Implementasi *Watermark* pada Kwitansi Digital dengan Kriptografi Visual

Zachrandika Alif Syahreza - 18219036
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail: 18219036@std.stei.itb.ac.id

***Abstrak*—Dengan pesatnya perkembangan teknologi, penggunaan dan penyebaran informasi secara digital semakin luas. Namun, hal ini juga membawa dampak negatif seperti penyebaran informasi palsu yang sulit dikendalikan. Selain itu, teknologi juga memudahkan manipulasi gambar dengan kualitas yang sangat baik. Gambar palsu dengan kualitas tinggi seringkali sulit untuk diverifikasi keasliannya. Untuk mengatasi masalah ini, salah satu metode yang digunakan adalah *digital watermarking* atau penyisipan *watermark* pada gambar. Namun, seringkali watermark yang terlihat dapat dengan mudah dideteksi oleh pihak yang tidak berkepentingan. Oleh karena itu, agar *watermark* sulit dideteksi, dapat dilakukan teknik penyembunyian terlebih dahulu dengan memanfaatkan kriptografi visual. Dalam makalah ini, akan dibahas implementasi dari teknik *watermarking* dengan melakukan enkripsi terlebih dahulu pada *watermark* menggunakan kriptografi visual, serta pengujian hasil implementasi tersebut.**

Kata kunci—watermark; kwitansi digital; kriptografi;

I. Pendahuluan

Perkembangan pesat dalam bidang teknologi telah membawa perubahan signifikan dalam cara penggunaan dan penyebaran informasi. Dalam era digital saat ini, informasi dapat dengan mudah diakses dan disebarluaskan melalui berbagai *platform* dan media elektronik. Meskipun demikian, dampak negatif dari kemajuan teknologi juga mulai muncul, seperti penyebaran informasi palsu yang sulit dikendalikan.

Selain masalah penyebaran informasi palsu, kemajuan teknologi juga memungkinkan manipulasi gambar dengan kualitas yang sangat baik. Gambar-gambar palsu dengan kualitas tinggi seringkali sulit untuk diverifikasi keasliannya. Dalam konteks ini, diperlukan metode yang dapat membantu mengatasi masalah ini, yaitu *digital watermarking* atau penyisipan *watermark* pada gambar.

Digital watermarking adalah teknik yang digunakan untuk menyisipkan informasi tambahan ke dalam suatu gambar atau media digital lainnya. Tujuan utama dari *digital watermarking* adalah untuk melindungi dan memverifikasi keaslian gambar tersebut. Namun, seringkali *watermark* yang terlihat dapat dengan mudah dideteksi oleh pihak yang tidak berkepentingan, sehingga menurunkan efektivitasnya.

Untuk mengatasi masalah tersebut, salah satu pendekatan yang dapat digunakan adalah dengan melakukan penyembunyian terlebih dahulu pada *watermark* menggunakan kriptografi visual. Kriptografi visual adalah teknik yang menggabungkan prinsip kriptografi dan citra digital untuk menyembunyikan informasi secara tidak terlihat pada gambar. Dengan menggunakan kriptografi visual, *watermark* dapat disisipkan ke dalam gambar dengan cara yang sulit dideteksi oleh pihak yang tidak berkepentingan.

Makalah ini bertujuan untuk membahas implementasi teknik *watermarking* dengan melakukan enkripsi terlebih dahulu pada watermark menggunakan kriptografi visual. Selain itu, makalah ini juga akan menguji hasil implementasi tersebut untuk mengevaluasi keefektifan dan keamanan dari teknik yang digunakan.

Melalui penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan metode *digital watermarking* yang lebih handal dan efektif dalam melindungi dan memverifikasi keaslian gambar. Dengan menggunakan teknik penyembunyian *watermark* melalui kriptografi visual, diharapkan dapat meningkatkan tingkat keamanan serta membuat *watermark* sulit dideteksi oleh pihak yang tidak berkepentingan.

II. Landasan Teori

A. Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [1]. Kriptografi berasal dari bahasa Yunani yaitu cryptós yang berarti *secret* atau dalam bahasa Indonesia berarti rahasia dan gráphein yang berarti *writing* atau dalam bahasa Indonesia tulisan [1].

Kriptografi terbagi kedalam empat layanan diantaranya sebagai berikut.

1. Kerahasiaan pesan (*Confidentiality*)

   Layanan kriptografi ini bertujuan untuk menjaga pesan tetap rahasia dan hanya dapat diakses oleh pihak yang berwenang. Hal ini dilakukan dengan menggunakan algoritma enkripsi yang mengubah pesan asli menjadi bentuk yang tidak terbaca

(*ciphertext*) kecuali untuk penerima yang memiliki kunci dekripsi yang sesuai [2].

2. Keaslian pesan (*Data integrity*)

   Layanan kriptografi ini memastikan bahwa pesan tidak diubah atau dimanipulasi selama proses pengiriman. Untuk mencapai ini, algoritma hash digunakan untuk menghasilkan nilai hash dari pesan asli. Penerima dapat memverifikasi integritas pesan dengan membandingkan nilai hash yang diterima dengan nilai hash yang dihasilkan dari pesan yang diterima [3].

3. Keaslian pengirim dan penerima pesan (*Authentication*)

   Layanan kriptografi ini digunakan untuk memverifikasi identitas pengirim dan penerima pesan. Hal ini dilakukan dengan menggunakan teknik kriptografi seperti tanda tangan digital atau sertifikat digital. Tanda tangan digital memastikan bahwa pesan berasal dari pengirim yang sah, sedangkan sertifikat digital menyediakan metode untuk memverifikasi identitas penerima [4].

4. Anti penyangkalan (Non-repudiation)

   Layanan kriptografi ini mencegah pengirim atau penerima pesan untuk menyangkal keterlibatan mereka dalam pertukaran pesan. Dengan menggunakan tanda tangan digital, penerima dapat membuktikan kepada pihak lain bahwa pesan tersebut berasal dari pengirim tertentu dan tidak dapat ditolak oleh pengirimnya [5].

Dalam ilmu kriptografi terdapat beberapa terminologi yang sebelumnya harus diketahui dan dipahami, diantaranya sebagai berikut.

1. Pesan

   Pesan merupakan data atau informasi yang dapat dibaca dan dimengerti maknanya baik dipersepsi secara visual maupun audial.

2. Pengirim

   Pengirim merupakan pihak yang mengirim pesan.

3. Penerima

   Penerima merupakan pihak yang menerima pesan.

4. Penyusup

   Penyusup merupakan pihak ketiga yang menyadap, mengintersepsi, menghapus, menambah, atau mengubah pesan.

5. *Ciphertext*

   Ciphertext merupakan pesan yang telah disandikan sehingga tidak bermakna lagi. tujuannya adalah agar pesan tidak dapat dibaca oleh pihak yang tidak berhak.

6. Enkripsi

   Enkripsi merupakan proses menyandikan sebuah pesan kedalam bentuk *ciphertext*.

7. Dekripsi

   Dekripsi merupakan proses mengembalikan ciphertext menjadi pesan semula.

8. Kunci

   Kunci merupakan parameter yang digunakan di dalam enkripsi dan dekripsi.

9. *Cipher*

   Cipher merupakan fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan.

10. Kriptanalisis

    Kriptanalisis merupakan ilmu dan snei untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Pelaku kriptanalisis disebut sebagai kriptanalis.

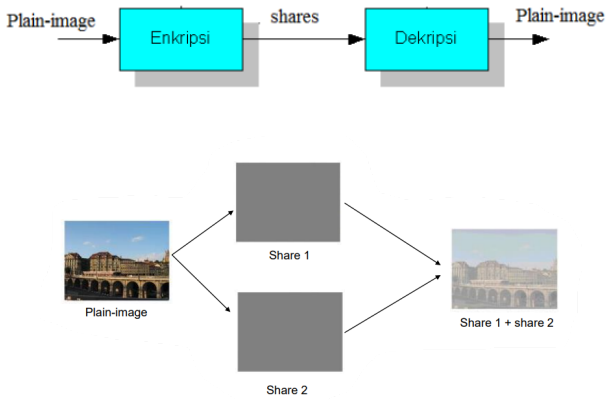
11. Kriptologi

    Kriptologi merupakan studi mengenai kriptografi dan kriptanalisis.

B. Kriptografi Visual

Kriptografi visual merupakan sebuah metode kriptografi yang mengamankan informasi visual dengan cara tertentu, sehingga proses dekripsi dapat dilakukan dengan hanya menggunakan persepsi visual melalui indra penglihatan, yaitu mata [6]. Enkripsi dilakukan dengan membagi gambar menjadi sejumlah bagian yang disebut share.

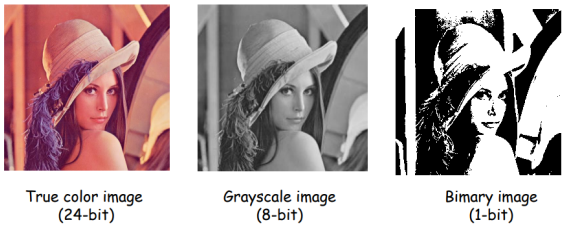
Dalam kriptografi visual, gambar dibagi menjadi sejumlah *share* oleh dealer. *Share* merupakan gambar acak yang apabila dilihat tidak memiliki makna. Sedangkan pihak yang menerima *share* dinamakan partisipan. Dekripsi dilakukan oleh partisipan dengan menumpuk *share* yang mereka miliki.



Gambar 1. Diagram proses kriptografi visual [6]

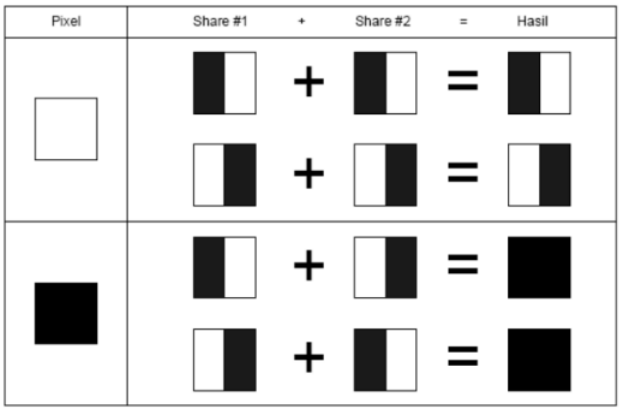
Citra terdiri dari sejumlah *pixel*. Contohnya citra dengan ukuran 1200 x 1500 berarti memiliki 1200 x 1500 *pixel* = 1.800.000 *pixel*. Setiap *pixel* memiliki panjang *n*-bit. Terdapat

tiga jenis citra, diantaranya citra biner, *greyscale*, dan *true color*.



Gambar 2. Contoh jenis citra beserta ukuran bit/pixel [6]

Proses kerja pada kriptografi visual dengan membagi setiap *pixel* dibagi menjadi sejumlah *sub-pixel*. Setiap *pixel* akan muncul pada setiap *share*. Apabila *sub-pixel* dari setiap *share* ditumpuk, akan membentuk *pixel* yang dipersepsi sebagai "putih" atau "hitam".



Gambar 3. *Pixel* dibagi menjadi 2 *share* dan 2 *sub-pixel* [6]

Pada gambar diatas dapat dilihat bahwa *pixel* berwarna hitam apabila dilakukan penumpukan *share* makan hasil penumpukan *share* akan kembali menjadi *pixel* berwarna hitam. Sedangkan untuk *pixel* berwarna putih akan memiliki warna putih yang tidak sempurna dari hasil penumpukan *share*.

C. *Image Watermarking*

Image watermarking adalah sebuah metode yang digunakan untuk menyisipkan *watermark* ke dalam gambar [7]. *Watermark* ini berisi informasi yang mengacu kepada pemilik gambar untuk melindungi hak cipta atau menjaga keaslian konten. *Watermark* yang disisipkan dapat berupa teks, gambar, audio, atau data lainnya.

Proses penyisipan dilakukan tanpa merusak kualitas citra asli. Setelah disisipkan, *watermark* dapat diekstraksi kembali untuk membuktikan kepemilikan atau sebagai bukti terjadinya modifikasi pada gambar.

Image watermarking dapat diklasifikasikan menjadi dua kategori utama diantaranya adalah sebagai berikut

.

1. *fragile* (rapuh)

   Watermarking fragile adalah metode yang digunakan untuk mendeteksi dengan akurat perubahan atau manipulasi pada gambar. Metode ini sangat sensitif terhadap perubahan apapun pada gambar, baik itu modifikasi kecil maupun besar.

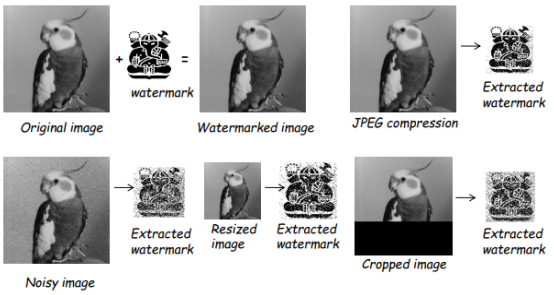
   Tujuan utama dari *watermarking fragile* adalah untuk memberikan keamanan terhadap keaslian dan integritas gambar. Jika terjadi modifikasi pada gambar, *watermarking fragile* akan menghasilkan tanda atau pesan yang menunjukkan adanya perubahan tersebut.

Gambar 4. Contoh *watermarking fragile* [7]

2. *robust* (tahan lama).

   Watermarking robust adalah metode yang dirancang untuk bertahan terhadap perubahan atau serangan yang mungkin terjadi pada gambar, seperti kompresi, *cropping*, atau *noise addition*.

   Metode ini memiliki tingkat keandalan yang tinggi dan mampu mempertahankan *watermark* yang disisipkan walaupun melalui proses pengolahan atau transformasi tertentu. Tujuan utama dari *watermarking robust* adalah untuk memberikan perlindungan terhadap pencurian hak cipta dan penggunaan ilegal gambar.



Gambar 5. Contoh *watermarking robust* [7]

III. Rancangan Implementasi

Pada bagian ini akan menjelaskan secara rinci mengenai perencanaan dan implementasi program *watermarking* pada kwitansi digital dengan menggunakan kriptografi visual.

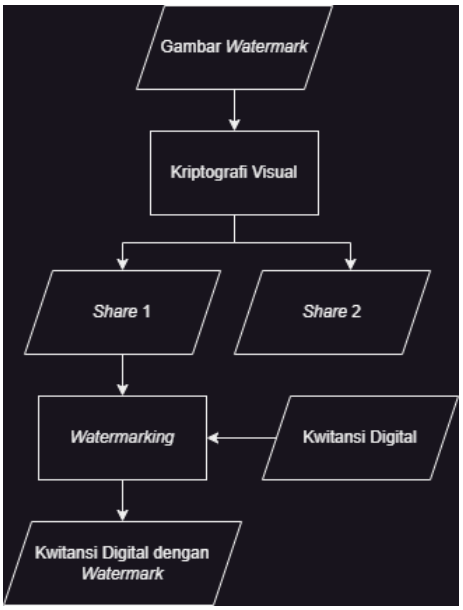
A. *Batasan dan Asumsi*.

Berikut merupakan batasan dan asumsi yang digunakan dalam melakukan implementasi program.

1. Kwitansi digital yang digunakan dalam implementasi program dalam bentuk citra.
2. Program dapat melakukan ekstraksi dari citra yang telah diberikan *watermark*.
3. Penggunaan jenis *watermarking* yang digunakan adalah *watermarking fragile*.
4. Skema kriptografi visual yang digunakan yaitu (2,2) dengan setiap *pixel* akan dipecah menjadi 4 *sub-pixel*.

B. *Proses Watermarking*

Berikut merupakan alur proses pemberian *watermark* pada program yang akan diimplementasikan.

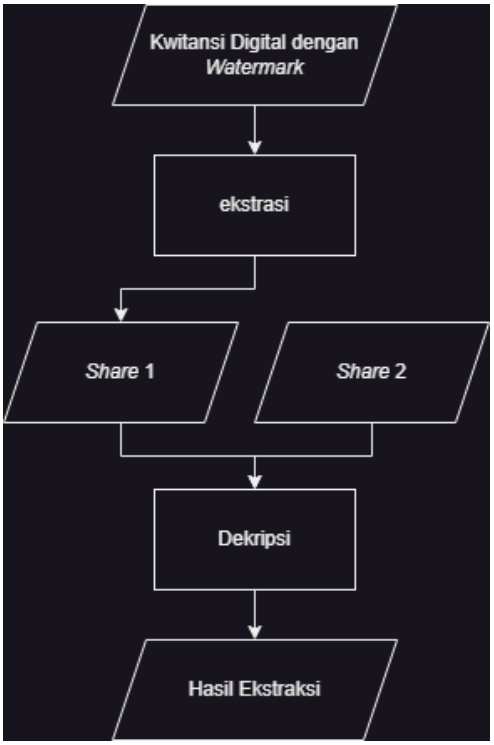


Gambar 6. *Flowchart Watermarking*

Proses melakukan *watermarking* pada kwitansi digital diawali dengan melakukan kriptografi visual untuk menghasilkan pasangan *share* yang disimpan pada perangkat pengguna dari gambar yang akan dijadikan sebagai *watermark*. Salah satu *share* akan dimasukkan ke dalam kwitansi digital dengan menggunakan metode LSB, yaitu dengan mengubah setiap bit terakhir pada *pixel*. Setelah proses penyisipan *share* kedalam kwitansi digital selesai, maka proses *watermarking* selesai.

C. *Proses Ekstraksi*

Berikut merupakan alur proses ekstraksi pada program yang akan diimplementasikan

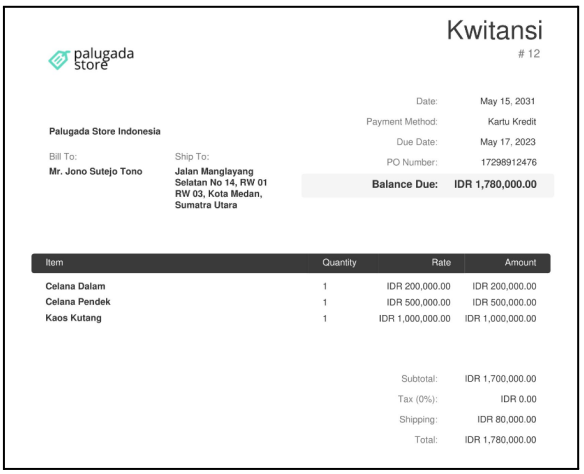


Gambar 7. *Flowchart* Ekstraksi

Proses melakukan ekstraksi pada kwitansi digital yang telah memiliki *watermark* diawali dengan melakukan ekstraksi dengan menempuh *share* yang sebelumnya sudah dimasukkan kedalam kwitansi digital dengan *share* yang lain. Selanjutkan akan dilakukan proses dekripsi dengan mengekstraksi *share* dari kwitansi digital yang memiliki *watermark*. Setelah proses dekripsi selesai maka akan dihasilkan gambar rekonstruksi *watermark*.

IV. Pengujian dan Analisis

Pada bagian ini, akan dilakukan pengujian program yang sudah berhasil diimplementasikan. Pengujian yang dilakukan berupa proses enkripsi, dekripsi, memberikan *watermark* pada kwitansi digital, dan melakukan ekstraksi *watermark* pada kwitansi digital. Berikut adalah contoh kwitansi digital dan gambar *watermark* yang digunakan.

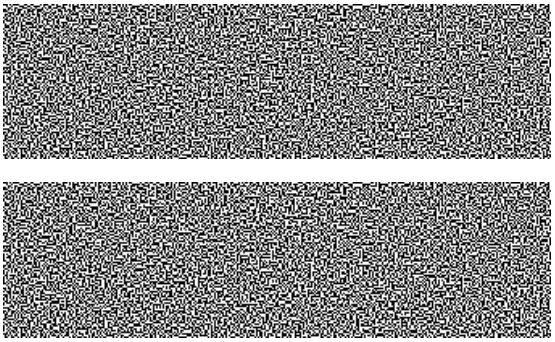


Gambar 8. Kwitansi Digital

Gambar 9. Gambar *Watermark*

A. Pengujian Kriptografi Visual

Berikut merupakan *share* yang dihasilkan dari enkripsi gambar *watermark*.



Gambar 10. *Share* dari hasil enkripsi *watermark*

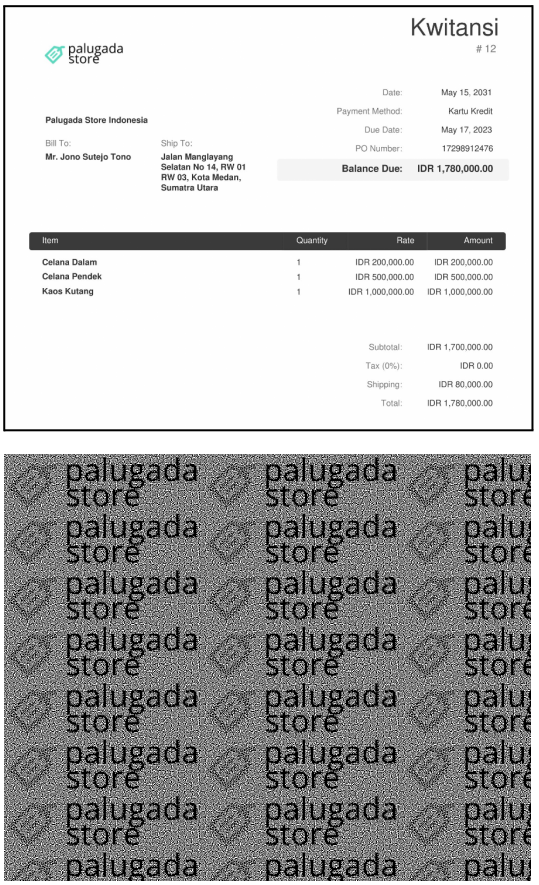
Berikut merupakan hasil dekripsi kedua *share* pada gambar 10.

Gambar 11. Hasil dekripsi kedua *share*

Dari hasil pengujian yang dilakukan, implementasi program kriptografi visual berhasil dalam melakukan proses enkripsi dan menghasilkan dua bagian gambar *watermark* dari gambar *input*. Selain itu, implementasi program juga dapat melakukan proses dekripsi terhadap kedua bagian tersebut dan menghasilkan gambar *watermark* yang dapat dilihat oleh manusia.

B. Pengujian Watermarking

Pengujian ini dilakukan untuk memverifikasi bahwa implementasi program dapat melakukan proses penyisipan dan ekstraksi *watermark* dengan benar. Berikut adalah hasil kwitansi digital yang telah disisipkan *watermark* beserta gambar kwitansi digital ber-*watermark* yang diekstraksi.



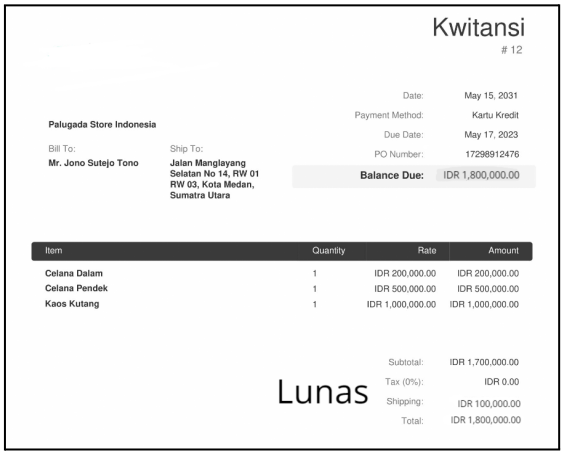
Gambar 12. Kwitansi Digital ber-*watermark* (atas) dan Hasil Ekstraksi Kwitansi Digital yang ber-*watermark* (bawah)

Berdasarkan hasil pengujian yang telah dilakukan, program telah berhasil dalam menyisipkan bagian *watermark* ke dalam kwitansi digital. Kwitansi digital yang telah ber-*watermark* terlihat serupa dengan kwitansi digital aslinya. Selain itu, program juga mampu mengekstraksi *watermark* yang ada pada kwitansi digital tersebut.

C. Pengujian Pemalsuan Kwitansi Digital

Pengujian pada bagian ini dilakukan untuk mengamati hasil dari ekstraksi *watermark* dari kwitansi digital yang telah mengalami pemalsuan.

Modifikasi yang dilakukan pada kwitansi digital mencakup menghilangkan logo toko, perubahan biaya *shipping*, penambahan teks “Lunas”, dan perubahan total nominal pada kolom “Balance Due” dan “Total”.



Gambar 13. Kwitansi Digital Palsu

Berikut merupakan gambar *watermark* hasil ekstraksi dari kwitansi digital yang telah dimanipulasi.

Gambar 14. Hasil Ekstraksi *Watermark* Kwitansi Digital Palsu

Berdasarkan hasil pengujian di atas, kwitansi digital yang telah dipalsukan terlihat menghasilkan ekstraksi *watermark* yang memiliki beberapa kecacatan *watermark* di beberapa titik *pixel*

V. Kesimpulan

Kriptografi visual dapat bekerja secara simultan dengan proses *image watermarking* untuk mengenkripsi *watermark* sebelum disisipkan ke dalam gambar. Dengan melakukan enkripsi menggunakan kriptografi visual, keberadaan *watermark* dapat disembunyikan, sehingga kemungkinan bagi penyerang untuk mendeteksi dan mengekstrak *watermark* menjadi lebih kecil.

Berdasarkan hasil pengujian yang telah dilakukan sebelumnya, dapat disimpulkan bahwa program yang diimplementasikan berhasil dalam melakukan *watermarking fragile* dengan langkah awal mengenkripsi *watermark* menggunakan kriptografi visual. Selain itu, program juga berhasil dalam proses ekstraksi *watermark* yang telah disisipkan.

References

[1] Munir, Rinaldi. “Pengantar Kriptografi”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/01-Pengantar-Kriptografi-(2023).pdf. Diakses pada 20 Mei 2023.

[2] W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson, 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7964751

[3] D. R. Stinson, "Cryptography: Theory and Practice," CRC Press, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8688747

[4] J. Katz and Y. Lindell, "Introduction to Modern Cryptography," CRC Press, 2014. [Online]. Available: https://ieeexplore.ieee.org/document/7904370

[5] D. R. Stinson, "Cryptography: Theory and Practice," CRC Press, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8688747

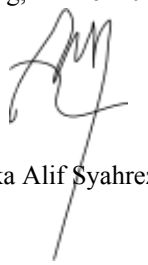
[6] Munir, Rinaldi. “Kriptografi Visual Bagian 1”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/38-Kriptografi-Visual-Bagian1-2023.pdf. Diakses pada 20 Mei 2023.

[7] Munir, Rinaldi. “Digital Watermarking”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/10-Digital-watermarking-2023.pdf. Diakses pada 20 Mei 2023.

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.

Bandung, 22 Mei 2023



Zachrandika Alif Syahreza