Perlindungan Hak Cipta Gambar dengan *Watermarking* berbasis MVQ

Gressia Melissa – NIM : 13506017

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jalan Ganesha no.10 Bandung
E-mail : if16017@students.if.itb.ac.id

Abstrak :

Steganografi merupakan salah satu pendekatan yang dapat digunakan dalam perlindungan hak cipta pada berbagai media. Media yang dimaksud dapat berupa gambar, audio, teks, maupun video. Pesatnya perkembangan teknologi multimedia dan jaringan komputer secara langsung mempermudah pembuatan dan pendistribusian konten *digital*, dalam waktu bersamaan timbul isu baru yaitu penyalahgunaan Hak Atas Kekayaan Intelektual (HAKI). Oleh karena itu, *watermark digital* diperkenalkan sebagai salah satu solusi dari masalah perlindungan hak cipta konten multimedia.

Pada makalah ini, akan dibahas mengenai metode MVQ (*Mean-removed Vector Quantization*) untuk perlindungan citra melalui *watermarking digital*. MVQ yang diperkenalkan pada tahun 2006 oleh Zhe Ming Lu et al. merupakan pengembangan dari pendekatan *vector quantization* untuk citra. *Vector quantization* merupakan pendekatan untuk membuat gambar mozaik, dimana untuk mensegmentasi sebuah objek citra dilakukan kuantisasi yang probabilitas distribusi input vektornya berdasarkan *codebook vector*. *Vector quantization* digunakan agar penempatan *codebook* menghasilkan karakteristik mozaik yang unik atau berbeda-beda. Dengan demikian, hasil gambar mozaik dapat dikontrol sesuai kebutuhan. Hal ini didasari fakta bahwa citra yang berdekatan memiliki hubungan, sehingga ada kemungkinan yang sangat besar bahwa piksel yang bertetangga dengan suatu piksel X akan mempunyai nilai yang sama atau hampir sama dengan piksel X tersebut.

Kata kunci : HAKI, gambar, MVQ, *watermarking* citra.

1. Pendahuluan

Pesatnya perkembangan teknologi multimedia dan jaringan komputer secara langsung mempermudah pembuatan dan pendistribusian konten *digital*, dalam waktu bersamaan timbul isu baru yaitu penyalahgunaan Hak Atas Kekayaan Intelektual (HAKI).

Dengan perkembangan komputer *digital* dan perangkat-perangkat lainnya, membuat data *digital* banyak digunakan dan dimanfaatkan untuk kebutuhan pokok maupun penunjang. Ada beberapa faktor yang membuat data *digital* (seperti audio, citra, video, dan tulisan) banyak digunakan, antara lain:

- Mudah diduplikasi dan hasil duplikasi sama dengan aslinya.
- Murah untuk melakukan penduplikasian dan penyimpanan terhadap data.
- Mudah disimpan untuk kemudian diolah atau diproses lebih lanjut.
- Mudah didistribusikan, baik melalui jaringan seperti internet, maupun media *storage*.

Oleh karena itu, sangat dibutuhkan adanya cara alternatif atau pelengkap kriptografi, teknologi yang mampu memproteksi isi media bahkan setelah didekripsi. *Watermarking* memiliki potensi untuk memenuhi kebutuhan ini karena peletakan informasi *watermark* dalam isi yang tidak dapat diambil dalam penggunaan normal. *Watermark digital* diperkenalkan sebagai salah satu solusi dari masalah perlindungan hak cipta konten multimedia. Untuk aplikasi perlindungan hak cipta, sebuah *watermark digital* harus memiliki kriteria dasar seperti transparansi (ketidaknampakan), yaitu *watermark* yang disisipkan pada konten secara sistem penglihatan manusia tidak tampak. Serta *robustness* (kekokohan), yaitu *watermark* yang disisipkan pada konten *digital* harus sulit dihilangkan kecuali terjadi perubahan drastis terhadap konten *digital* yang dikenali dengan

adanya perubahan secara sistem penglihatan manusia.

2. *Watermarking*

2.1. Definisi

Pada dasarnya, teknik *watermarking* adalah proses menambahkan kode identifikasi secara permanen ke dalam data *digital*. Kode identifikasi tersebut dapat berupa teks, gambar, suara, atau video. Selain tidak merusak data *digital* produk yang akan dilindungi, kode yang disisipkan seharusnya memiliki ketahanan (*robustness*) dari berbagai pemrosesan lanjutan seperti pengubahan, transformasi geometri, kompresi, enkripsi, dan sebagainya.

Sifat *robustness* berarti data *watermark* tidak rusak akibat pemrosesan lanjutan tersebut. Kode yang disisipkan dalam citra *digital* pun tidak akan merusak citra aslinya. *Watermark* dalam citra *digital* tersebut tidak dapat diketahui keberadaannya oleh pihak lain yang tidak mengetahui rahasia skema penyisipan *watermark*. *Watermark* tersebut juga tidak dapat diidentifikasi dan dihilangkan.

Watermarking ini memanfaatkan kekurangan-kekurangan sistem indera manusia seperti mata dan telinga. Dengan adanya kekurangan inilah, metoda *watermarking* ini dapat diterapkan pada berbagai media *digital*. Jadi *watermarking m*erupakan suatu cara untuk penyembunyian atau penanaman data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu data *digital* lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran), dan mampu menghadapi prosesproses pengolahan sinyal *digital* sampai pada tahap tertentu.

2.2. Pelabelan Hak Cipta

Beberapa cara yang pernah dilakukan oleh orang-orang untuk mengatasi masalah pelabelan hak cipta pada data *digital*, antara lain:

- ***Hearder Marking***
  Dengan memberikan keterangan atau informasi hak cipta pada header dari suatu data *digital*.

- ***Visible Marking***
  Merupakan cara dengan memberikan tanda hak cipta pada data *digital* secara eksplisit.

- ***Encryption***
  Mengkodekan data *digital* ke dalam representasi lain yang berbeda dengan representasiaslinya (tetapi dapat dikembalikan ke bentuk semula) dan memerlukan sebuah kunci dari pemegang hak cipta untuk mengembalikan ke representasi aslinya.

- ***Copy Protection***
  Memberikan proteksi pada data *digital* dengan membatasi atau dengan memberikan proteksi sedemikian rupa sehingga data *digital* tersebut tidak dapat diduplikasi.

Cara-cara diatas memiliki kelemahan tersendiri, sehingga tidak dapat banyak diharapkan sebagai metoda untuk mengatasi masalah pelabelan hak cipta ini. Kekurangan tersebut antara lain :

- ***Header Marking***
  Dengan menggunakan software sejenis Hex Editor, orang lain dengan mudah membuka file yang berisi data *digital* tersebut, dan menghapus informasi yang berkaitan dengan hak cipta dan sejenisnya yang terdapat di dalam header file tersebut.

- ***Visible Marking***
  Penandaan secara eksplisit pada data *digital*, memang memberikan sejenis tanda semi-permanen, tetapi dengan tersedianya software atau metoda untuk pengolahan, maka dengan sedikit ketrampilan dan kesabaran, tanda yang semipermanen tersebut dapat dihilangkan dari data *digital*nya.

- ***Encryption***
  Penyebaran data *digital* dengan kunci untuk decryption tidak dapat menjamin penyebarannya yang legal. Maksudnya setelah data *digital* terenkripsi dengan kuncinya telah diberikan kepada pihak yang telah membayar otoritas (secara legal), maka tidak dapat dijamin penyebaran data *digital* yang telah terdekripsi tadi oleh pihak lain tersebut.

- ***Copy Protection***
  Proteksi jenis ini biasanya dilakukan secara hardware, seperti halnya saat ini proteksi hardware DVD, tetapi kita ketahui banyak data *digital* saat ini tidak dapat diproteksi secara hardware (seperti dengan adanya Internet) atau dengan kata lain tidak

memungkinkan dengan adanya proteksi secara hardware.

Gambar 1 Citra asli

Gambar 2 Citra yang telah dihapus labelnya

Maka, diperlukan cara untuk melabeli citra terkait solusi pelanggaran hak cipta ini. Sifat-sifat yang dibutuhkan antara lain :

- ***Invisible atau inaudible***
  Tidak tampak (untuk data *digital* seperti citra, video, text) atau tidak kedengaran (untuk jenis audio) oleh pihak lain denganmenggunakan panca indera kita (dalam hal ini terutama mata dan telinga manusia).

- ***Robustness***
  Tidak mudah dihapus/diubah secara langsung oleh pihak yang tidak bertanggung jawab, dan tidak mudah terhapus/terubah dengan adanya proses pengolahan sinyal *digital*, seperti kompresi, filter, pemotongan dan sebagainya.

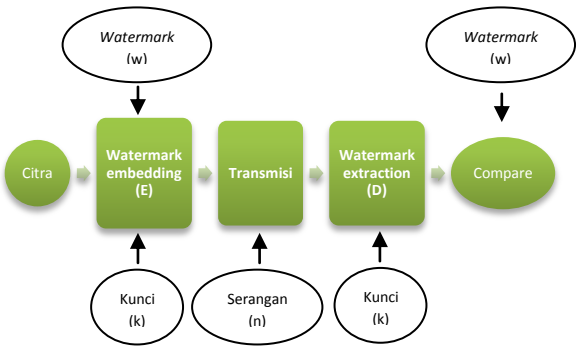
- ***Trackable***
  Tidak menghambat proses penduplikasian tetapi penyebaran data *digital* tersebut tetap dapat dikendalikan dan diketahui.

Watermarking sebagai metoda untuk pelabelan hak cipta dituntut memiliki berbagai kriteria (ideal) sebagai berikut agar memberikan unjuk kerja yang bagus:

- Label Hak Cipta yang unik mengandung informasi pembuatan, seperti nama, tanggal, dst, atau sebuah kode hak cipta seperti halnya ISBN (*International Standard for Book Notation*) pada buku-buku.
- Data terlabel tidak dapat diubah atau dihapus (*robustness*) secara langsung oleh orang lain atau dengan menggunakan software pengolahan sinyal sampai tingkatan tertentu.
- Pelabelan yang lebih dari satu kali dapat merusak data *digital* aslinya, supaya orang lain tidak dapat melakukan pelabelan berulang terhadap data yang telah dilabel.

2.3. Proses *Watermarking*

Skema *watermarking* pada citra dapat digambarkan melalui bagan di bawah ini :



Gambar 3 Proses *Watermarking*

Bagan tersebut menunjukkan skema dalam sebuah proses penyisipan *watermark* pada citra *digital* sekaligus pengujian ekstraksi *watemark*. Terlihat bahwa terjadi serangan pada sebuah citra, kemudian *watermark* diekstraksi. Dari hasil ekstraksi *watermark* inilah nantinya akan diketahui apakah citra tersebut telah dimanipulasi. Jika memang citra tersebut telah dimanipulasi oleh pihak-pihak tertentu, maka *watermark* yang diekstraksi akan rusak. Dalam *watermarking*, terdapat dua proses yang cukup penting, yaitu enkripsi dan dekripsi. Enkripsi dalam hal ini berarti proses penyisipan pesan atau informasi ke dalam suatu citra *digital*.

Sistem *watermarking* terdiri 3 komponen yang membentuknya yaitu:
i) Penghasil label *watermark*.
ii) Proses penyembunyian label

iii) Menghasilkan kembali label *watermark* dari data yang sudah diberi *watermark*.

Kajian *watermark* mengkhususkan pada isu-isu berikut ini :

i) Label *Watermark*
Label harus panjang atau hanya memberitahu ada tidaknya *watermark* pada data *digital* yang ter-*watermark*. Maksudnya bila label yang panjang, maka kita dapat mendapatkan informasi tambahan dari data yang ter*watermark* tersebut, sedangkan sebaliknya hanya diperoleh ada tidaknya (ada atau tidak saja) *watermark* dalam data ter-*watermark*.

ii) Ekstraksi atau Verifikasi
Cara menghasilkan kembali (ekstrasi atau verifikasi) label *watermark* tersebut apakah diperlukan data *digital* aslinya, atau tidak. Dari hasil penelitian memberikan hasil bahwa verifikasi dengan menggunakan data aslinya akan memberikan performansi yang lebih baik dibandingkan dengan cara yang tanpa menggunakan data asli. Dan cara ini dapat digunakan untuk menangani masalah pengakuan kepemilikan oleh beberapa orang.

2.4. Metode *Watermarking* Citra *Digital*

Teknik penyisipan *watermark* ke dalam sebuah citra dapat dibedakan berdasarkan ranah penyisipannya, yaitu :

- **Ranah spasial**
  Penyisipan *watermark* dilakukan dengan melakukan pengubahan bit-bit data secara langsung pada data spasial citra penampungnya. Contohnya adalah penyisipan *watermark* pada LSB (*Least Significant Bit*).

- **Ranah frekuensi**
  Penyisipan *watermark* dilakukan dengan cara melakukan transformasi pada data penampung, kemudian perubahan dilakukan terhadap koefisien transformasinya. Contohnya adalah penyisipan *watermark* di ranah frekuensi dengan terlebih dahulu melakukan transformasi DCT (*Discrete Cosine Transform*).

- **Ranah *feature***
  Penyisipan *watermark* dilakukan dengan menggunakan *feature point extraction* untuk menentukan daerah yang akan disisipi *watermark*. Metode ini termasuk metode baru di bidang *watermarking*. Namun, penyisipan *watermark* tetap dilakukan pada ranah spasial dan ranah frekuensi.

Pada makalah ini, yang akan dibahas ialah metode *Mean-removed quantification*, yaitu metode *watermarking digital* berbasis kuantifikasi. Metode ini merupakan teknik *watermarking* citra *digital* berdasarkan ranah frekuensi.

3. Algoritma Berbasis *Vector Quantification*

Pada awalnya, tujuan dari teknik kuantisasi warna adalah untuk menyediakan detail citra yang berbeda untuk *display device* yang berbeda yang memiliki *frame buffer* yang terbatas. Operasi utama teknik kuantisasi warna terletak pada prosedur pendesainan palet dan prosedur pemetaan piksel. Tugas dari prosedur pendesainan palet adalah untuk memilih warna-warna representatif untuk citra-citra tertentu. Secara umum, setiap warna-warna representatif terpilih mengandung tiga dimensi untuk mode warna Red-Green-Blue (RGB) yang bisa dianggap sebagai kata-kata kode pada sebuah buku kode, dimana palet merupakan buku kodenya. Pendesainan palet ini membutuhkan sebuah algoritma khusus yang bertujuan untuk memilih warna representatif yang paling baik dengan sedikit biaya komputasi dan seminimal mungkin distorsi.

Setelah desain palet warna selesai, pemetaan piksel dari citra dilakukan. Tujuan pemetaan piksel ini adalah untuk menemukan warna yang sesuai yang paling dekat dari palet untuk merepresentasikan piksel dari suatu citra dengan menimbulkan seminimal mungkin distorsi warna. Setiap piksel pada citra berwarna asli dipetakan ke warna terdekat yang ada di palet.

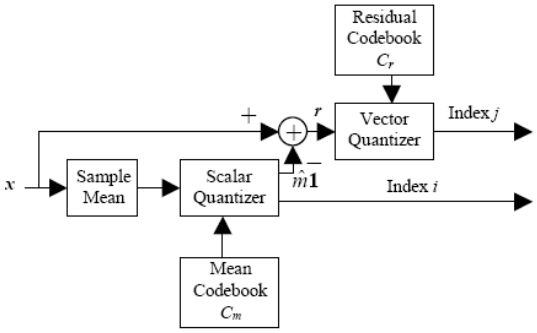
3.1. *Mean-removed Vector Quantization*

Algoritma ini merupakan salah satu pendekatan pada basis *vector*

quantization, diperkenalkan pada tahun 2006 oleh Zhe-Ming Lu dan Wei-Min Zheng. Konsepnya sama dengan algorima kuantisasi lainnya, hanya perbedaannya secara khusus pada proses encoding dan decoding akan dibahas lebih lanjut di bawah.

Terkadang, kita berhadapan pada vektor yang menghasilkan statistik nol. Hal ini berarti nilai yang diekspektasi setiap komponen adalah nol. Meskipun demikian, banyak vektor seperti gambar sampel intensitas rasters hanya memiliki komponen non-negatif dan dengan demikian tidak memiliki rata-rata nol.

Secara umum, proses algoritma kuantifikasi dalam pelabelan *watermark* ini dapat dijelaskan melalui gambar berikut

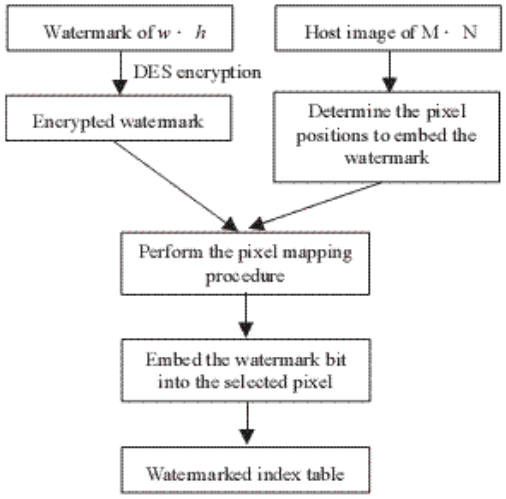


Gambar 4 Proses *Encoding* pada Algoritma MVQ

Metode MVQ pada intinya sama dengan metode algoritma berbasis kuantisasi umum, yaitu dengan menggunakan codebook yang menyimpan properti indeks kunci yang akan ditempel pada citra. MVQ menggabungkan dua buah watermark, yaitu *fragile* dan *robust*. Kuantisasi rata-rata skalar (nonvektor) dilihat sebagai vektor kuantisasi rata-rata. Pembentukan kunci sendiri disimpan dalam bentuk mean vector, yaitu dengan melihat suatu objek gambar sebagai rangkaian *chain code* vektor. *Mean vector* diartikan sebagai kode kunci yang akan ditempel pada citra. Semua komponen *mean vector* di-*assign* dengan nilainya pada indeks *codebook*.

Watermark asli pertama kali diproses melalui permutasi dengan kunci awal untuk kemudian dilakukan permutasi lagi pada *watermark* yang ditempel. Dengan kata lain, dapat digunakan jaringan *feistel* untuk memperkuat algoritma MVQ.. Proses ini merupakan proses encoding algoritma MVQ secara *robust* (di awal telah dijelaskan bahwa pendekatan yang cocok untuk melindungki HAKI ialah *robust*, bukan algoritma *fragile*).

3.2. *Proses* Penyisipan dan Ekstraksi *Watermark*



Gambar 5 Penyisipan *Watermark*

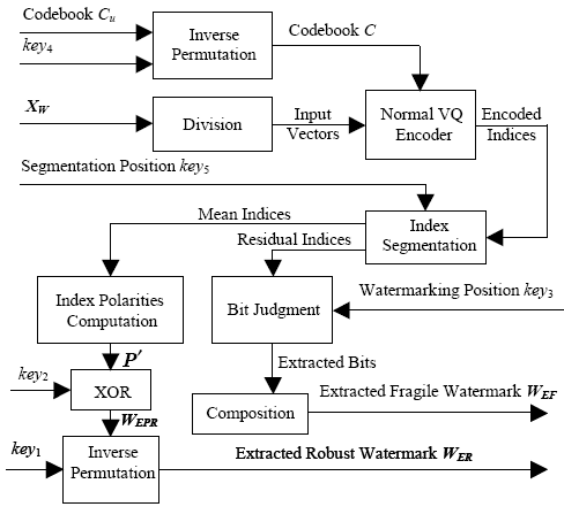
Sebuah citra yang akan disisipi *watermark* (host image) H adalah sebuah citra berwarna RGB berukuran *M* x *N* piksel, dimana H = (h1,h2,...,hMxN). *Watermark* W adalah sebuah citra biner yang terdiri dari *w* x *h* bit, dimana W = (w1,w2,...,wwxh) dan Wi ϵ (0,1). Palet dengan pilihan optimal yang digunakan dapat di-*generate* langsung oleh program-program pengolah grafis seperti Adobe Photoshop.

Setelah melakukan pendesainan palet, prosedur yang akan dilakukan kemudian adalah melakukan pemetaan piksel untuk mengkuantisasi warna. Ketika prosedur pemetaan ini dilakukan, pada saat inilah proses penyisipan *watermark* juga dilakukan. Untuk keamanan, bit-bit *watermark* yang akan disisipkan akan terlebih dahulu dienkripsi dengan prosedur DES, sebelum *watermark* benar-benar disisipkan. Sebagai tambahan, sebuah *pseudorandom number generator* (PRNG) digunakan untuk menentukan posisi-posisi

piksel yang akan dipergunakan untuk menyisipkan bit-bit *watermark* tadi.

Pada skema diatas, bit-bit *watermark* disisipkan ke dalam tabel index warna, dimana ukuran dari tabel index tidak dimodifikasi. Selain itu, penggunaan prosedur enkripsi DES dan PRNG akan meningkatkan keamanan dari skema *watermarking* ini.

Sedangkan untuk proses ekstraksinya, skemanya ialah sebagai berikut



Gambar 6 Proses Ekstraksi dengan MVQ

Pada proses ekstraksi, digunakan codebook yang sama dengan pada proses encoding. Bagaimana cara untuk mempartisi keseluruhan indeks menjadi indeks rata-rata sebagai kunci rahasia ialah dengan mempublikasikan codebook yang telah dikenai proses permutasi pada pengguna. Proses ekstraksi dapat dilakukan tanpa host image (citra awal).

Langkah-langkah yang dilakukan ialah :

- Melakukan invers permutasi pada kunci terakhir pada codebook C' untuk memperoleh perkalian codebook C.
- Citra yang telah dikenai *watermark* dibagi menjadi blok atau vektor.
- Encoder VQ generik melakukan pencarian codeword dengan metode nearet neighbor pada seluruh vektor masukan untuk memperoleh keseluruhan indeks ter-*encode*.
- Membagi *watermark robust* dan *fragile* untuk diekstrak.
- Menghitung polaritas P dari indeks-indeks rata-rata dan melakukan operasi XOR antara P dengan kunci$_2$ untuk memperoleh *watermark* terekstraksi.
- Melakukan invers permutasi dengan kunci$_1$ untuk memperoleh *watermark* awal.

4. Pengujian Algoritma MVQ

Berikut ini merupakan objek citra awal dan citra yang ingin disisipkan. Citra yang akan disisipkan terbagi 2, yaitu citra kuat (*robust*) dan lemah (*fragile*).

Gambar 8 Citra Asli / *Host Image* (kiri) dan Citra Sisipan (kanan)

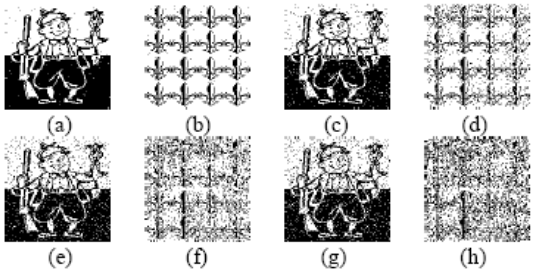
Citra asli yang dikenakan penyisipan *watermark*

Gambar 7 *Watermark robust* (kiri) dan *Watermark Fragile* (kanan)

menjadi seperti di bawah ini :
Pada citra dengan penyisipan *watermark robust* maupun *watermark fragile* dapat dikenai serangan. Serangan pertama adalah kompresi gambar, hasil ekstraksinya akan menjadi :

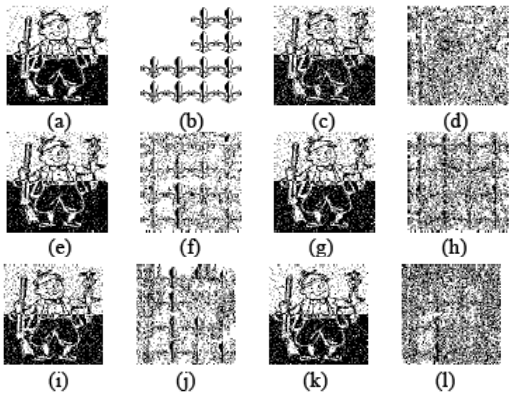
Gambar 9 Ekstraksi Watermark robust (kiri) dan fragile (kanan)

Untuk ukuran kompresi gambar yang semakin besar, akan menyebabkan gambar semakin "pecah". Hasil ekstraksi untuk berbagai tingkat kompresi ini dapat dilihat sebagai berikut



Gambar 10 Tingkat kompresi 0.99 (a,b), 0.94 (c,d), 0.83 (e,f), 0.45 (g,h)

Serangan lainnya yang dapat mempengaruhi penyisipan watermark ialah pemotongan gambar (cropping), filter median, pengaburan (blur), penajaman (sharpen), kontras, noise, dan sebagainya. Untuk proses operasi ini, dapat dilihat pengujiannya pada gambar di bawah :



5. Kesimpulan

Salah satu pendekatany ang dapat digunakan untuk melindungi hak-hak cipta pada suatu media digital yaitu dengan penyisipan *watermark*. Makalah ini membahas salah satu contoh watermarking pada citra/gambar yang berbasiskan teknik vektor kuantisasi , yaitu warna citra asli akan dipetakan pada suatu palet sehingga warna yang akan ditampilkan nantinya adalah warna dari palet yang paling dekat menyerupai warna aslinya.

Sejauh ini, MVQ merupakan salah satu metode berbasis vektor kuantisasi yang efisien dan tahan terhadap berbagai serangan. Algoritma ini lebih murah dari segi komputasi dibandingkan algoritma pada ranah lainnya, seperti LSB.

6. Daftar Pustaka

[1] Lu, Zhe-Ming; Wei-Min Zheng; Jen-Shyang Pan. 2006. *Multipurpose Image Watermarking Method Based on Mean-removed Vector Quantization*. *Journal of Information Assurance and Security*, vol. 1, p.33-42. China : Harbin Institute of Technology Shenzhen Graduate School, Visual Information Analysis and Processing Research Center.

[2] Munir, Rinaldi. 2004. *Bahan Kuliah IF3054, Steganografi dan Watermarking*. Bandung : Departemen Teknik Informatika, Institut Teknologi Bandung.

[3] Supangkat, Suhono; Kuspriyanto; Juanda. 2000. *Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital*. Bandung : Departemen Teknik Elektro, Institut Teknologi Bandung.