1 atau d = (1 + k * φ(n)) / e, nilai k dapat dihitung dengan cara mencoba nilai-nilai sehingga diperoleh nilai bilangan d adalah bilangan bulat. Nilai d bersifat rahasia.

Maka hasil dari algoritma tersebut dapat disederhanakan menjadi beberapa bagian rumus yaitu :

Kunci Publik : $e = relative\ prima\ (p-1)(q-1)$

Kunci Privat : $d = (1 + k\ \emptyset\ (n))/e$

Enkripsi : $C = Pe\ mod\ n$

Dekripsi : $P = Cd\ mod\ n$ (Andika, 2021)

Proses Enkripsi dengan menggunakan Algoritma RSA Enkripsi Metode RSA :

Kunci PRIVATE (e,n) = (23, 184)

Kunci PUBLIC (d,n) = (23, 184)

Plainteks = jakarta

Rubah plainteks menjadi “jakarta” ke bilang ASCII decimal. Adapun nilainya menjadi sebagai berikut :

(j=106) (a=97) (k=107) (a=97) (r=114) (t=116) (a=97)

Susun plainteks menjadi blok-blok p1 , p2 , …, (nilai setiap blok di dalam bentuk [0, p – 1].

P1 = 106

P2 = 97

P3 = 107

P4 = 97

P5 = 114

P6 = 116

P7 = 97

Adapun rumus enkripsi algoritma RSA yaitu :

$C = pe\ Mod\ n$

Enkripsi P1 = 106

$C1$ = $106^{23}\ Mod\ 184$

$106^{23}\ phi\ (184)\ Mod\ 184$

$106^{23}\ (Mod\ 21)\ Mod\ 184$

$(23\ Mod\ 21 = 3)\ Mod\ 184$

$C1$ = $106^{2}\ Mod\ 184$

= $11.236\ Mod\ 184$

$C1$ = 12

Enkripsi P2 = 97

$C2$ = $97^{23}\ Mod\ 184$

$97^{23}\ phi\ (184)\ Mod\ 184$

$97^{23}\ (Mod\ 21)\ Mod\ 184$

$(23\ Mod\ 21 = 3)\ Mod\ 184$

$C2$ = $97^{2}\ Mod\ 184$

= $9.409\ Mod\ 184$

$C2$ = 25

Enkripsi P3 = 107

$C3$ = $107^{23}\ Mod\ 184$

$107^{23}\ ph(184)\ Mod\ 184$

$107^{23}\ (Mod\ 21)\ Mod\ 184$

$(23\ Mod\ 21 = 3)\ Mod\ 184$

$C3$ = $107^{2}\ Mod\ 184$

= $11.449\ Mod\ 184$

$C3$ = 41

Enkripsi P4 = 97

$C4$ = 97^{23} Mod 184

97^{23} phi (184) Mod 184

(23 Mod 21 = 3) Mod 184

$C4$ = 97^{2} Mod 184

= 9.409 Mod 184

$C4$ = 25

Enkripsi P5 = 114

$C5$ = 114^{23} Mod 184

114^{23} phi (184) Mod 184

(23 Mod 21 = 3) Mod 184

$C5$ = 114^{2} Mod 184

= 12.996 Mod 184

$C5$ = 116

Enkripsi P6 = 116

$C6$ = 116^{23} Mod 184

116^{23} phi (184) Mod 184

(23 Mod 21 = 3) Mod 184

$C6$ = 116^{2} Mod 184

= 13.456 Mod 184

$C6$ = 24

Enkripsi P7 = 97

$C7$ = 97^{23} Mod 184

97^{23} phi (184) Mod 184

(23 Mod 21 = 3) Mod 184

$C7$ = 97^{2} Mod 184

= 9.409 Mod 184

$C7$ = 25

Sehingga dapat dihasilkan hasil Enkripsi dari sample data diatas adalah :

12, 25, 41, 25, 116, 24, 25

Selanjutnya merubah hasil Enkripsi kebilangan ASCII. Adapun nilainya sebagai berikut : FFEM)EMtCANEM. (Andika, 2021)

2.3 Steganografi

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Pengertian lain dari steganografi adalah ilmu, teknik atau seni menyembunyikan pesan rahasia (hidding message) atau tulisan rahasia (covered writing), menjadikan pesan tersebut tidak terbaca orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi awalnya dari bahasa Yunani yakni "steganos" yang artinya tersembunyi/menyembunyikan dan "graphy" yang artinya tulisan yang secara lengkap memiliki arti tulisan yang disembunyikan. Dalam buku Histories of Herodatus Steganografi dengan media kepala budak yaitu dengan cara kepala budak dibotaki kemudian ditulisi pesan dan rambut budak tersebut dibiarkan tumbuh selanjutnya budak baru dikirim. Ditempat penerima kepala budak pembawa pesan tersebut digundul supaya pesan dapat terbaca. Pemakaian tinta tak-tampak (*invisible ink*), tinta dibuat dari campuraan sari buah, susu dan cuka. Tulisan diatas kertas bisa dibaca dengan memanaskan kertas tersebut. (Nur'aini, 2019)

Pada perang dunia II adalah periode pengembangan teknik-teknik baru steganogafi. Pada awal Perang Dunia II walaupun masih digunakan teknik tinta yang tak terlihat, namun teknik-teknik baru mulai dikembangkan seperti menulis pesan rahasia ke dalam kalimat lain yang tidak berhubungan langsung dengan isi pesan rahasia tersebut, kemudian teknik menulis pesan rahasia ke dalam pita koreksi karbon mesin ketik, dan juga teknik menggunakan pin berlubang untuk menandai kalimat terpilih yang digunakan dalan pesan, teknik terakhir adalah microdots yang dikembangkan oleh tentara Jerman pada akhir Perang Dunia II. Dari contoh-contoh steganografi konvensional tesebut dapat dilihat bahwa semua teknik steganografi konvensional berusaha merahasiakan komunikasi dengan cara menyembunyikan pesan ataupun mengkamuflase pesan. Maka sesungguhnya prinsip dasar dalam steganogafi lebih dikonsentrasikan pada kerahasiaan komunikasinya bukan pada datanya.

Cara kerja atau prinsip dari steganografi adalah dengan menggunakan dua unsur untuk menyisipkan suatu pesan atau data yang ingin disembunyikan. Unsur pertama adalah media penampung seperti citra, suara, video, dan lain sebagainya

yang tidak membuat curiga bahwa ada pesan rahasia dalam media tersebut. Unsur kedua adalah pesan yang hendak disembunyikan. (Nur'aini, 2019)

2.3.1 Penggunaan Steganografi

Steganografi sebagai suatu teknik penyembunyian informasi pada data digital lainnya dapat dimanfaatkan untuk berbagai tujuan seperti :

1) Tamper-proofing, steganografi digunakan sebagai alat untuk mengidentifikasikan atau alat indikator yang menunjukkan data host telah mengalami perubahan dari aslinya.
2) Feature location, steganografi digunakan sebagai alat untuk mengidentifikasikan isi dari data digital pada lokasi-lokasi tertentu, seperti contohnya penamaan objek tertentu dari beberapa objek yang lain pada suatu citra digital.
3) Annotation/caption Steganografi hanya digunakan sebagai keterangan tentang data digital itu sendiri.
4) Copyright-Labeling Steganografi dapat digunakan sebagai metoda untuk penyembunyian label hak cipta pada data digital sebagai bukti otentik kepemilikan karya digital tersebut. (Alam, 2018)

2.3.2 Kriteria Steganografi

Penyembunyian data rahasia ke dalam media cover akan mengubah kualitas media tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data diantaranya adalah:

1) *Fidelity*, kualitas berkas *cover* tidak jauh berubah setelah penyisipan data rahasia. berkas *cover* hasil steganografi masih terlihat/terdengar dengan baik. Pengamat tidak mengetahui kalau di dalam berkas tersebut terdapat data rahasia.
2) *Recovery*, data yang disembunyikan harus dapat diungkapkan/diekstrak kembali. Karena tujuan steganografi adalah penyembunyian informasi, maka sewaktu-waktu informasi di dalam berkas *cover* harus dapat diambil kembali untuk digunakan lebih lanjut.
3) *Robustness*, *robustness* merupakan salah satu isu desain algoritma steganografi yang utama. Data rahasia yang disisipkan harus tahan

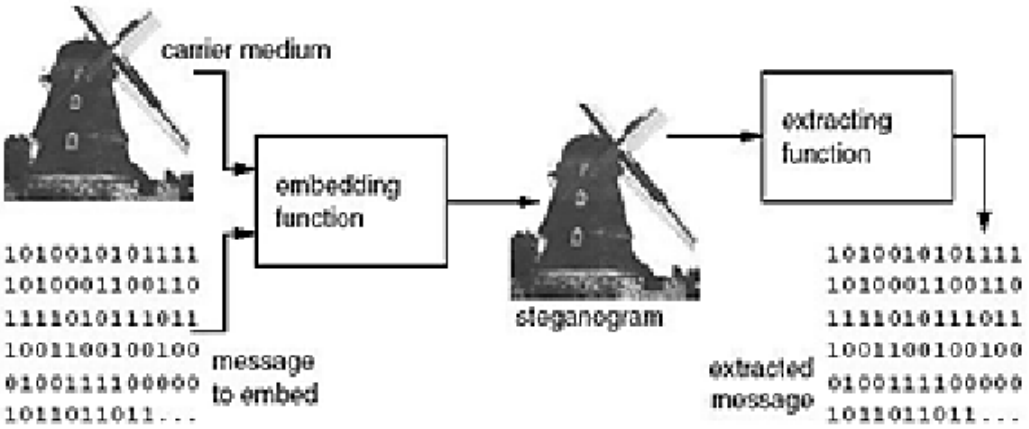
terhadap pengolahan sinyal yang mungkin dilakukan termasuk konversi *digital-analog* dan *analog-digital*, *linear* dan *non-linear filtering*, kompresi dan perubahan ukuran (*scaling*).

4) *Security*, data rahasia harus kebal terhadap deteksi pembajakan dan juga diharapkan bisa menyulitkan dari usaha *steganalisis*. (Malese, 2021)

2.4 Algoritma LSB 2 Bit

LSB (Least Significant Bit) 2-bit mengacu pada penggantian atau manipulasi dua bit terakhir dalam representasi biner suatu angka. Dalam sistem biner, setiap angka direpresentasikan oleh serangkaian bit (0 atau 1). Bit terakhir dalam representasi biner disebut sebagai LSB, sedangkan bit terakhir sebelumnya disebut sebagai bit kedua terakhir. Manipulasi LSB 2-bit melibatkan mengubah atau memanipulasi bit-bit ini untuk menghasilkan angka yang berbeda. Misalnya, jika kita ingin mengubah angka biner 0110 menjadi 0101 menggunakan LSB 2-bit, kita akan mengganti bit terakhir menjadi 0 dan bit kedua terakhir menjadi 1. Penggunaan LSB 2-bit dapat diterapkan dalam berbagai konteks, seperti steganografi (penyembunyian pesan rahasia dalam gambar atau file lainnya), enkripsi dan dekripsi data, atau dalam algoritma pemrosesan sinyal digital. Dalam konteks ini, LSB 2-bit sering digunakan sebagai metode untuk menyisipkan atau mengekstrak informasi tambahan dalam bit-bit terakhir suatu data, dengan tujuan pengamanan atau penyembunyian.

Pengubahan *Least Significant Bit* (LSB) pada citra/gambar yang terkompresi sangat sulit diketahui secara kasat mata, sehingga metode ini termasuk kategori sangat baik dan banyak digunakan. Metode ini memanfaatkan ketidakmampuan indera penglihatan manusia dalam menemukan perbedaan antara gambar yang asli dengan gambar yang sudah dimasukkan/disisipkan pesan rahasia. Pada Gambar 2.1 ditunjukan bahwa medium pembawa yang disisipkan pesan dengan menggunakan suatu fungsi penyisipan, dalam hal ini LSB , menghasilkan *Stego-Image* yang tidak mengalami perubahan yang *significant* dari gambar aslinya.



Gambar 2.3. Penyisipan Pesan Pada Gambar

(Sumber : Rismawati, 2019)

Untuk menjelaskan metode LSB ini, maka digunakan citra digital sebagai *Image-Object*. Setiap *Pixel* pada citra digital memiliki ukuran 1 sampai 3 byte. Pada susunan bit didalam byte (1 byte = 8 bit), terdapat bit yang kurang berarti *Least Significant Bit* (LSB). Misalnya pada byte 00110011, maka bit LSB-nya adalah bit yang terletak paling kanan yaitu 1. Dengan demikian untuk melakukan penyisipan pesan terhadap citra, maka bit paling cocok untuk diubah dengan bit pesan adalah bit LSB, karena pengubahan bit pada citra/gambar hanya akan merubah nilai byte-nya menjadi satu lebih tinggi atau satu lebih rendah.

Sebagai contoh, urutan bit berikut ini menggambarkan 3 *Pixel* pada *Cover-Image* 24 bit.

(01010110 10111001 10000110)
(10001001 10001010 00010011)
(01011110 01111000 10101010)

Pesan yang akan disisipkan pada sebuah citra/gambar adalah karakter “M”, yang nilai binernya adalah 10010011, maka yang aka dihasilkan *Stego-Image* dengan urutan bit sebagai berikut :

(01010111 10111000 10000110)
(10001001 10001010 00010010)
(01011111 01111001 10101010)

Perubahan dapat dilihat pada bagian cetak tebal pada nilai biner. Perubahan yang tidak significant ini tidak dapat ditangkap oleh indera penglihatan manusia (jika media wadah berupa gambar, audio dan video). Dalam contoh diatas

penggantian pixel tak significant dilakukan secara terurut. Penggantian *pixel* tak *significant* juga bisa dilakukan secara tidak terurut, bahkan hal seperti ini bisa lebih meningkatkan keamanan sebuah data.

Pada gambar Bitmap 24-bit , tiap *pixel*-nya terdapat 24-bit kandungan warna atau 8-bit untuk masing-masing warna dasar (R, G dan B), dengan besaran nilai kandungan antara 0 (00000000) samapai dengan 255 (11111111) untuk setiap warna. perubahan LSB ini pada gambar jenis ini hanya akan merubah 1 nilai dari 256 nilai sehingga gambar hasil Steganografi akan sulit dibedakan dengan gambar aslinya.

Steganografi dengan menggunakan metode LSB hanya mampu untuk menyimpan informasi dengan ukuran yang relatif sangat terbatas. Sebagai contoh: suatu citra 24-bit (R = 8, G = 8, B = 8) digunakan sebagai tempat untuk menyimpan data berukuran 100-bit, jika masing-masing komponen warnanya (RGB) menggunakan satu *pixel* untuk menyimpan informasi/pesan rahasia tersebut, maka setiap *pixel*-nya menyimpan 3-bit informasi, dengan demikian setidaknya dibutuhkan citra/gambar wadah berukuran 34 *pixel*. Jadi suatu citra/gambar 24-bit jika digunakan untuk menyimpan/menyisipkan informasi rahasia, maka hanya dapat menampung informasi berukuran 1/8 dari ukuran citra/gambar penampung tersebut.

Kapasitas gambar maksimum pesan yang dapat ditampung adalah panjang gambar x lebar gambar x 3 bit. Sebagai contoh, Desktop umum berukuran 1024 *pixel* x 768 pixel. Jadi ukuran pesan maksimum pada gambar dengan ukuran tersebut adalah 2.359.296 bit, atau sebanyak 294.912 karakter (1 karakter = 1 byte atau 8 bit). Selanjutnya jika *file* lebih besar dari *Image* maka akan manfaatkan metode *Resize Image* dan Kompres pada *file*. Untuk menutupi kelemahan yang dimiliki oleh Metode *Least Significant Bit*. (Rismawati, 2019)

2.5 Pesan

Pesan adalah komunikasi atau informasi yang disampaikan dari satu pihak kepada pihak lain melalui berbagai media atau saluran komunikasi. Tujuan dari pesan adalah untuk menyampaikan suatu gagasan, informasi, instruksi, perasaan, atau pesan lainnya dengan harapan bahwa penerima pesan akan memahami dan

meresponsnya. Pesan bisa berbentuk lisan atau tertulis, dan dapat disampaikan melalui berbagai media, seperti percakapan langsung, telepon, surat, email, pesan teks, atau platform media sosial. Pesan juga bisa berupa gambar, grafik, atau simbol yang memiliki arti khusus dan dapat menyampaikan informasi atau pesan tertentu.

Pesan yang efektif harus jelas, ringkas, dan mudah dimengerti agar dapat mengkomunikasikan tujuannya dengan baik. Selain itu, konteks dan pemahaman budaya juga penting, terutama ketika berkomunikasi dengan orang dari latar belakang atau bahasa yang berbeda. Pesan merupakan elemen penting dalam proses komunikasi manusia dan merupakan sarana utama bagi individu atau organisasi untuk berbagi informasi, gagasan, pandangan, atau tujuan mereka dengan orang lain.

Mengingat percakapan dalam interaksi berkomunikasi mengalami perubahan dan perkembangan yang sangat signifikan, yakni dari tatap muka secara langsung dan menggunakan media daring, mengakibatkan terjadinya interaksi percakapan komunikasi yang merubah sistem percakapan dalam kehidupan manusia sehari-hari. Perubahan komunikasi dalam percakapan sehari-hari yang dipengaruhi perkembangan teknologi informasi komunikasi, tentunya sangat menarik untuk dibahas. Berdasarkan perkembangan dan kemajuan terknologi informasi dan komunikasi saat ini berkembang pesat, baik secara teori komunikasi maupun implementasinya. Perkembangan tersebut membutuhkan suatu bentuk peningkatan keamanan agar pesan yang dikirim dan diterima dapat dijaga kerahasiaannya antara pengirim dan penerima pesan. (Hidayat, 2021)

2.6 Video

Video berasal dari bahasa latin yaitu darikata vidi atau visum yang artinya melihat atau mempunyai penglihatan. Video didefinisikan sebagai media digital yang menunjukkan susunan atau urutan gambar-gambar dan memberikan ilusi, gambaran serta fantasi pada gambar bergerak. Video merupakan media penyampai pesan yang bersifat fakta maupun fiktif, inforamatife, edukatif maupun instruksional. Adapun seorang ahli mengatakan bahwa video merupakan rekaman gambar dan suara dalam kaset pita video ke dalam pita magnetik yang dapat memberikan gambaran nyata, dan mampu memanipulasi waktu dan tempat. Sedangkan video digital sebenarnya terdiri atas serangkaian gambar digital yang ditampilkan dengan cepat pada kecepatan yang konstan. Dalam konteks video, gambar ini disebut *frame*. Satuan ukuran untuk menghitung *frame* rata-rata yang ditampilkan disebut *frame per second* (FPS). Setiap *frame* merupakan gambar digital yang terdiri dari raster *pixel*.

Video adalah teknologi untuk menangkap, merekam, memproses, mentransmisikan dan menata ulang gambar bergerak. biasanya menggunakan film seluloid, sinyal elektronik atau media digital. Video juga bisa dikatakansebagai gabungan gambar-gambar mati yang dibaca berurutan dalam suatu waktu dengan kecepatan tertentu. Gambar-gambar yang digabung tersebut dinamakan frame dan kecepatan pembacaan gambar disebut dengan frame rate, dengan satu fps. Video merupakan gabungan gambar-gambar mati yang dibaca berurutan dalam satu waktu dengan kecepatan tertentu. Kata video berasal dari kata latin yang berarti “saya lihat” Video adalah teknologi pemprosesan sinyal elektronik yang mewakilkan gambar bergerak. Sehingga dapat disimpulakn video merupakan sebuah kumpulan gambar-gambar mati yang bergerak dalam suatu framedan kecepatan tertentu dalam sebuah bentuk dimensi yang berbeda. (Eko Valentino & Jodi Hardiansyah, 2020)

2.7 Android

Android merupakan sistem operasi berbasis Linux yang digunakan untuk telepon seluler (*mobile*) seperti telepon pintar (*smartphone*) dan komputer tablet (PDA). Android adalah sebuah sistem operasi untuk perangkat mobile berbasis Linux yang mencangkup sistem operasi, *middleware* dan aplikasi. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi

mereka sendiri yang akan digunakan untuk membantu kegiatan dalam berbagai bidang, sehingga bisa digunakan oleh setiap orang yang ingin menggunakannya pada perangkat mereka. Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat bergerak layar sentuh seperti telepon pintar dan komputer *tablet*. Android awalnya dikembangkan oleh Android, Inc dengan dukungan finansial Google, yang kemudian membelinya pada tahun 2005. (Khaliq, 2021)

Pada tanggal 23 september 2008, sistem operasi Android versi 1.0 resmi diluncurkan. Sekitar sebulan berikutnya, pada tanggal 22 Oktober 2008, smartphone pertama yang menjalankan Android 1.0 itu, yaitu HTC Dream, diluncurkan ke pasar. Pada tanggal 9 februari, Android versi 1.1 diluncurkan untuk memperbaiki bug dari versi sebelumnya dan menambah fitur yang tersedia. Setelah versi 1.1, rilis Android berikutnya menggunakan nama makanan manis dengan urutan alfabetis, dimulai dengan 1.5 Cupcake yang diluncurkan pada tanggal 30 April 2009. Rilis-rilis Android selanjutnya, yaitu Donut, clair, Froyo, dan Gingerbread semua dibuat untuk *smartphone*. Namun, Apple meluncurkan iPad pada tahun 2010 dan meningkatkan ketertarikan masyarakat luas kepada *computer tablet*. Beberapa pengembang Android mencoba mengembangkan tablet Android untuk menyaingi iPad, seperti Samsung Galaxy Tab yang menggunakan Gingerbread yang dikustomisasi. Google dan OHA pun bergerak dengan melakukan pengembangan Android versi baru yang lebih optimal untuk *tablet*.

Pada tanggal 22 februari 2011, android Honeycomb diluncurkan ke pasar dan pada tanggal 24 februari 2011, tablet pertama yang menggunakan honeycomb, yaitu Motorola Xoom, diluncurkan ke pasar. Pada tanggal 19 Oktober 2011, Android meluncurkan Ice Cream Sandwich versi ini dapat bekerja secara optimal baik di *smartphone* maupun di tablet. Rilis android berikutnya, yaitu Jelly Bean, bertujuan untuk semakin meningkatkan apa yang sudah tersedia di Ice Cream Sandwich, dengan memperbaiki bug-bug dan menambahkan fitur-fitur. Pada tanggal 3 september 2013, diumumkan versi Android selanjutnya adalah Android 4.4 Kit Kat. Android sudah mendapatkan izin dari Nastle dan Hershey selaku pemilik dagang Kit Kat. Sebelum pengumuman ini, banyak yang berspekulasi bahwa versi Android berikutnya akan diberi nomor 5.0 dengan nama Key Lime Pie brikut adalah tabel

untuk semua sistem operasi Android yang sudah diluncurkan sampai sekarang. (Yusfrizal, 2019)

2.8 Android Studio

Android studio merupakan sebuah Integrated Development Environment (IDE) yang digunakan untuk mengembangan sebuah aplikasi android. Android studio digunakan sebagai alat pengembangan aplikasi android. Android studio ialah IDE resmi untuk keperluan pengembangan aplikasi android. Android studio juga merupakan pengembangan dari eclipse, namun memakan RAM lebih besar daripada eclipse. (Shani et al., 2020)

Android Studio merupakan lingkungan pengembangan perangkat lunak terpadu *Integrated Development Environment* (IDE) untuk pengembangan aplikasi Android, berdasarkan Intellij IDEA. Selain merupakan *editor* kode Intellij dan alat pengembang yang berdaya guna, Android Studio juga menawarkan banyak fitur untuk meningkatkan produktivitas saat membuat aplikasi Android. Android studio sendiri dikembangkan berdasarkan IntelliJ IDEA yang mirip dengan Eclipse disertai dengan ADT *plugin* (*Android Development Tools*). Android Studio memiliki fitur :

1) Projek berbasis pada *Gradle Build*
2) Refactory dan pembenahan *bug* yang cepat
3) Tools baru yang bernama "*Lint*" dikllaim dapat memonitor kecepatan, kegunaan, serta kompetibelitas aplikasi dengan cepat.
4) Mendukung *Proguard And App-signing* untuk keamanan.
5) Memiliki GUI aplikasi android lebih mudah
6) Didukung oleh *Google Cloud Platfrom* untuk setiap aplikasi yang dikembangkan. (Khaliq, 2021)

2.9 Android SDK

Android *SDK* (*Software Development Kit*) mencakup perangkat *tools* pengembangan yang komprehensif. Android *SDK* terdiri dari *debugger, libraries, handset emulator*, dokumentasi, contoh kode program dan tutorial. Saat ini *Android* sudah mendukung arsitektur x86 pada *Linux* (distribusi *Linux* apapun untuk *desktop*

modern), Mac OS X 10.4.8 atau lebih, *Windows* XP atau Vista. Persyaratan mencakup *JDK*, Apache Ant dan Python 2.2 atau lebih. *IDE* yang didukung secara resmi adalah *Eclipse* 3.2 atau lebih dengan menggunakan plugin Android *Development Tools* (*ADT*), dengan ini pengembang dapat menggunakan *IDE* untuk mengedit dokumen *Java* dan *XML* serta menggunakan peralatan *command line* untuk menciptakan, membangun, melakukan *debug* aplikasi Android dan pengendalian perangkat Android (misalnya *reboot*, menginstal paket perangkat lunak).

Android SDK mencakup perangkat *tools* pengembangan yang komprehensif. android SDK terdiri dari *debugger*, *libraries*, *handset emulator*, dokumentasi, dengan menggunakan plugin *Android Development Tools* (ADT), dengan ini pengembang dapat menggunakan ide untuk mengedit dokumen java dan XML serta menggunakan peralatan *command line* untuk menciptakan, membangun, melakukan *debug* aplikasi android dan pengendalian perangkat android. (Taruna et al., 2021)

Android SDK adalah adalah kit tools dari platform android khususnya bagi para programmer yang mengembangkan aplikasi berbasis android. Di dalam android SDK terdapat beberapa tools terdiri dari debugger, software libraries, emulator, dokumentasi, contoh kode, dan tutorial. Android SDK adalah tool untuk mengakses library Android dan menggunakannya untuk mengembangkan aplikasi Android. Android SDK terdapat file-file dan utilities (alat bantu) lainnya yang berfungsi untuk mempermudah pembuatan aplikasi Android secara cepat. (Cokro & Iskandar, 2019)

2.10 Java

Java adalah suatu teknologi di dunia *software* komputer, yang merupakan suatu bahasa pemrograman, dan sekaligus suatu *platform*. Sebagai bahasa pemrograman, Java dikenal sebagai bahasa pemrograman tingkat tinggi. Java mudah dipelajari, terutama bagi *programmer* yang telah mengenal C/C++. Java merupakan bahasa pemrograman berorientasi objek yang merupakan paradigma pemrograman masa depan. Sebagai bahasa pemrograman Java dirancang menjadi handal dan aman. Java juga dirancang agar dapat dijalankan di semua *platform*. Dan

juga dirancang untuk menghasilkan aplikasi-aplikasi dengan performansi yang terbaik, seperti aplikasi *database* Oracle 8i/9i yang *core*-nya dibangun menggunakan bahasa pemrograman Java.

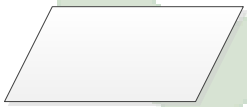
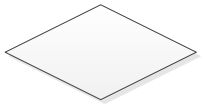
Java adalah bahasa pemrograman yang popular, dikembangkan oleh *Sun Microsystems*. Salah satu penggunaan terbesar Java adalah dalam pembuatan aplikasi *native* untuk Android. Bahasa pemrograman ini bersifat *multi platform* yakni bahasa ini dapat digunakan di berbagai *platform*, seperti *desktop, android* dan bahkan untuk sistem operasi *Linux*. Sedangkan Java bersifat neutral *architecture*, karena Java *Compiler* yang digunakan untuk mengkompilasi kode program Java dirancang untuk menghasilkan kode yang netral terhadap semua arsitektur perangkat keras yang disebut sebagai Java *Bytecode*. (Mubarok et al., 2021)

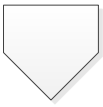
2.11 Flowchart

Flowchart adalah penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program. Bagan alir (*flowchart*) adalah bagan (*chart*) yang menunjukkan alir (*flow*) di dalam program atau prosedur sistem secara logika. Bagan alir digunakan terutama untuk alat bantu komunikasi dan untuk dokumentasi. Ada lima macam bagan alir, di antaranya :

1) Bagan Alir Sistem (*system flowchart*) merupakan bagan yang menunjukkan arus pekerjaan secara keseluruhan dari sistem.
2) Bagan Alir Dokumen (*document flowchart*) disebut juga bagan alir formulir (*form flowchart*) merupakan bagan alir yang menunjukkan arus dari laporan dan formulir termasuk tembusan-tembusannya.
3) Bagan Alir Skematik (*schematic flowchart*) merupakan bagan alir yang menggambarkan prosedur di dalam sistem dengan menggunakan simbol-simbol bagan alir sistem dan gambar-gambar komputer serta peralatan lainnya yang digunakan oleh sistem.
4) Bagan Alir Program (*program flowchart*) merupakan bagan yang menjelaskan secara rinci langkah-langkah dari proses program.
5) Bagan Alir Proses (*process flowchart*) merupakan bagan alir yang banyak digunakan di teknik industri untuk menggambarkan proses dalam suatu prosedur. (Verawati & Liksha, 2018)

Tabel 2.1. Simbol-simbol Flowchart

Simbol	Nama	Fungsi
	Terminator	Permulaan/akhir program
	Garis Alir (Flow Line)	Arah aliran program
	Preparation	Proses inisialisasi/pemberian harga awal
	Process	Proses perhitungan/proses pengolahan data
	Input/Output Data	Proses input/output data, parameter, informasi
	Predefine Process	Permulaan sub program/proses menjalankan sub program
	Decision	Perbandingan pernyataan, penyeleksian data yang memberikan pilihan untuk langkah selanjutnya
	On Page Connector	Penghubung bagian-bagian flowchat yang

		berada pada satu halaman
	Off Page Connector	Penghubung bagian-bagian flowchat yang berada pada halaman berbeda

(Sumber : Verawati & Liksha, 2018)

2.12 Penelitian terkait

Penelitian ini dilaksanakan berdasarkan beberapa penelitian terdahulu. Beberapa penelitian terdahulu yang dijadikan acuan pada penelitian ini dapat dilihat pada tabel 2.2.

Tabel 2.2. Penelitian Terdahulu

No	Peneliti	Judul	Kesimpulan
1	(Paramita & Usman Sudibyo, 2021)	Kriptografi Audio MP3 Menggunakan RSA dan Transposisi Kolom. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 5(3), 483-488. Sinta 2	Penelitian ini bertujuan untuk meneliti tentang pengamanan dari file mp3 dengan merancang aplikasi berbasis ilmu kriptografi. Algoritma kriptografi yang digunakan merupakan algoritma kombinasi dari algoritma RSA dan transposisi kolumnar. Hasilnya, dengan menggabungkan kedua algoritma tersebut, sistem aplikasi akan memiliki kemampuan untuk mengelola file mp3 dan mengenkripsi file mp3 dengan hasil data yang tidak

			dapat di putar layaknya file mp3 pada umumnya.
2	(Aminudin & Ilyas Nuryasin, 2021)	Analisis dan Implementasi Algoritma Asimetris Dual Modulus RSA (DM-RSA) pada Aplikasi Chat. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *5*(4), 768-773. Sinta 2	Penelitian ini bertujuan untuk membangun sebuah aplikasi chat dengan penerapan algoritma Asimetris Dual Modulus RSA (DM-RSA). Dari hasil pengujian faktorisasi kraitchik didapatkan bahwa algoritme DM-RSA ini terbukti lebih tahan hingga 2 kali lipat bahkan lebih dibandingkan algoritme RSA standar.
3	(Hutasuhut et al., 2019)	Digital Signature untuk Menjaga Keaslian Data dengan Algoritma MD5 dan Algoritma RSA. *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, *3*(2), 164-169. Sinta 3	Penelitian ini bertujuan untuk menjaga keaslian data untuk memberikan jaminan kepada sipenerima bahwa data tersebut bebas dari modifikasi yang dilakukan oleh pihak lain, dan jika terjadi suatu modifikasi terhadap data tersebut, maka si penerima akan mengetahui bahwa data tersebut tidak lagi terjaga keasliannya. Untuk menjaga keaslian data digunakan teknik digital signature dengan

			menggunakan algoritma MD5 sebagai algoritma fungsi hash untuk menghasilkan message digest, dan algoritma RSA sebagai algoritma kunci publik, dengan kombinasi kedua algoritma tersebut akan dihasilkan digital signature dari setiap data yang akan dijaga keasliannya.
4	(Lorien & Wellem, 2021)	Implementasi Sistem Otentikasi Dokumen Berbasis Quick Response (QR) Code dan Digital Signature. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *5*(4), 663-671. Sinta 2	Penelitian ini bertujuan untuk mengimplementasikan suatu sistem otentikasi dokumen berbasis Quick Response (QR) code dan digital signature. Sistem otentikasi dokumen yang diimplementasikan digunakan untuk menguji keaslian pada dokumen sertifikat mahasiswa sebagai contoh kasusnya. Dari pengujian sistem didapatkan hasil bahwa implementasi sistem otentikasi dokumen berbasis QR code dan digital signature ini dapat memastikan keaslian dan

			integritas dokumen sehingga mencegah pemalsuan dokumen.
5	(Labolo & Senung, 2022)	Penerapan QrCode dan Digital Signature Menggunakan Algoritma SHA Untuk Lembar Disposisi Elektronik. *JURIKOM (Jurnal Riset Komputer)*, *9*(6), 1707-1713. Sinta 4	Penelitian ini mengambil gagasan dengan memanfaatkan QRCode dan Digital signature dengan algoritma SHA yang diterapkan pada smartphone dengan sistem operasi Android untuk mempermudah proses distribusi lembar disposisi elektronik sehingga dapat mengurangi penggunaan kertas yang ada di lingkungan pemerintahan. Hasil riset ini mampu menciptakan Digital signature dan QRCode untuk dokumen elektronik pada sebuah sistem menjadi lebih terpercaya. Tanda Tangan pada dokumen diganti dengan QRCode yang digenerate menggunakan Algoritma SHA sebagai penanda unik sebuah dokumen.
6	(Wibisono et al., 2020)	Kajian Metode Metode Steganografi Pada	Tujuan dari penelitian ini adalah memberikan

		Domain Spasial. *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, *5*(2), 259-264. Sinta 2	pengetahuan tentang teknik atau metode yang ada dalam domain spasial steganografi. Steganografi adalah ilmu teknik atau seni untuk menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat di-akses oleh orang lain yang tidak mempunyai kewenangan.
7	(Wati et al., 2020)	Pendekatan Stego-Kripto Mode Cipher Block Chaining Untuk Pengamanan Informasi Pada Citra Digital. *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, *5*(2), 197-204. Sinta 2	Penelitian ini bertujuan untuk mengamankan data dengan pengamanan menggunakan Cipher Block Chaining (CBC) kemudian hasil enkripsi tersebut diamanakan melalui citra digital menggunakan algoritma LSB. Berdasarkan Hasil pengujian dengan mengukur kapasitas informasi pada citra menghasilkan data uji jika CBC dapat memproses karakter berupa huruf besar-kecil, spasi dan karakter lainnya dan hasil plainteks dan cipherteks

			menghasilkan perbandingan jumlah 1:2, namun kinerja LSB hanya menampung karakter bergantung pada jumlah ukuran pada citra digital.
8	(Ridwan et al., 2020)	Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (Dct) Pada Perusahan Alat Berat. *JITK (Jurnal Ilmu Pengetahuan Dan Teknologi Komputer)*, *5*(2), 177-182. Sinta 2	Penelitian ini dibuat untuk mengamankan dokumen digital dengan algoritma Discrete Cosine Transform (DCT) dan algoritma Advanced Encryption Standard (AES -192) berbasis Java Dekstop. Hasilnya adalah sebuah aplikasi yang dapat mengamankan sebuah data atau file yang akan disembunyikan pada file image cover. Sebelum disisipkan dengan file image cover, file tersebut dilakukan proses enkripsi pesan text terlebih dahulu dengan kunci simetris menggunakan algoritma AES-192.
9	(Hermansa et al., 2020)	Implementation of Playfair Cipher and Least Significant Bit Algorithms in Digital	Penelitian ini bertujuan untuk menerapkan pengamanan pesan informasi dengan teknik

		Imagery. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *4*(3), 454-461. Sinta 2	enkripsi dan dekripsi pesan menggunakan algoritma Playfair Cipher dengan dikombinasikan menggunakan metode Least Significant Bit (LSB). Dalam penelitian ini diperoleh bahwa algoritma playfair cipher cukup aman dalan implementasi enkripsi pesan rahasia sehingga ciphertext menjadi kumpulan data yang sudah teracak. Untuk metode steganografi Least Significant Bit (LSB) dalam penyisipan pesan rahasia atau embedded sulit ditebak secara kasat mata melihat perubahan yang terjadi antara sebelum dan sesudah gambar disisipkan tidak terlalu signifikan.
10	(Mulyono et al., 2020)	LSB Stegano Pada Kombinasi Kritpografi Simetris Caesar-Vigenere. *Dinamika Rekayasa*, *16*(2), 139-146. Sinta 3	Penelitian ini bertujuan untuk mengkombinasikan algoritma caesar, vigenere dan LSB. Dari hasil penggabungan metode antara LSB dan kriptografi dapat disimpulkan bahwa sistem pengamanan pesan menggunakan kriptografi

			dan steganografi terbagi menjadi empat, yaitu encode, decode, enkripsi dan dekripsi. Tujuan utama untuk mengamankan subtansi data rahasia dengan cara menyamarkan dengan sebuah media agar sulit untuk teridentifikasi.
11	Siahaan, R. F., Sijabat, P. I., & Sitorus, M. (2023). Penerbit Lakeisha.	Steganografi Berbasis Teks	Buku tersebut berisi pembahasan teknik-teknik steganografi yang dapat digunakan dalam menyembunyikan teks ke dalam media atau file cover seperti citra, audio dan video.
12	Prabowo, I. A., Wijayanto, H., Yudanto, B. W., & Nugroho, S. (2021). Lembaga Penelitian dan Pengabdian pada Masyarakat Universitas Dian Nuswantoro.	Buku Ajar : Pemrograman Mobile Berbasis Android (teori, latihan dan tugas mandiri)	Buku yang berisi tutorial pemrograman untuk membangun aplikasi mobile berbasis android.

13	Firly, N. (2019). Elex Media Komputindo.	Android Application Development for Rookies with Database	Buku yang diterbitkan oleh Elex Media Komputindo yang berisikan informasi-informasi untuk membangun aplikasi berbasis android dengan database yang dapat digunakan oleh pemula dalam bidang pemrograman aplikasi berbasis android.