

# Implementasi *Image Watermarking* dengan Memanfaatkan Kriptografi Visual

Reyhan Emyr Arrosyid - 13519167  
Program Studi Teknik Informatika  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung  
E-mail: 13519167@std.stei.itb.ac.id

**Abstrak**—Seiring dengan perkembangan teknologi, persebaran informasi secara digital semakin umum untuk digunakan. Persebaran informasi yang banyak dan tidak termoderasi ini mengakibatkan informasi palsu mudah untuk disebar secara luas. Perkembangan teknologi juga mengakibatkan mudahnya memanipulasi sebuah gambar dengan kualitas yang bagus. Gambar palsu dengan kualitas yang bagus akan sulit untuk diverifikasi kebenarannya. Salah satu metode untuk memverifikasi kebenaran sebuah gambar digital adalah *digital watermarking* atau penyisipan *watermark* pada gambar. Terkadang, *watermark* yang disisipkan dapat dideteksi oleh pihak yang tidak berkepentingan. Agar keberadaan *watermark* lebih sulit untuk dideteksi, *watermark* dapat disembunyikan terlebih dahulu dengan memanfaatkan kriptografi visual. Makalah ini akan membahas implementasi *watermarking* dengan terlebih dahulu mengenkripsi *watermark* dengan kriptografi visual beserta dengan pengujian dari implementasi tersebut.

**Kata kunci**—*citra; kriptografi visual; image watermarking; fragmen watermarking;*

## I. PENDAHULUAN

Pada zaman sekarang, teknologi informasi sudah berkembang dengan sangat pesat. Informasi dapat dengan mudah didapatkan dan disebar oleh orang melalui media digital seperti media sosial. Salah satu informasi yang paling sering disebar di media digital adalah gambar. Kemudahan penyebaran informasi ini terkadang membuat informasi asli bercampur dengan informasi palsu sehingga informasi sulit untuk membedakan informasi yang asli dengan yang palsu. Hal tersebut juga berlaku pada informasi berupa gambar.

Terdapat beberapa cara untuk memverifikasi keaslian suatu gambar, salah satunya adalah dengan memberi tanda khusus pada gambar yang asli. Pemberian tanda ini dapat dilakukan dengan menambahkan label atau pesan pada gambar, misalnya dengan label *copyright*. Namun, cara tersebut terkadang kurang efektif karena label tersebut dapat dipotong atau dibuang menggunakan program manipulasi gambar. Oleh karena itu, penandaan gambar dapat dilakukan dengan teknik *digital watermarking*. Teknik *digital watermarking* bekerja dengan menyisipkan tanda tersebut ke dalam gambar sedemikian sehingga tanda tersebut tidak dapat dilihat oleh mata manusia. Teknik *digital watermarking* juga tidak akan merusak gambar aslinya.

Meskipun pada dasarnya *digital watermark* tidak dapat terlihat oleh mata manusia, seseorang dengan pengetahuan yang cukup dapat mengekstraksi *watermark* tersebut. Jika seorang penyerang mengetahui keberadaan *watermark* pada suatu gambar, ia dapat mengekstrak *watermark* tersebut dan menyisipkan *watermark* tersebut ke sebuah gambar palsu sebagai upaya untuk membuat gambar palsu yang terkesan asli. Agar *watermark* lebih sulit untuk dideteksi, gambar *watermark* dapat terlebih dahulu dienkripsi dengan teknik kriptografi visual.

## II. LANDASAN TEORI

### A. Kriptografi

Kriptografi berasal dari bahasa Yunani *cryptós* yang berarti rahasia dan *gráphein* yang berarti tulisan. Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan (Schneier, 1996) [1]. Menurut Menez, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [1].

Keamanan dalam kriptografi dapat didefinisikan dengan 4 poin sebagai berikut

1. Terjaga kerahasiaannya (*confidentiality*)
2. Terjaga keasliannya (*data integrity*)
3. Yakin pengirim pesan adalah asli (*authentication*) dan bukan pihak ketiga yang menyamar
4. Pengirim pesan tidak dapat menyangkal (*non-repudiation*) telah pengirim pesan

Dalam kriptografi, terdapat beberapa terminologi yang harus dimengerti, yaitu sebagai berikut.

#### 1. Pesan

Pesan adalah informasi yang dapat dibaca dan dimengerti maknanya baik dipersepsi secara visual maupun audial. Pesan dapat berupa teks, gambar, musik, video, dll.

#### 2. Pengirim

Pengirim merupakan pihak yang mengirim pesan. Pengirim dapat berupa manusia, mesin, komputer, dll,

3. Penerima

Penerima merupakan pihak yang menerima pesan. Penerima dapat berupa manusia, mesin, komputer, dll.

4. Cipherteks

Cipherteks adalah pesan yang telah disandikan sehingga tidak lagi bermakna. Pesan disandikan dengan tujuan agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.

5. Enkripsi

Enkripsi adalah proses menyandikan pesan menjadi cipherteks.

6. Dekripsi

Dekripsi adalah proses mengembalikan cipherteks menjadi pesan semula.

7. Cipher

Cipher merupakan fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan. Cipher dapat juga disebut algoritma enkripsi dan dekripsi.

8. Kunci

Kunci adalah sebuah parameter yang digunakan di dalam enkripsi dan dekripsi. Berdasarkan prinsip Kherkoff, semua algoritma kriptografi harus bersifat tidak rahasia sedangkan kunci harus bersifat rahasia.

9. Penyadap

Penyadap adalah orang atau mesin yang mencoba menangkap pesan selama ditransmisikan.

10. Kriptanalisis

Kriptanalisis merupakan ilmu dan seni untuk memecahkan cipherteks menjadi pesan tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut kriptanalisis.

11. Kriptologi

Kriptologi merupakan studi mengenai kriptografi dan kriptanalisis.

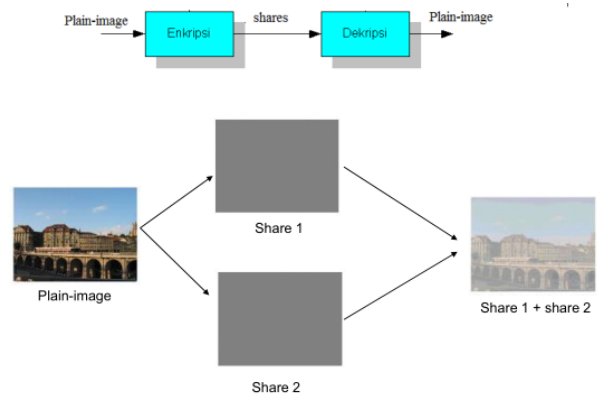
Kriptografi sudah ada sejak lama. Pada zaman dahulu, kriptografi hanya digunakan untuk mengenkripsi huruf dan angka menggunakan kertas dan pena. Zaman sekarang, kriptografi sudah sangat berkembang. Kriptografi digunakan untuk mengenkripsi dan dekripsi pesan digital seperti gambar dan video.

B. Kriptografi Visual

Kriptografi visual adalah teknik kriptografi yang mengenkripsi informasi visual dengan suatu cara sehingga dekripsi cukup dilakukan dengan mempersepsi informasi menggunakan indra penglihatan (mata) [2]. Kriptografi visual pertama kali diperkenalkan dalam makalah berjudul "Visual Cryptography" oleh Moni Naor dan Adi Shamir.

Dalam kriptografi visual, enkripsi dilakukan dengan membagi citra menjadi beberapa bagian gambar yang disebut















share. Setiap share merupakan gambar acak yang terlihat tidak bermakna. Dekripsi dalam kriptografi visual tidak membutuhkan komputasi melainkan dilakukan dengan menumpuk sejumlah share.



Gambar 1. Proses Kriptografi Visual [2]

Sebuah citra digital terdiri dari sejumlah pixel. Sebagai contoh, citra berukuran 800 x 600 berarti memiliki 800 x 600 pixel = 480.000 pixel. Dalam representasi digital, setiap pixel panjangnya n-bit sesuai dengan jenis citranya. Citra biner yang hanya terdiri atas warna hitam dan putih memiliki panjang 1 bit untuk setiap pixel-nya. Citra grayscale yang mengandung campuran warna hitam dan putih memiliki panjang 8 bit untuk setiap pixel, dan citra true color yang merupakan campuran warna merah, hijau, dan biru memiliki panjang 24 bit untuk setiap pixel-nya.

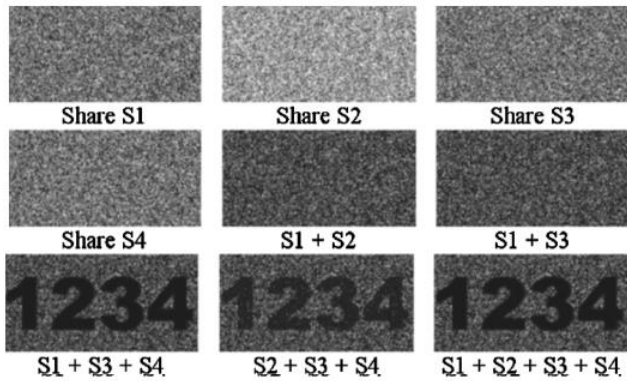
Kriptografi visual pada citra biner bekerja dengan cara membagi setiap pixel menjadi sejumlah sub-pixel. Setiap pixel pada citra akan muncul pada setiap share. Jika sub-pixel dari setiap share ditumpuk, hasil pixel dapat dilihat sebagai warna "putih" atau "hitam".

Pixel	Share #1	+	Share #2	=	Hasil
		+		=	
		+		=	
		+		=	
		+		=	

Gambar 2. Pembagian Pixel Menjadi 2 Share dengan 2 Sub-pixel [2]

Jika diperhatikan, pixel berwarna hitam akan tampak berwarna hitam juga pada hasil penumpukan share. Berbeda dengan pixel hitam, pixel putih akan terlihat tidak putih sempurna dan mengandung noise. Meskipun terdapat noise, mata manusia masih dapat mempersepsi citra semula.

Kriptografi visual dapat dilakukan dengan beberapa skema. Skema (k, n) berarti satu gambar akan dibagi menjadi n buah share. Untuk melakukan dekripsi, dibutuhkan minimal k buah share. Jika kurang dari k buah share yang ditumpuk, tidak akan menghasilkan gambar semula.



Gambar 3. Contoh Kriptografi Visual Skema (3, 4) [3]

### C. Image Watermarking

Image watermarking merupakan sebuah teknik menyisipkan watermark yaitu informasi yang mengacu kepada pemilik gambar untuk melindungi kepemilikan copyright atau menjaga keaslian konten [4]. Watermark yang disisipkan dapat berupa teks, gambar, audio, ataupun data lain. Penyisipan dilakukan tanpa merusak kualitas citra aslinya. Ketika sudah disisipkan, watermark dapat diekstraksi kembali untuk membuktikan kepemilikan atau sebagai bukti terjadinya modifikasi pada gambar.

Image watermarking dapat diklasifikasikan menjadi dua jenis, yaitu sebagai berikut.

#### 1. Fragile Watermarking

Pada fragile watermarking, watermark yang disisipkan mudah rusak jika dilakukan manipulasi pada gambar. Fragile watermarking biasa digunakan untuk membuktikan keaslian gambar dan mendeteksi modifikasi terhadap gambar.



Gambar 4. Contoh Fragile Watermarking [4]

#### 2. Robust Watermarking

Pada robust watermarking, watermark tetap kokoh dan tahan terhadap manipulasi yang dilakukan pada gambar seperti resizing, cropping, dan kompresi. Robust watermarking digunakan sebagai perlindungan hak kepemilikan suatu citra. Robust watermarking memiliki tiga persyaratan yakni imperceptible, robustness, dan secure.

### III. RANCANGAN IMPLEMENTASI

Pada bagian ini, akan dibahas dengan detail mengenai rancangan implementasi dari program image watermarking dengan menggunakan kriptografi visual.

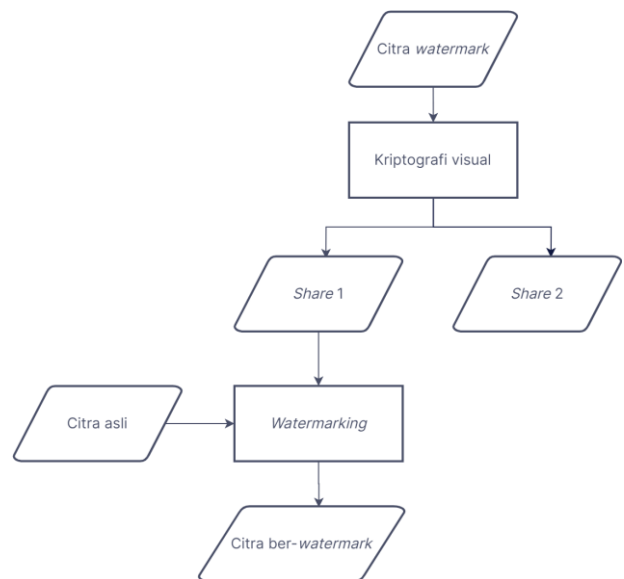
#### A. Batasan dan Asumsi

Berikut merupakan batasan dan asumsi yang digunakan dalam program yang akan diimplementasikan.

1. Program dapat melakukan watermarking terhadap citra dan watermark masukan dengan memanfaatkan kriptografi visual pada watermark.
2. Program dapat melakukan ekstraksi watermark dari citra yang sudah disisipkan watermark.
3. Jenis watermarking yang diimplementasikan hanya fragile watermarking.
4. Citra asli yang akan di-watermark merupakan citra RGB.
5. Citra Watermark merupakan citra biner.
6. Kriptografi visual dilakukan dengan menggunakan skema (2, 2) dan setiap pixel akan dipecah menjadi 4 sub-pixel.

#### B. Proses Watermarking

Berikut merupakan alur proses watermarking pada program yang akan diimplementasikan.



Gambar 5. Alur Proses Watermarking

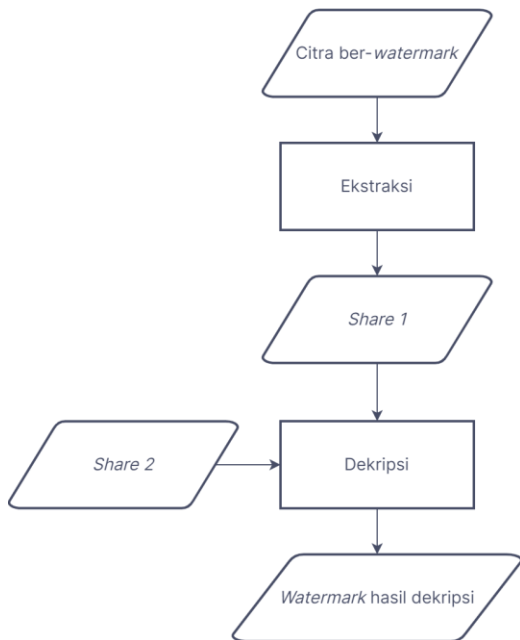
Proses watermarking menerima dua masukan yaitu citra asli yang ingin di-watermark dan citra watermark itu sendiri dan mengeluarkan dua output yaitu citra yang sudah disisipkan watermark berupa share dari citra watermark dan share lainnya.

Pertama, dilakukan kriptografi visual terhadap citra watermark masukan. Dalam program sudah didefinisikan daftar pasangan pixel share yang jika ditumpuk akan menghasilkan pixel berwarna putih dan hitam. Proses enkripsi dilakukan dengan memilih pasangan pixel share secara acak untuk setiap pixel pada citra watermark sesuai dengan warna pixel tersebut. Pasangan inilah yang akan membentuk kedua share hasil. Karena setiap pixel akan dipecah menjadi 4 sub-pixel, ukuran share empat kali lebih besar dibandingkan dengan ukuran citra watermark awal.

Selanjutnya, salah satu share dari proses enkripsi akan disisipkan pada citra asli yang ingin di-watermark. Penyisipan dilakukan dengan fragile watermarking menggunakan metode LSB. Ukuran dari hasil share tersebut akan disesuaikan sehingga sama dengan ukuran citra dengan melakukan pengulangan share. Setelah itu, setiap pixel pada citra asli diubah bit terakhirnya pada ketiga kanal R, G, dan B dengan bit pada share. Bit pada share bernilai 1 jika berwarna putih dan 0 jika berwarna hitam. Setelah proses penyisipan selesai, proses watermarking sudah selesai. Citra hasil penyisipan dan share hasil enkripsi lainnya akan disimpan pada perangkat pengguna.

C. Proses Ekstraksi

Berikut merupakan alur proses ekstraksi pada program yang akan diimplementasikan.



Gambar 6. Alur Proses Ekstraksi

Proses ekstraksi menerima dua masukan yaitu citra ber-watermark yang dihasilkan dari proses watermarking

sebelumnya dan share lainnya dari citra watermark. Proses ekstraksi mengeluarkan satu output yaitu citra watermark yang disisipkan pada citra aslinya.

Proses ekstraksi share dilakukan dengan mengambil nilai bit terakhir dari setiap pixel citra ber-watermark. Hasil dari proses ini merupakan rekonstruksi share yang akan ditumpuk dengan share masukan pengguna.

Pada proses dekripsi, share yang diekstraksi dari citra ber-watermark dan share masukan pengguna memiliki ukuran yang berbeda. Oleh karena itu, ukuran dari share masukan pengguna harus disesuaikan terlebih dahulu dengan proses yang serupa dengan pada proses penyisipan share pertama. Setelah ukuran share disesuaikan, kedua share ditumpuk menghasilkan rekonstruksi watermark yang akan disimpan pada perangkat pengguna.

IV. PENGUJIAN DAN ANALISIS

Pada bagian ini, akan dibahas mengenai pengujian program yang sudah diimplementasi. Pengujian dilakukan melalui beberapa percobaan yaitu percobaan enkripsi dan dekripsi kriptografi visual, percobaan watermarking, dan percobaan ekstraksi watermark pada citra ber-watermark yang sudah dimanipulasi. Percobaan dilakukan dengan citra asli dan citra watermark berikut.



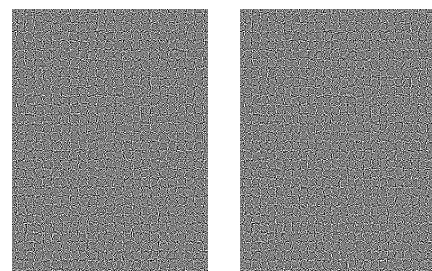
Gambar 7. Citra asli "test.bmp"



Gambar 8. Citra watermark "itb.png"

A. Pengujian Kriptografi Visual

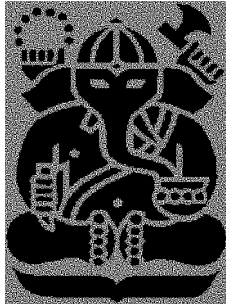
Berikut merupakan share hasil enkripsi dari citra watermark "itb.png".



Gambar 9. Dua hasil share dari citra watermark



Berikut merupakan hasil dekripsi dari kedua *share* pada Gambar 9.



Gambar 10. Hasil dekripsi kedua *share*

Berdasarkan hasil pengujian, implementasi program kriptografi visual berhasil melakukan enkripsi dan menghasilkan dua buah *share* dari citra *watermark* masukan. Implementasi program juga dapat mendekripsi kedua *share* tersebut dan menghasilkan citra *watermark* yang dapat dipersepsi manusia.

### B. Pengujian Watermarking

Pengujian ini bertujuan untuk memastikan implementasi program sudah dapat menyisipkan dan mengekstrak *watermark* dengan benar. Berikut merupakan hasil citra yang sudah disisipkan *watermark* beserta dengan citra *watermark* yang diekstrak.



Gambar 11. Citra ber-*watermark* (kiri) dan *watermark* hasil ekstraksi (kanan)

Berdasarkan hasil pengujian di atas, program sudah berhasil menyisipkan *share watermark* ke dalam citra asli. Citra ber-*watermark* tampak sama dengan citra aslinya. Program juga sudah dapat mengekstraksi *watermark* yang terdapat pada citra tersebut.

### C. Pengujian Manipulasi Citra

Pengujian pada bagian ini bertujuan untuk mengetahui hasil *watermark* yang diekstrak dari citra yang telah dimodifikasi. Modifikasi yang dilakukan pada citra yaitu modifikasi penambahan objek pada gambar (*insertion*), modifikasi *brightness* dan *contrast*, dan modifikasi warna citra (*hue*). Berikut merupakan citra ber-*watermark* yang telah dimodifikasi.



(a)

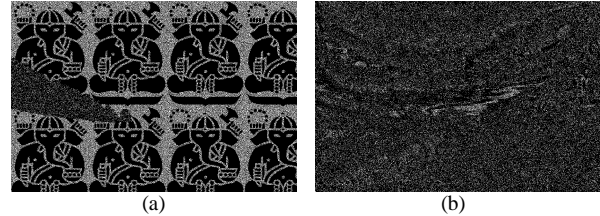
(b)



(c)

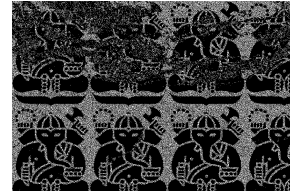
Gambar 12. Citra ber-*watermark* yang sudah dimodifikasi dengan penambahan objek (a), pengaturan *brightness* dan *contrast* (b), dan perubahan *hue* (c)

Berikut merupakan citra *watermark* hasil ekstraksi dari ketiga citra yang terdapat pada Gambar 12.



(a)

(b)



(c)

Gambar 13. Citra *watermark* yang diekstrak dari citra yang sudah dimodifikasi dengan penambahan objek (a), pengaturan *brightness* dan *contrast* (b), dan perubahan *hue* (c)

Berdasarkan hasil pengujian di atas, modifikasi penambahan objek, *brightness* dan *contrast*, serta perubahan warna pada citra ber-*watermark* akan merusak *watermark* yang telah disisipkan. Hal ini sesuai dengan konsep *fragile watermarking* yakni *watermark* mudah rusak jika dilakukan manipulasi terhadap citra.

Pada manipulasi penambahan objek, kerusakan *watermark* hanya terjadi pada bagian kecil *watermark* yaitu pada tempat ditambahnya objek. Hal ini terjadi karena penyisipan *watermark* dilakukan untuk setiap *pixel* citra secara berurutan dan penambahan objek hanya mengubah nilai *pixel* pada tempat objek ditambahkan saja.

Pada manipulasi *brightness* dan *contrast*, perubahan terjadi pada seluruh *pixel* citra. Hasil *watermark* yang diekstrak dari citra rusak total hingga *watermark* asli sudah tidak dapat dilihat. Hal ini dapat terjadi karena pengubahan *brightness* dan *contrast* mengubah nilai bit terakhir dari hampir semua *pixel* dalam citra ber-*watermark*. Ini mengakibatkan *share* yang diekstrak dari citra sangat berbeda dengan *share* aslinya dan jika ditumpuk dengan *share* lainnya tidak akan menghasilkan gambar yang bermakna.

Pada pengujian manipulasi *hue*, kerusakan *watermark* terjadi pada sebagian *watermark* dan masih terdapat bagian *watermark* yang dapat dilihat. Meskipun perubahan *hue* dilakukan untuk seluruh *pixel* citra seperti perubahan *brightness* dan *contrast*, perubahan *hue* tidak mengubah nilai bit terakhir *pixel* pada sebagian *pixel*. Hal ini menyebabkan *share* hasil ekstraksi masih sama dengan *share* aslinya di

sebagian tempat sehingga sebagian tumpukan kedua *share* masih dapat menghasilkan gambar bermakna.

## V. KESIMPULAN

Kriptografi visual dapat digunakan bersamaan dengan proses *image watermarking* untuk mengenkripsi *watermark* sebelum disisipkan pada suatu citra. Enkripsi dengan kriptografi visual dilakukan untuk menyembunyikan keberadaan *watermark* sehingga kemungkinan penyerang untuk mendeteksi dan mengekstrak *watermark* lebih kecil.

Berdasarkan pengujian yang telah dilakukan pada bagian sebelumnya, dapat disimpulkan program yang diimplementasikan sukses untuk melakukan *fragile watermarking* dengan terlebih dahulu mengenkripsi *watermark* dengan kriptografi visual. Program juga sukses dalam mengekstraksi *watermark* yang telah disisipkan.

## UCAPAN TERIMA KASIH

Pertama-tama, penulis mengucapkan puji syukur kepada Allah SWT karena berkat kehendak-Nya penulis dapat menyelesaikan tugas makalah untuk mata kuliah Kriptografi ini dengan baik. Selanjutnya, penulis juga ingin mengucapkan terima kasih kepada keluarga, teman, dan pihak lain yang terlibat dalam pembuatan makalah ini. Terakhir, penulis berterima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT. selaku dosen IF4020 Kriptografi yang sudah memberikan ilmu dan pengetahuan kepada penulis selama perkuliahan sehingga penulis dapat menyelesaikan makalah ini.

## REFERENSI

- [1] Munir, Rinaldi. "Pengantar Kriptografi". [https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2021-2022/Pengantar-Kriptografi-\(2021\).pdf](https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2021-2022/Pengantar-Kriptografi-(2021).pdf). Diakses pada 18 Desember 2021.
- [2] Munir, Rinaldi. "Kriptografi Visual, Teori dan Aplikasinya (Bagian 1)". <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Visual-Bagian1.pdf>. Diakses pada 18 Desember 2021.
- [3] Munir, Rinaldi. "Kriptografi Visual, Teori dan Aplikasinya (Bagian 2)". <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Visual-Bagian2.pdf>. Diakses pada 18 Desember 2021.
- [4] Munir, Rinaldi. "Digital Watermarking". <https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Digital-watermarking-2020.pdf>. Diakses pada 19 Desember 2021.
- [5] Tanha, M., Torshizi, S. D. S., Abdullah, M. T., & Hashim, F. (2012). An overview of attacks against digital watermarking and their respective countermeasures. Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012.

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Jakarta, 20 Desember 2021



Reyhan Emyr Arrosyid 13519167