Pengembangan Metode Difference Expansion pada Data Hiding dengan Fungsi Modulo

YOGI KURNIAWAN
5114201028

Dibimbing Oleh
Dr. Tohari Ahmad, S.Kom, MIT.

Publikasi yang Dihasilkan

1. Jurnal Defense science (Hiding Secret Data by using Modulo Function in Quad Difference Expansion, Defence Science Journal) -> submitted / proses review, indeks Scopus
2. Draft paper untuk di-submit (kemungkinan ke 2016 IEEE International Conference on Knowledge Engineering and Applications - Singapore), indeks IEEE/Scopus

Latar Belakang

- Salah satu cara melindungi informasi digital dengan melakukan penyembunyian data.
- Steganography merupakan cabang penyembunyian data (Tang, Hu, Song, & Zeng, 2015)
- Ekstraksi sebuah pesan dapat menghancurkan cover media, akan tetapi tidak boleh pada dunia kesehatan, militer, dan hukum

Latar Belakang

- Pada Tahun 2003 Tian mengusulkan metode Difference Expansion(DE)
- Metode ini menyembunyikan pesan pada perbedaan pixel yang bertetangga
- Tahun 2004 diperbaiki oleh Alatar dengan menggeneralisir sebagai integer dan membuat menjadi blok

	1	2	3
1	162	162	162
2	162	162	162
3	162	162	162
4	162	162	162
5	162	162	162

	1	2	3
1	162	162	162
2	162	162	162
3	162	162	162
4	162	162	162
5	162	162	162

Latar Belakang

- Kelemahan dari metode DE adalah
  - $\tilde{V} = 2x\ v + b$
  - Expansi 2 kali dari perbedaan
- Diperbaiki oleh Lou, Hu dan Liu 2009 dengan mengecilkan perbedaan akan tetapi tetap melakukan expansi perbedaan 2 kali
  - $V_N - 2^{\lfloor \log V_N \rfloor - 1}$
- Diperbaiki oleh Holil & Ahmad pada 2014 dengan mengintegrasikan metode Alatar dan Lou, Hu dan Liu

Usulan

- Metode yang diusulkan adalah
  - Merubah metode expansi pada DE dengan fungsi modulo 3 pada perbedaan tiap pasang pixel yang bertetangga
  - Modulo 3 dipilih karena perubahan yang akan terjadi hanya +2,-2, atau tidak dilakukan perubahan.

Rumusan Masalah

- Bagaimana metode penyisipan pesan rahasia menggunakan fungsi modulus pada perbedaan nilai *pixel* dan titik referensi?
- Bagaimana pengaruh fungsi modulo dalam penyembunyian data dengan *diference expansion*

Tujuan

- Melakukan penyisipan informasi dengan fungsi modulus pada sebuah citra digital
- Menyimpan informasi yang dibutuhkan pada saat proses ekstraksi informasi.
- Mendapatkan informasi dan mengembalikan citra dari hasil ekstraksi pada citra yang telah dilakukan penyisipan informasi
- Mengamankan *location map* dalam proses pengiriman.
- Menguji metode yang diusulkan untuk mengetahui peforma dengan dibandingkan dengan metode yang sudah ada sebelumnya.

Batasan Masalah

- *Cover* media yang digunakan adalah berupa citra digital
- Data citra digital yang digunakan berupa data set citra testing standar *greyscale* dan RGB dengan ukuran 512x512 *pixel* (California 2015)
- Data citra digital yang digunakan berupa data set citra x-ray medis RGB yang diambil dari (Library 2015)
- Informasi yang disisipkan berupa teks pengisi standar "lorem ipsum"
- Pada proses pengamanan *Location map,* nilai *Initialization Vector* (IV) dan bilangan prima (p) dan *prime root primitive* (g) merupakan kesepakatan antara pengirim dan penerima
- Pengembangan metode data hiding *difference expansion* mencakup distribusi *location map*.
- Fungsi modulo yang digunakan adalah modulo 3.

Kontribusi Penelitian

- Menurunkan ekspansi perbedaan pada Reversible Data Hiding Difference Expansion dengan fungsi Modulus. Fungsi modulus digunakan untuk menggantikan metode penyipan pada Metode DE
- Metode penyimpanan *Location map* yang digunakan untuk menyimpan informasi ekstraksi akan dibagi dua, satu bagian akan disimpan pada file dan bagian lain akan disisipkan kembaali pada cover media

Diagram Alir Sistem

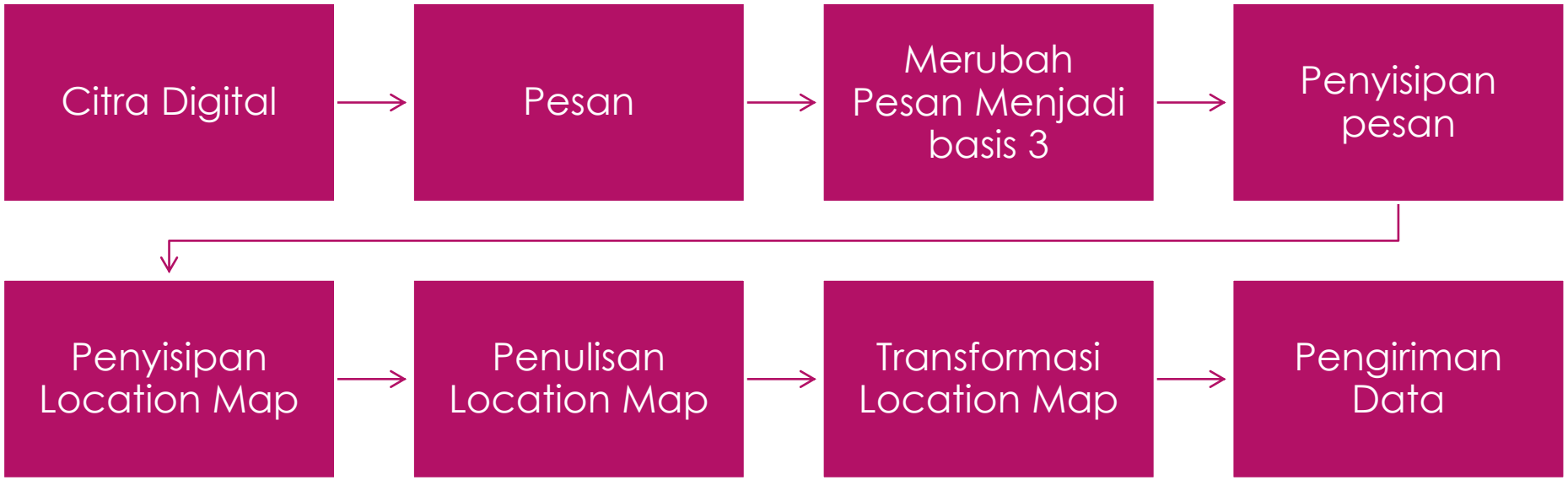
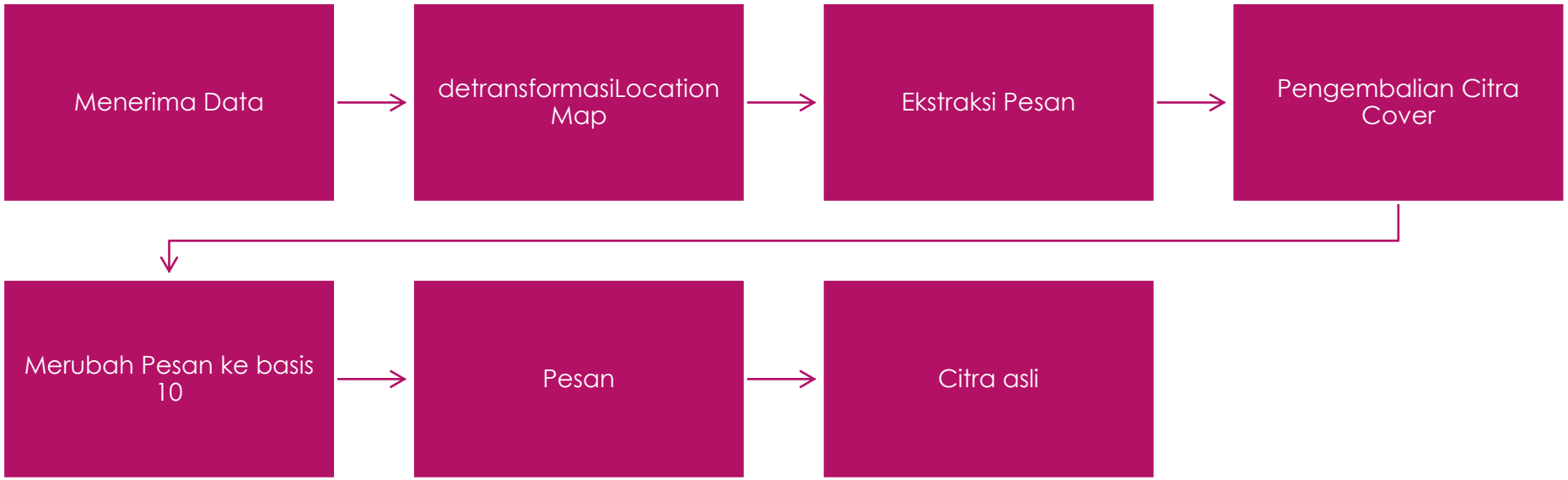


Diagram Alir Sistem



Proses Penyisipan

- Merubah pesan ke basis 3
- Mencari perbedaan dari tiap pasangan pixel
- Proses pencocokan nilai modulo 3 dari perbedaan dan pesan
- Menyusun nilai pixel yang baru

U_m	U_1
U_3	U_2

$$V_n = U_n - U_m$$

$$\tilde{V}\begin{cases} Vn\ , jika\ Vn\ mod 3 = M_3 \\ Vn + 1, jika\ Vn\ mod 3 + 1 = M_3 \\ Vn - 1, jika\ Vn\ mod 3 + 2 = M_3\ dan\ d > 0 \\ Vn + 2, jika\ Vn\ mod 3 + 2 = M_3\ dan\ d = 0 \end{cases}$$

If 1<Un<254

$$\widetilde{Un} = Um + \widetilde{Vn}$$

Proses Ekstraksi

Mencari perbedaan tiap pasang

Melakukan modulo 3 dari tiap perbedaan

Merubah pesan dari basis 3 ke basis 10

$d_n = U_n - U_m$

$m_{(3)} = d_n \; mod \; 3$

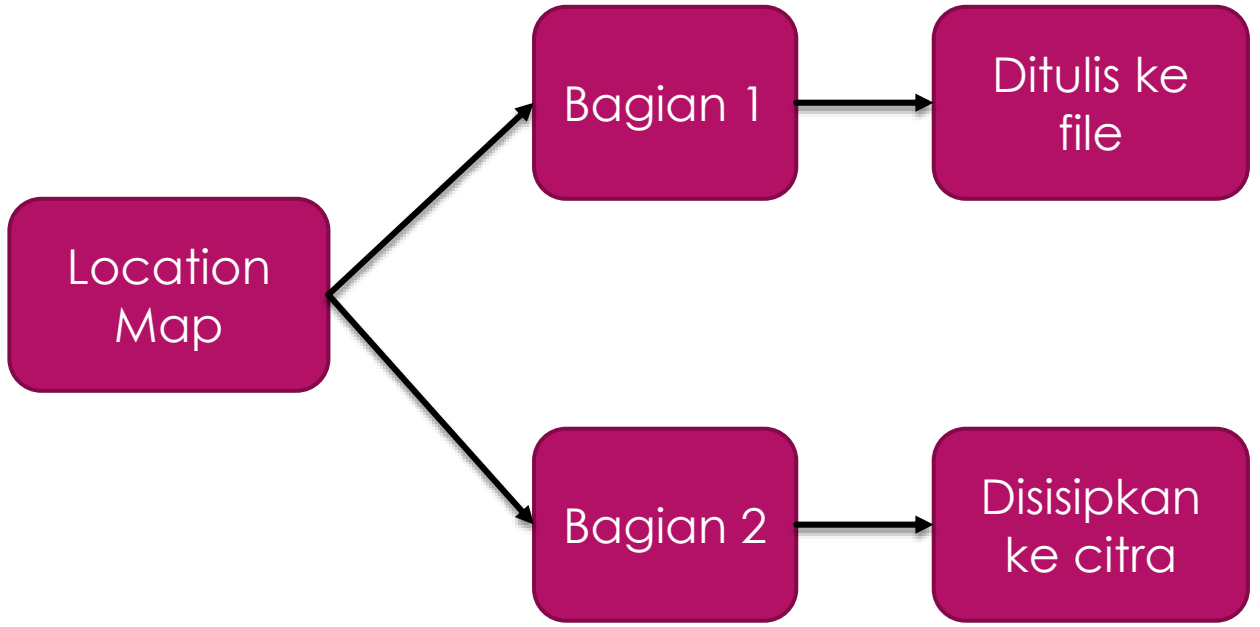
$m_{(3)} \; dirubah \; ke \; m_{(10)}$

Proses Pengembalian Cover Media

$$U_n \begin{cases} 2\ x\ \left\lfloor \frac{V}{2} \right\rfloor, jika\ nilai\ LM = 10\ dan\ ganjil \\ 2\ x\ \left\lfloor \frac{V-2}{2} \right\rfloor + 1, jika\ nilai\ LM = 10\ dan\ genap \\ 2\ x\ \left\lfloor \frac{V+2}{2} \right\rfloor, jika\ nilai\ LM = 01\ dan\ ganjil \\ 2\ x\ \left\lfloor \frac{V}{2} \right\rfloor + 1, jika\ nilai\ LM = 01\ dan\ genap \\ V-2, \quad jika\ LM = 11 \end{cases}$$

Location Map

REGION	Bagian 1	Bagian 2
Region positif	1	0
Region negatif	0	1
Region tak dirubah	0	0
Region d=0	1	1



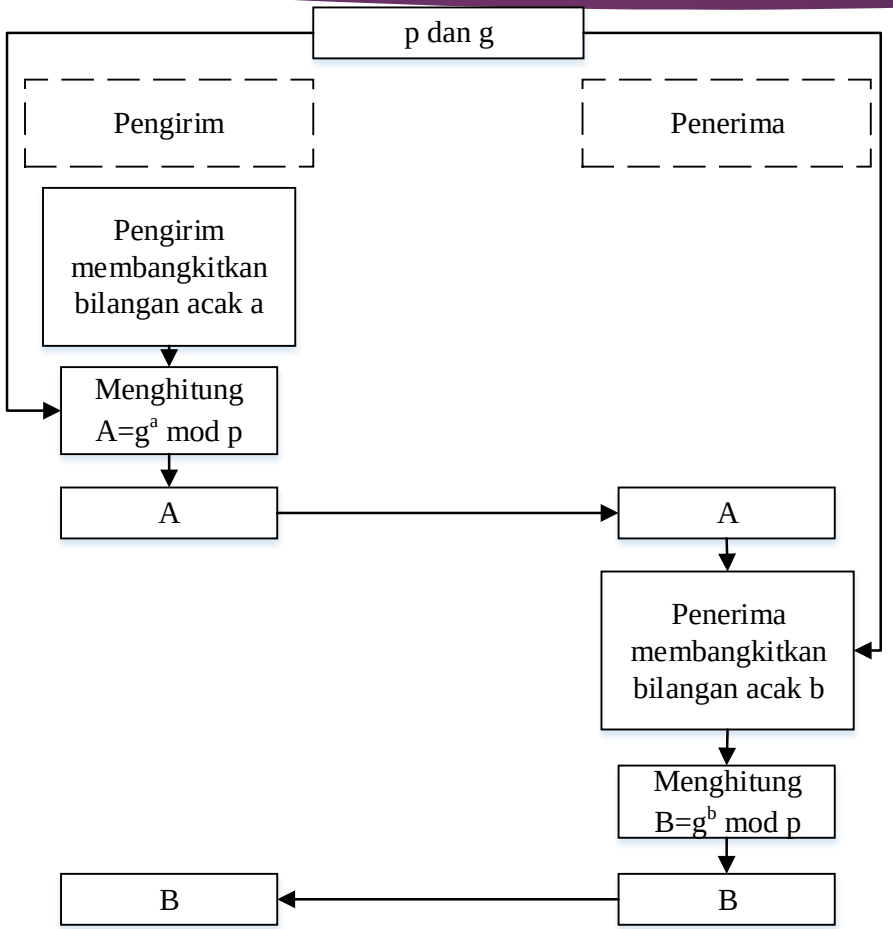
Location Map

- Pada Location Map bagian ke dua dilakukan Penyisipan dengan fungsi modulus dilakukan dengan membandingkan hasil modulo 8 dari titik referensi
- Kemudian penambahanya ikut dituliskan di berkas location map

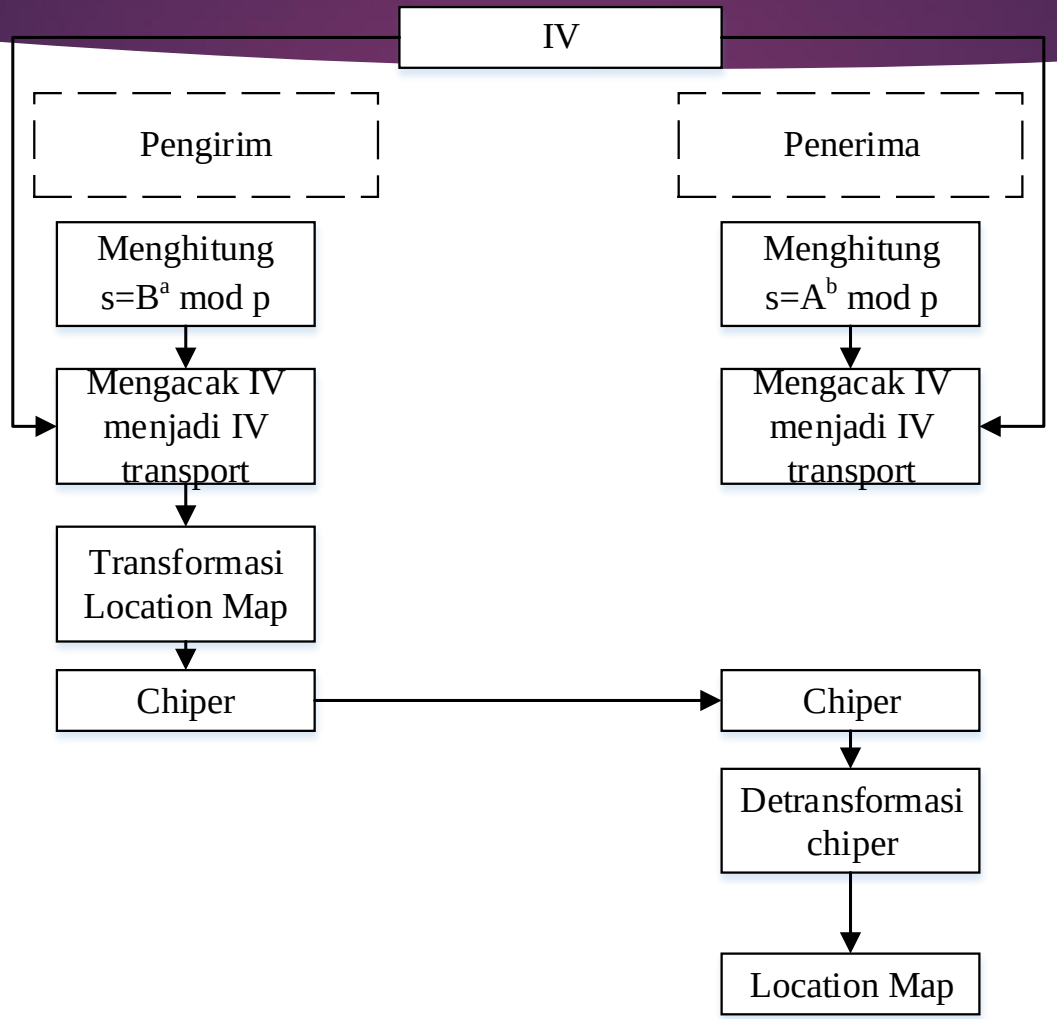
$$U_m mod\ 8 + n = LM_2$$
$$\widetilde{U_m} = U_m + n$$

lm1,penambahan lm2,operasi;#
7,2,1;6,1,0;#2,1,1;

Pengamanan Berkas Location Map



Pengamanan Berkas Location Map



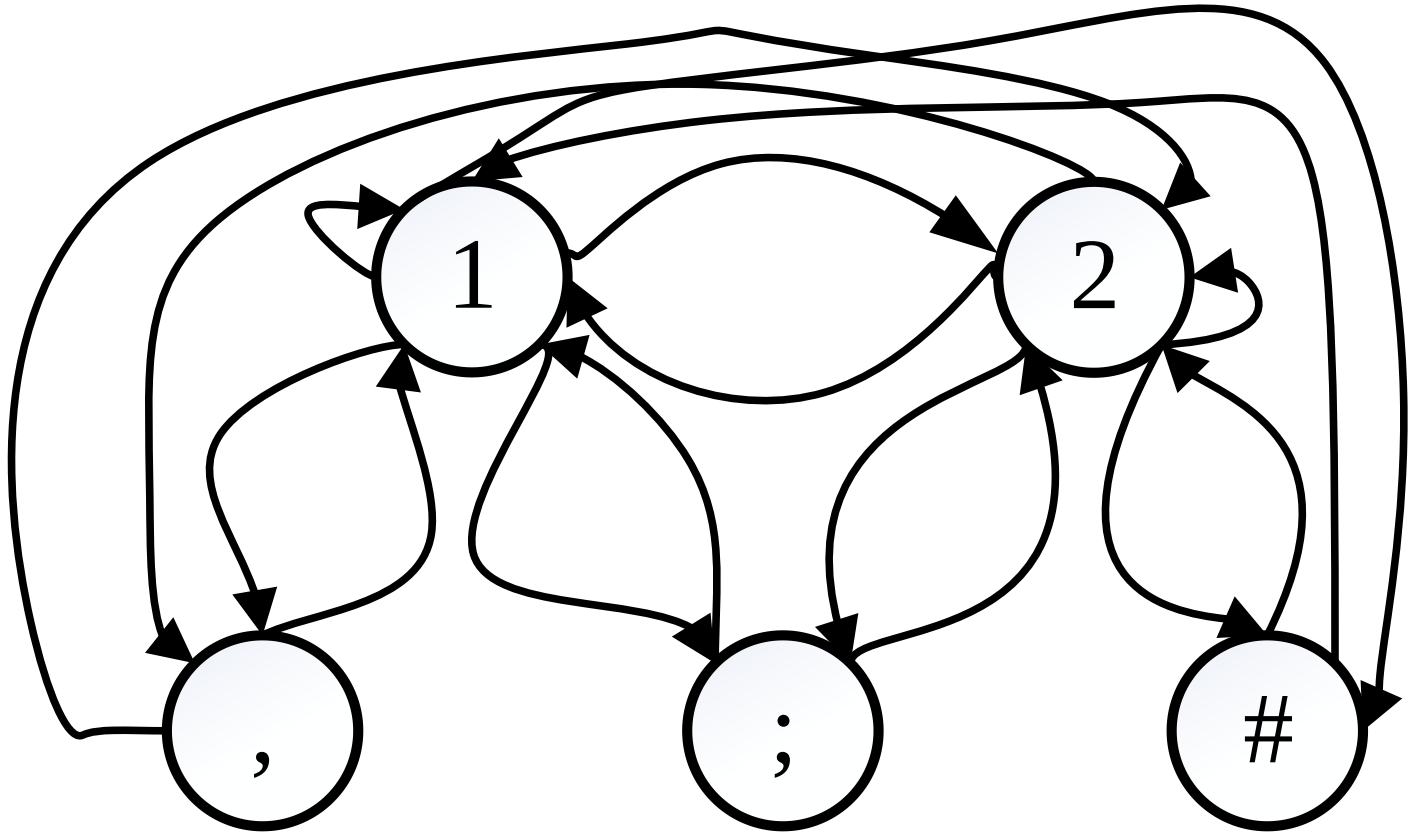
Pengamanan Berkas Location Map

```
IV=26 huruf+10 angka
I=s mod length(IV)
count=1
a=0
while count <=length(IV)
        if IV[i] telah ada pada IV'
                i=(i+1) mod length(IV)
        IV'[count]=IV[i]
        i=(i+a+s) mod length(IV)
        a++
        count++
```

Misalkan IV{1,2,3,4} dan s=2
count = 1, IV' = {2}
count = 2, IV' = {2, 3}
count = 3, IV' = {2,3,4}
count = 4, IV' = {2,3,4,1}

- Pengacakan IV menjadi IV' dan IV transport.
- IV' dibentuk dengan mengacak IV dengan bilangan B.
- IV transport dibentuk dengan mengacak IV' dengan bilangan s .

Pengamanan Berkas Location Map



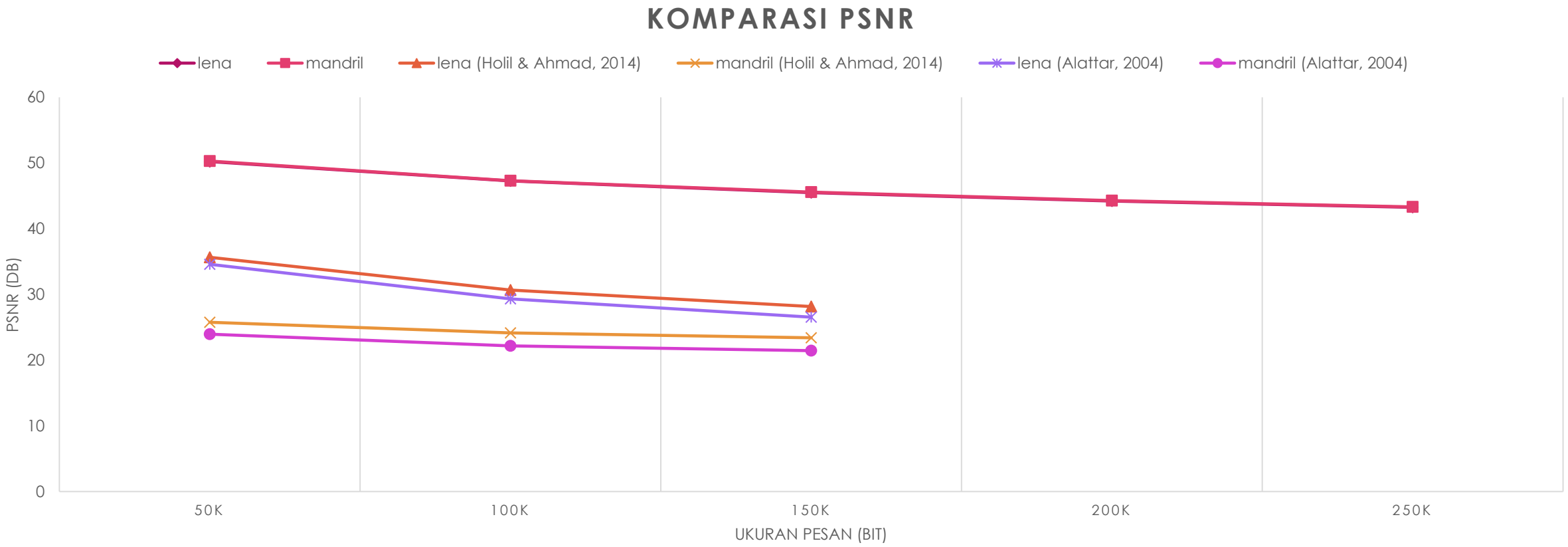
Perancangan Uji Coba

- Seluruh cover media disisipi dengan 50 ribu bit pesan kemudian disisipi 50 ribu bit kembali sampai mencapai kapasitas maksimal
- Pengukuran kualitas dengan PSNR, SSIM, dan UQI .
- Pengukuran keamanan dengan KL divergence dan chi-square attack

Hasil Penelitian

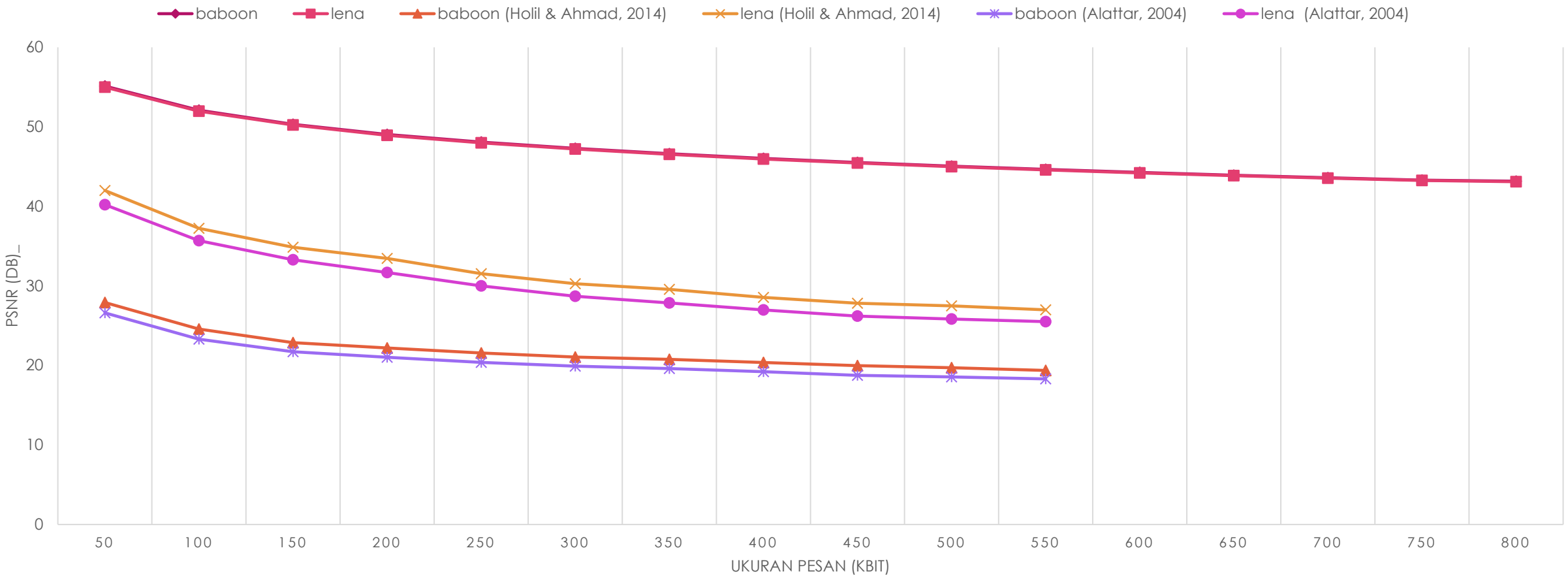
- Pengukuran kualitas pada citra greyscale
- Pengukuran kualitas pada citra RGB
- Pengukuran kemanan pada citra greyscale
- Pengukuran keamanan pada citra RGB

Pengukuran kualitas pada citra greyscale

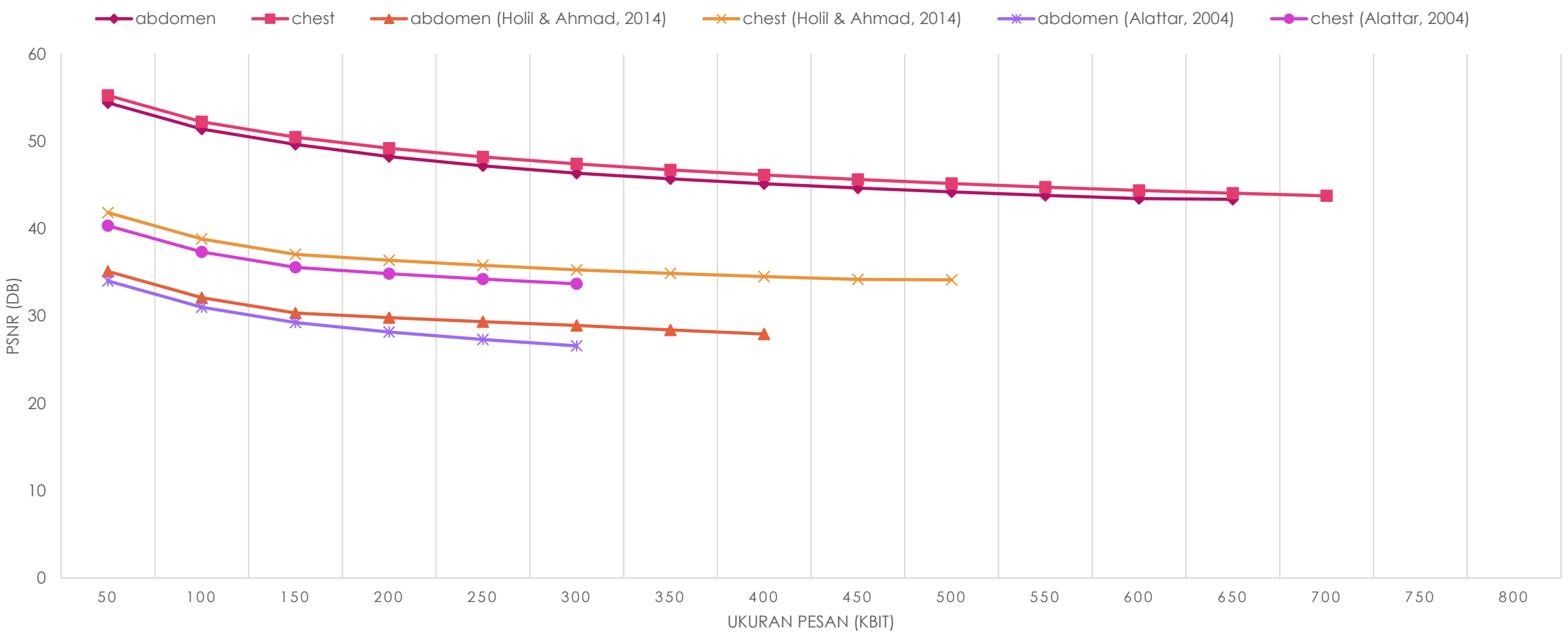


Selisih PSNR dibandingkan dengan metode sebelumny diantara 20 -16db

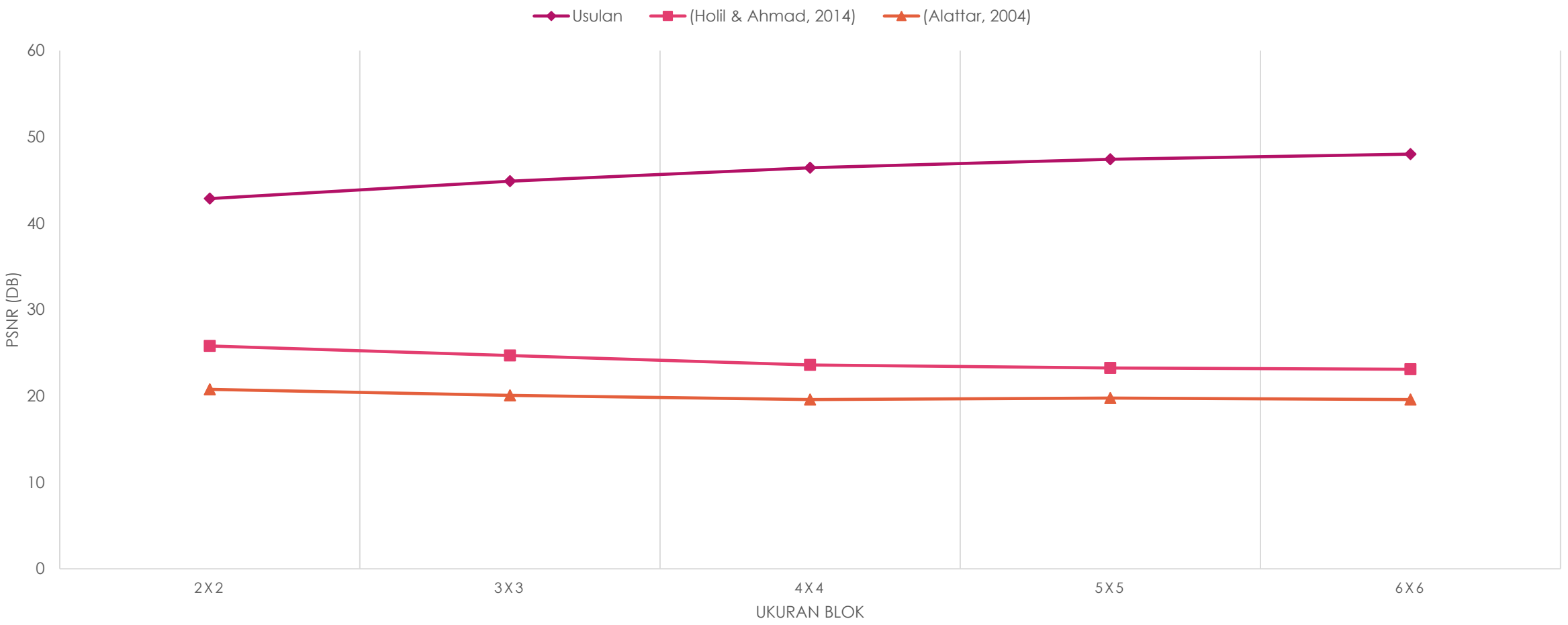
KOMPARASI PSNR



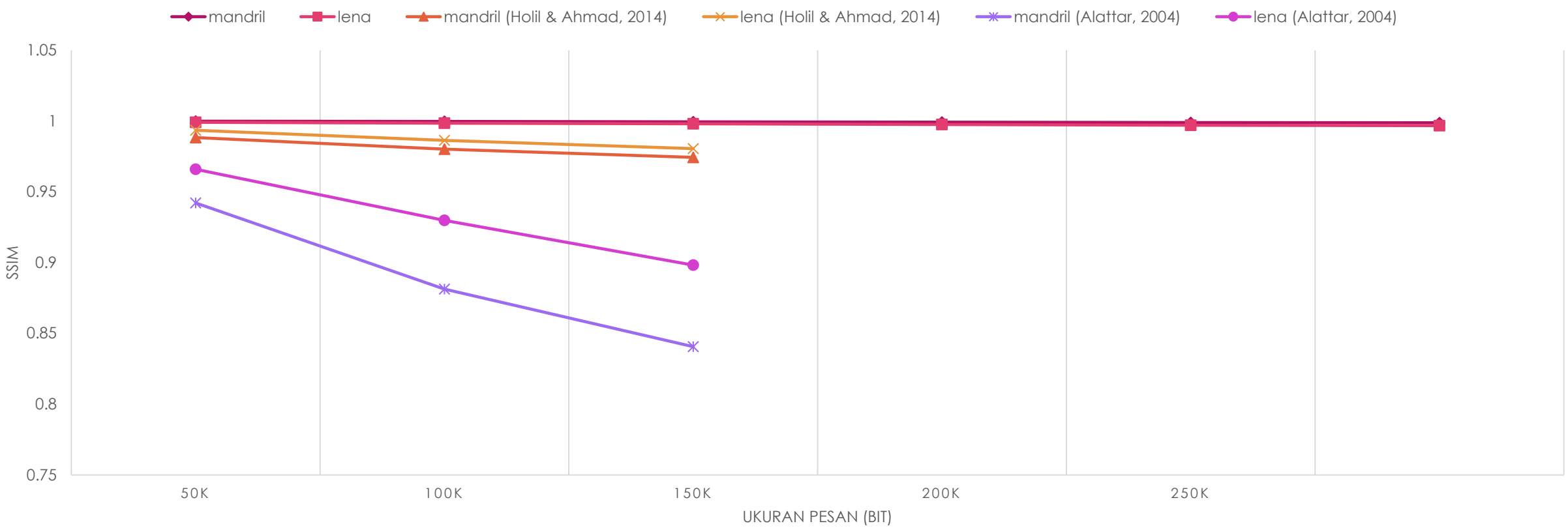
Penyisipan dilakukan dari 50Kbit sampai dengan 1050Kbit
Perbedaan PSNR dari metode yang diusulkan dan metode sebelumnya berkisar antara 28 – 24 db



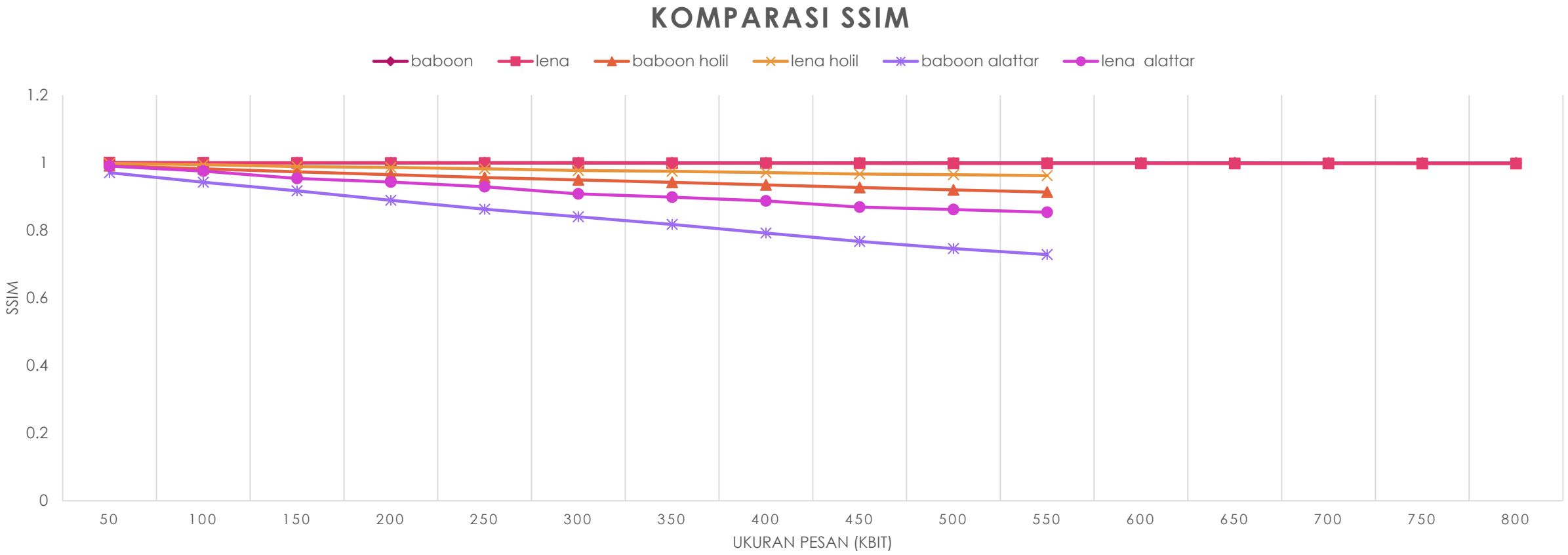
Pada citra medis hasil PSNR metode yang diusulkan mengungguli metode yang diusulkan Holil dan Ahmad dan Alattar dengan selisih 10-16 db



Pada metode yang diusulkan ketika ukuran blok diperbesar maka akan meningkatkan kualitas citra yang dihasilkan

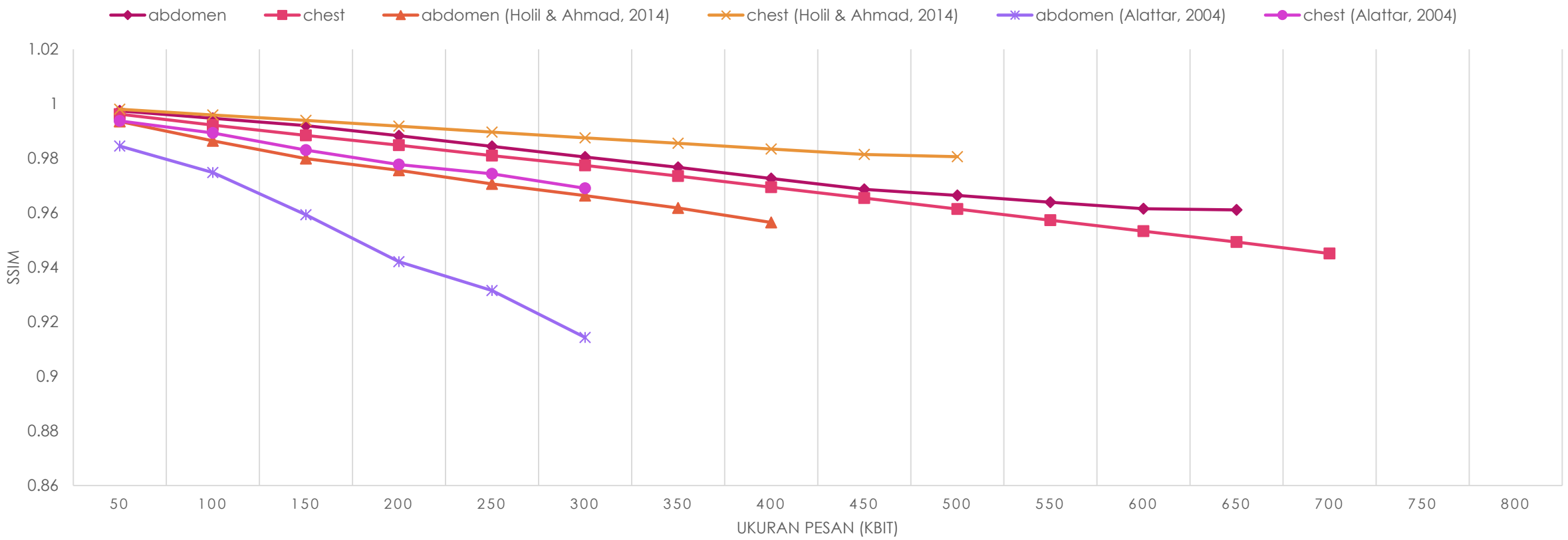


- Pada pengukuran SSIM pada citra greyscale bernilai diantara 0,9999 samapai dengan 0,9988

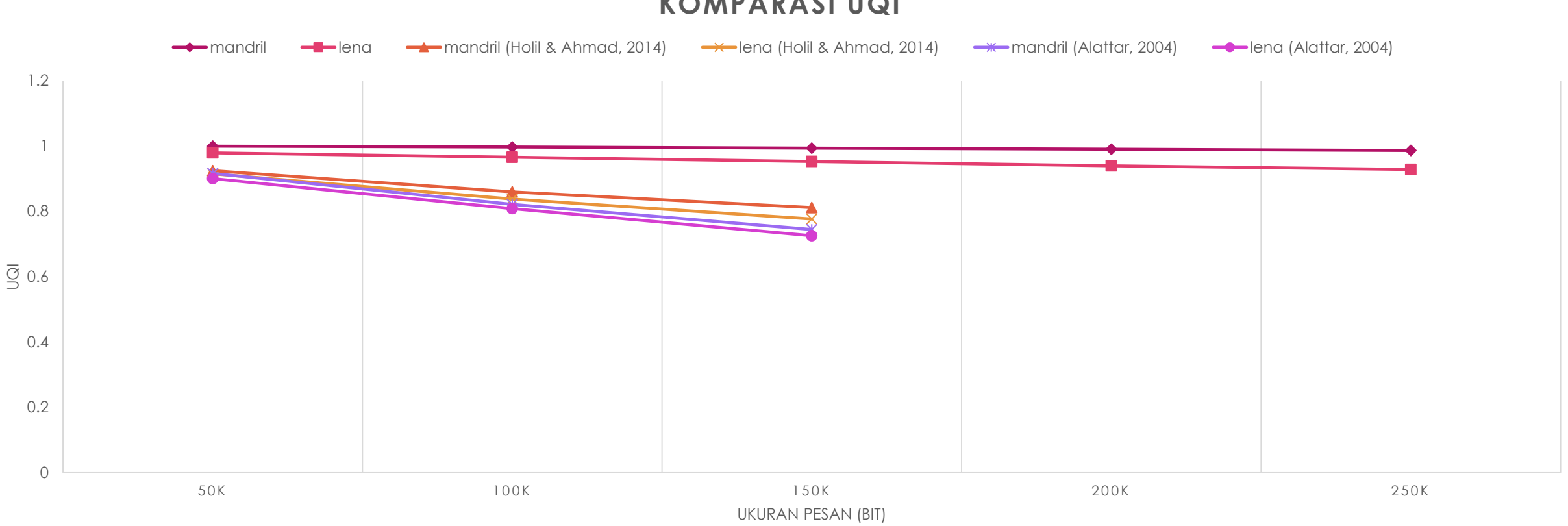


- Pada citra RGB SSIM yang dihasilkan diantara 0,9999 sampai dengan 0,9989

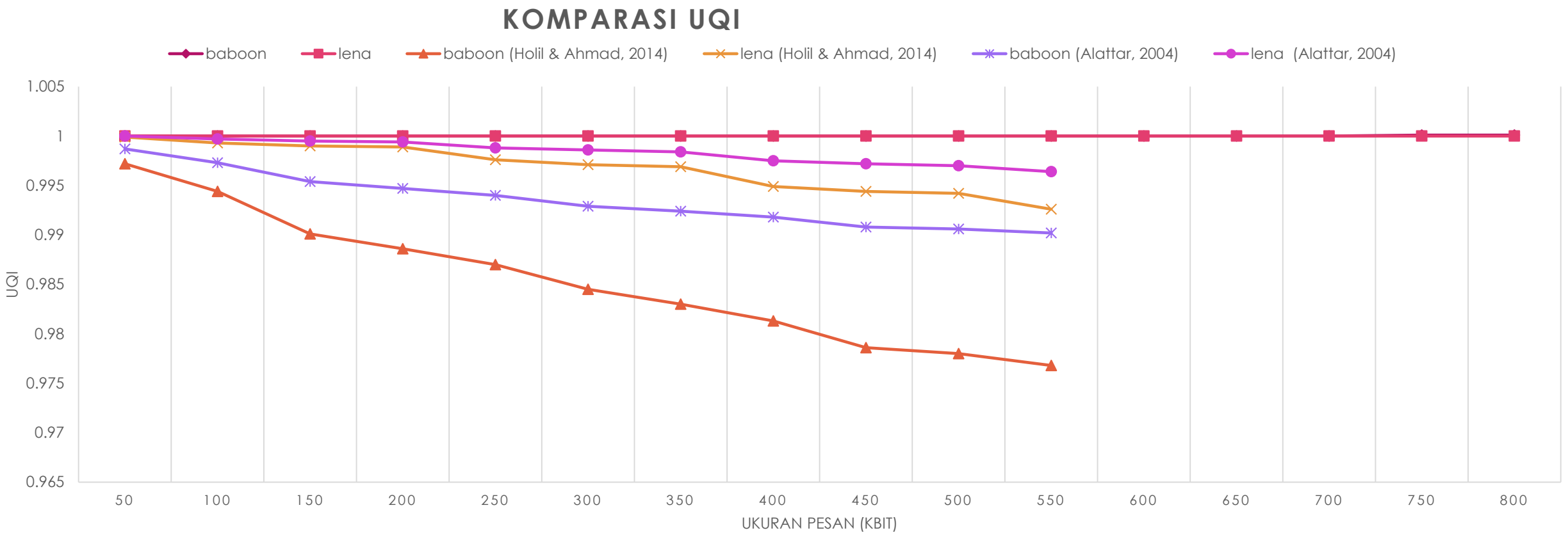
KOMPARASI SSIM PADA CITRA MEDIS



- pada metode yang diusulkan oleh (Holil & Ahmad, 2014) pada citra chest mampu mengungguli metode yang diusulkan.
- Hal ini dikarenakan banyaknya nilai *pixel* yang sama sehingga pergeseran *pixel* yang terjadi pada nilai perbedaan maksimal yaitu +2 dan -2

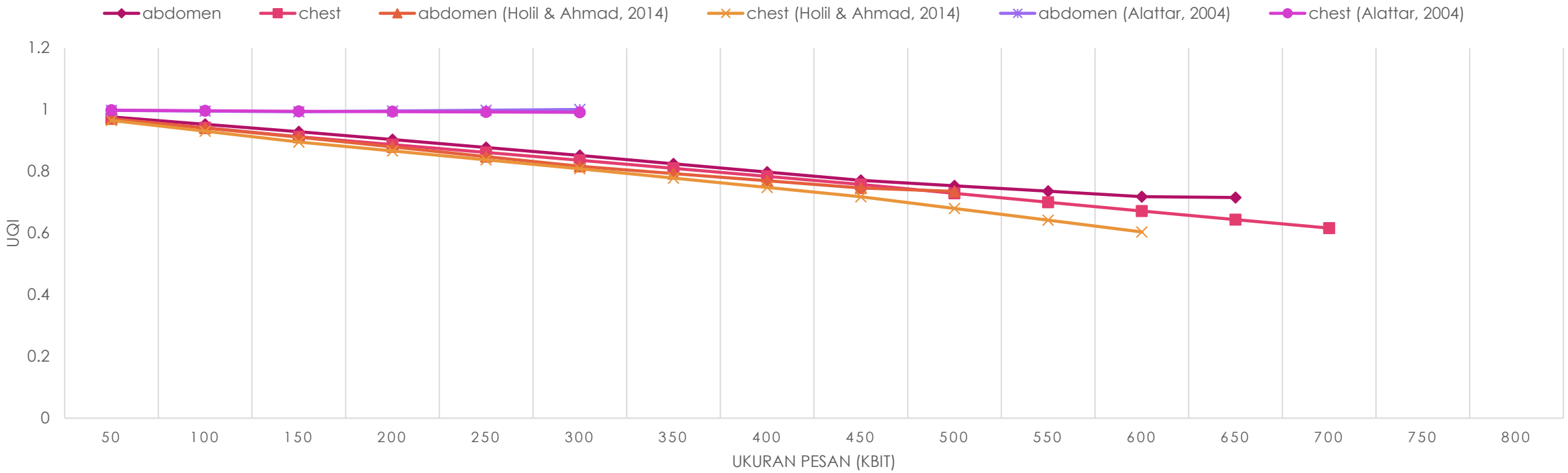


- Nilai UQI yang dihasilkan cenderung untuk mendekati nilai satu.
- Dengan nilai untuk mandril antara 0.99 sampai 0.98 dan lena diantara 0.97 dan 0.92.
- Sedangkan dua metode yang lain mengalaimi penurunan dari 0.9 ke 0.7.



- Pada metode yang diusulkan selau bernilai 1 atau dianggap sama oleh pengukuran UQI

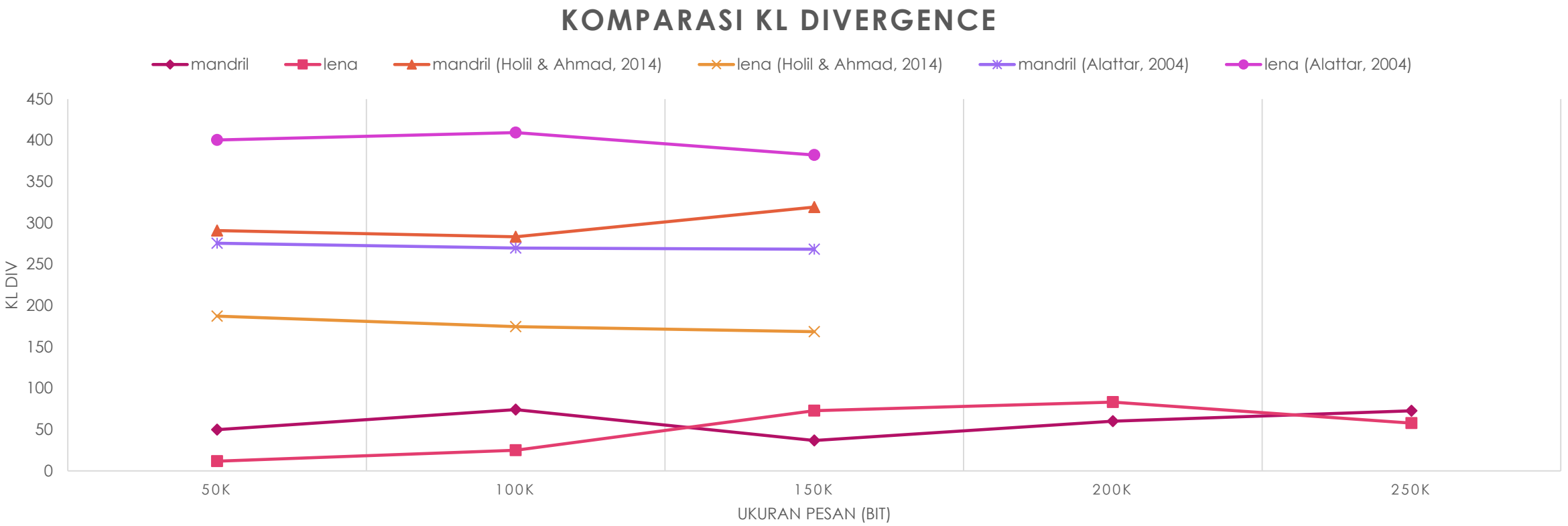
KOMPARASI UQI PADA CITRA MEDIS



- citra medis memiliki warna dasar yang hampir sama sehingga membuat banyak nilai *pixel* yang sama, hal ini berakibat pada nilai perbedaan pada nilai maksimal yaitu +2 dan -2

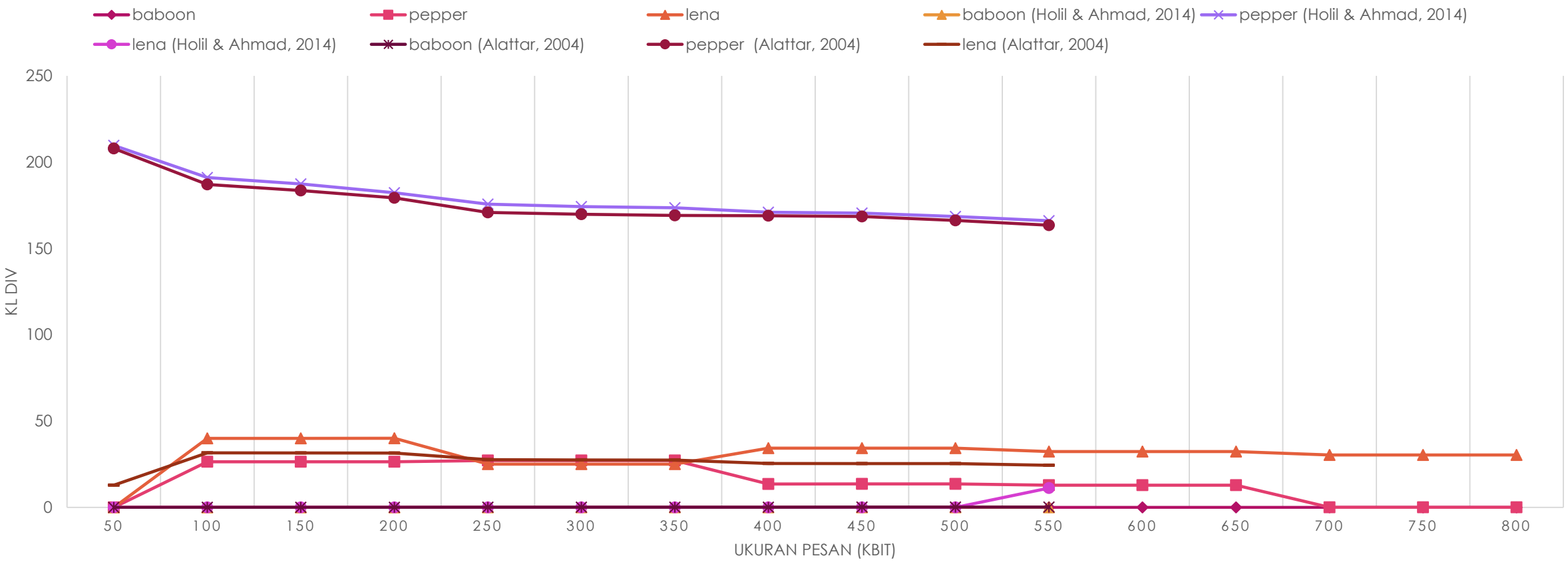
citra	Kapasitas (Alattar, 2014) (bit)	kapasitas (Holil & Ahmad, 2014) (bit)	Kapasitas Metode Usulan (bit)
lena	195250	196576	275254
mandril_gray	194602	196609	275254
pirate	194599	196543	275254
cameramen	191299	196570	275254
peppers	193087	196606	275254
jetplane	191128	196609	275254

Pengukuran Keamanan



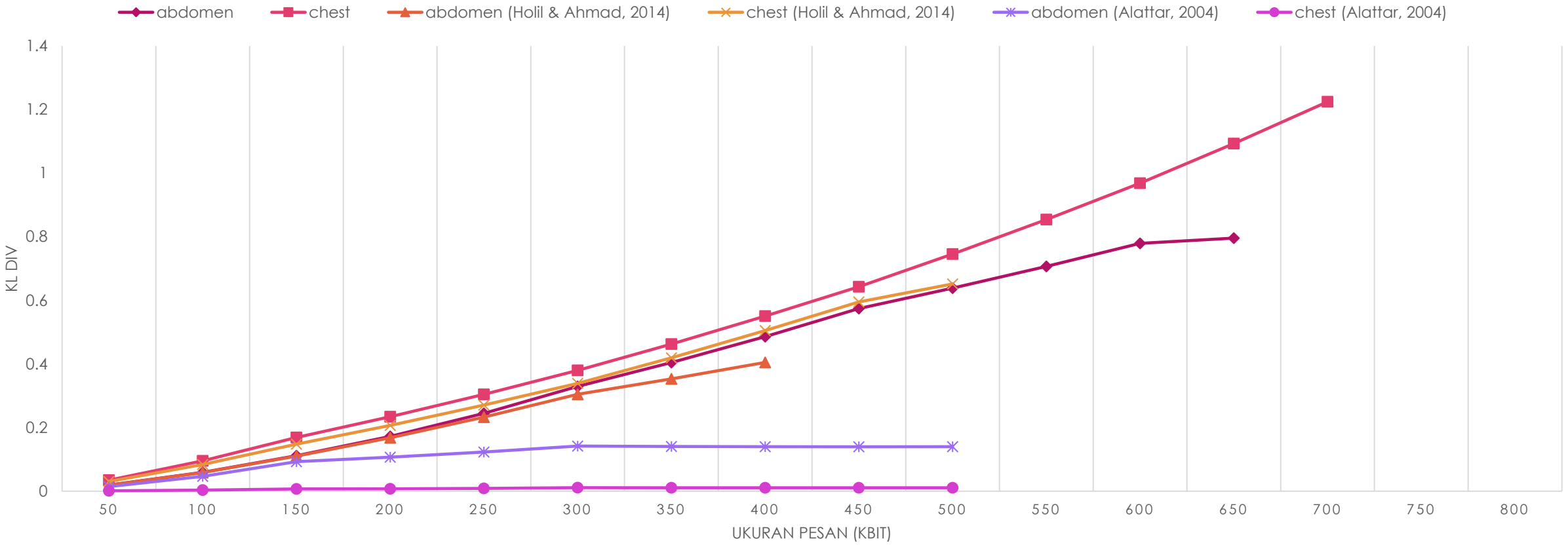
- Penyisipan dengan metode yang diusulkan selalu mempunyai nilai dibawah 100 sedangkan pada dua metode sebelumnya bernilai diatas 150

KOMPARASI KL DIVERGENCE



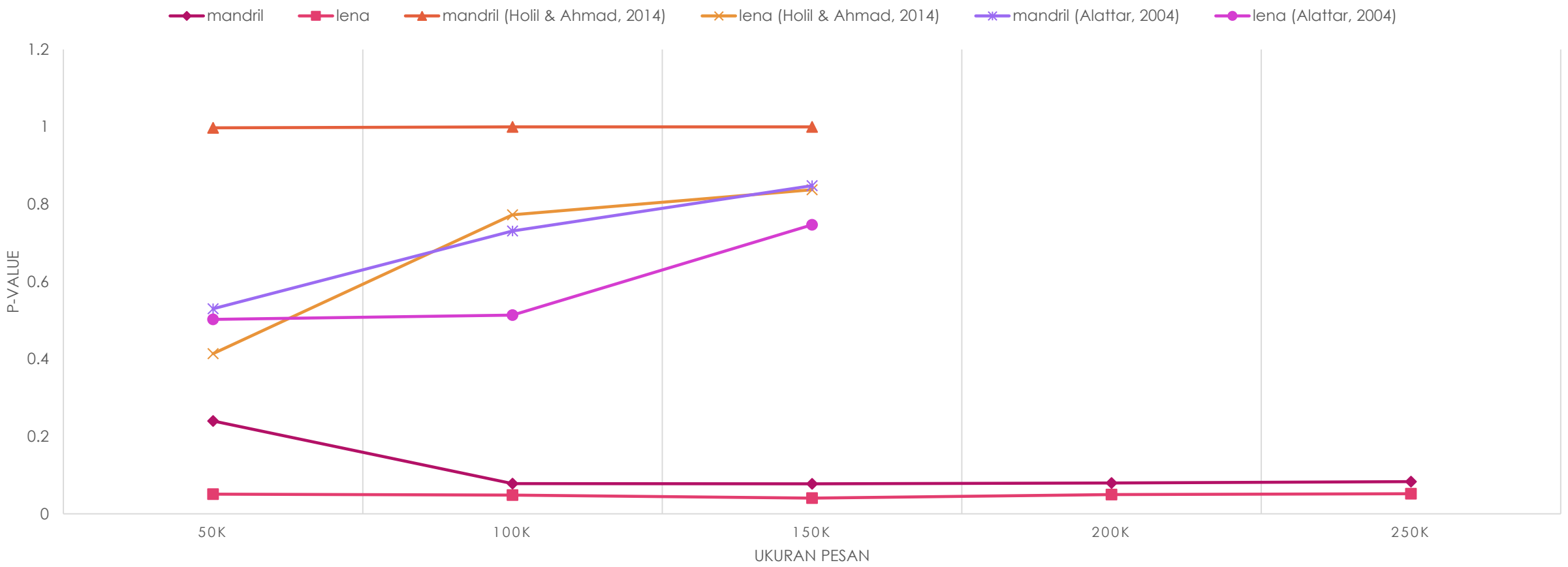
- Pada metode yang diusulkan citra baboon memiliki nilai 0,0001 sampai dengan 0.0023, sedangkan pada metode sebelumnya nilai minimalnya adalah 0.001 pada penyisipan 50Kbit.
- citra lena terdapat beberapa nilai *pixel* yang memiliki jumlah jauh diatas nilai aslinya.

KOMPARASI KL DIVERGENCE PADA CITRA MEDIS



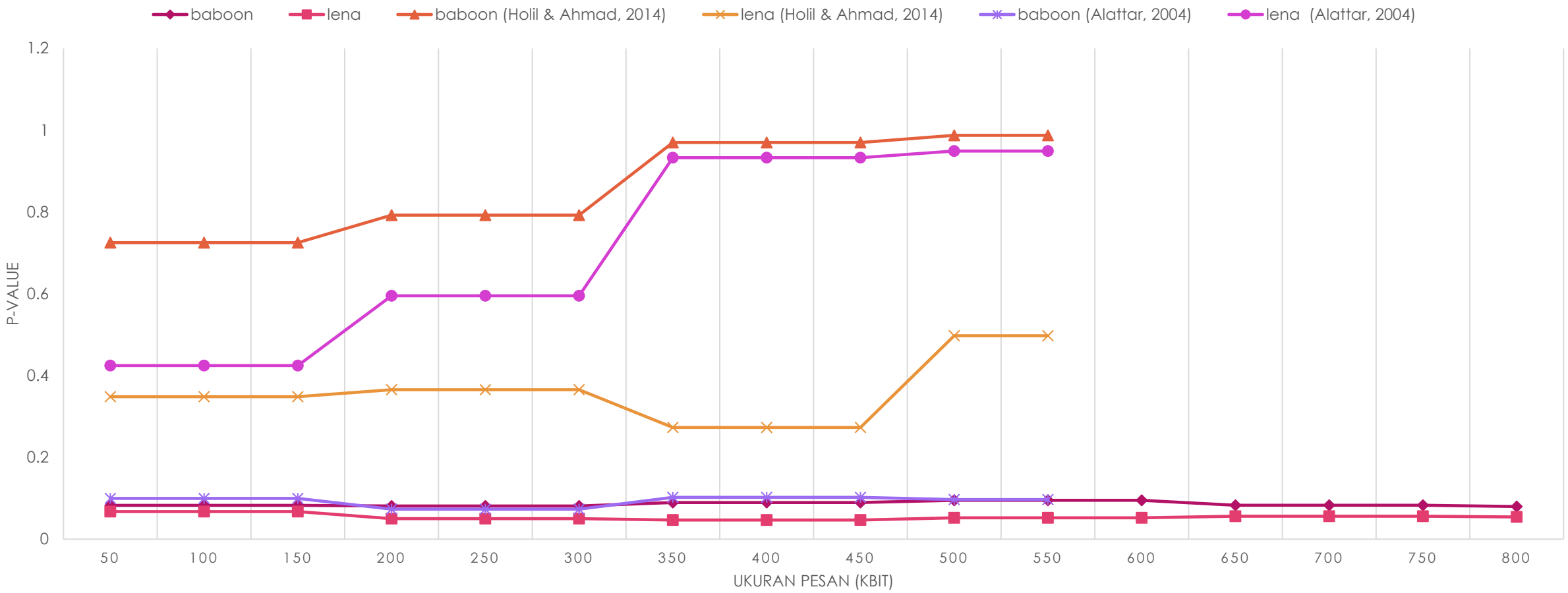
- histogram yang dihasilkan oleh metode (Alattar, 2014) memiliki jumlah *pixel* yang hampir sama pada tiap *pixel*
- sedangkan pada metode yang diusulkan ada beberapa *pixel* yang memiliki jumlah lebih dominan dibanding nilai *pixel* sebelahnya

KOMPARASI RATA RATA P-VALUE CHI SQUARE ATTACK



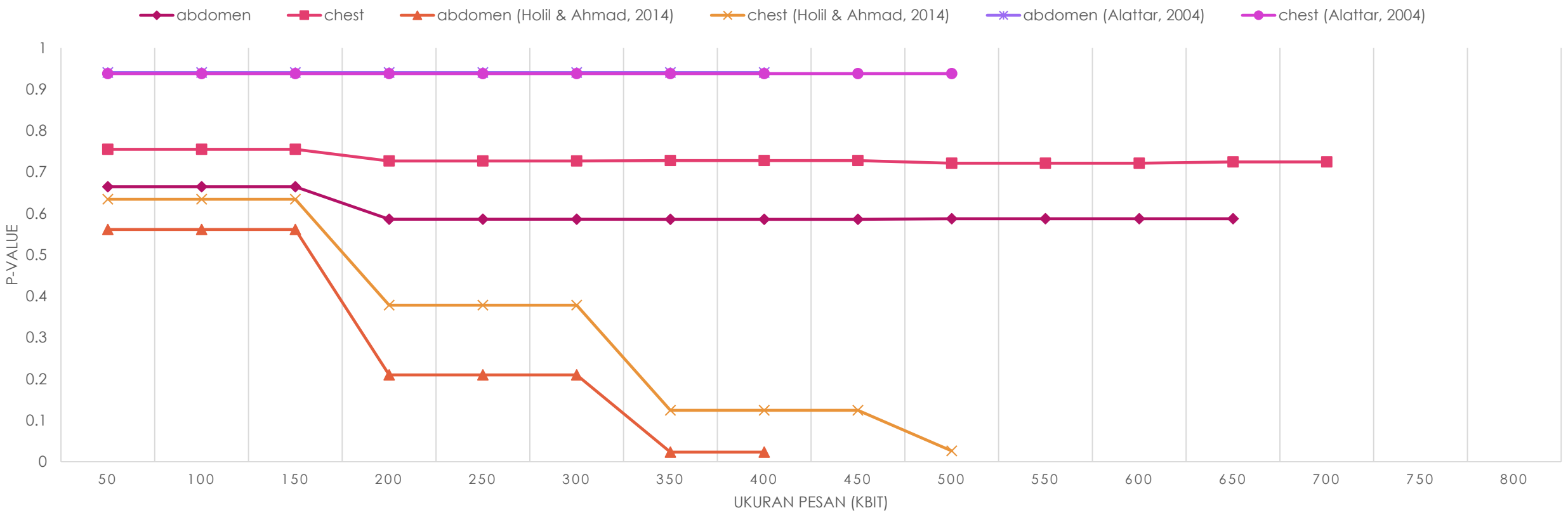
- Pada metode yang diusulkan tidak tampak terdapat rata rata P-value yang melebihi angka lebih dari 0,5.
- Sedangkan pada metode belumnya hanya pada citra lena dengan penyisipan 50Kbit saja yang tidak melebihi 0,5.

KOMPARASI RATA RATA P-VALUE CHI SQUARE ATTACK

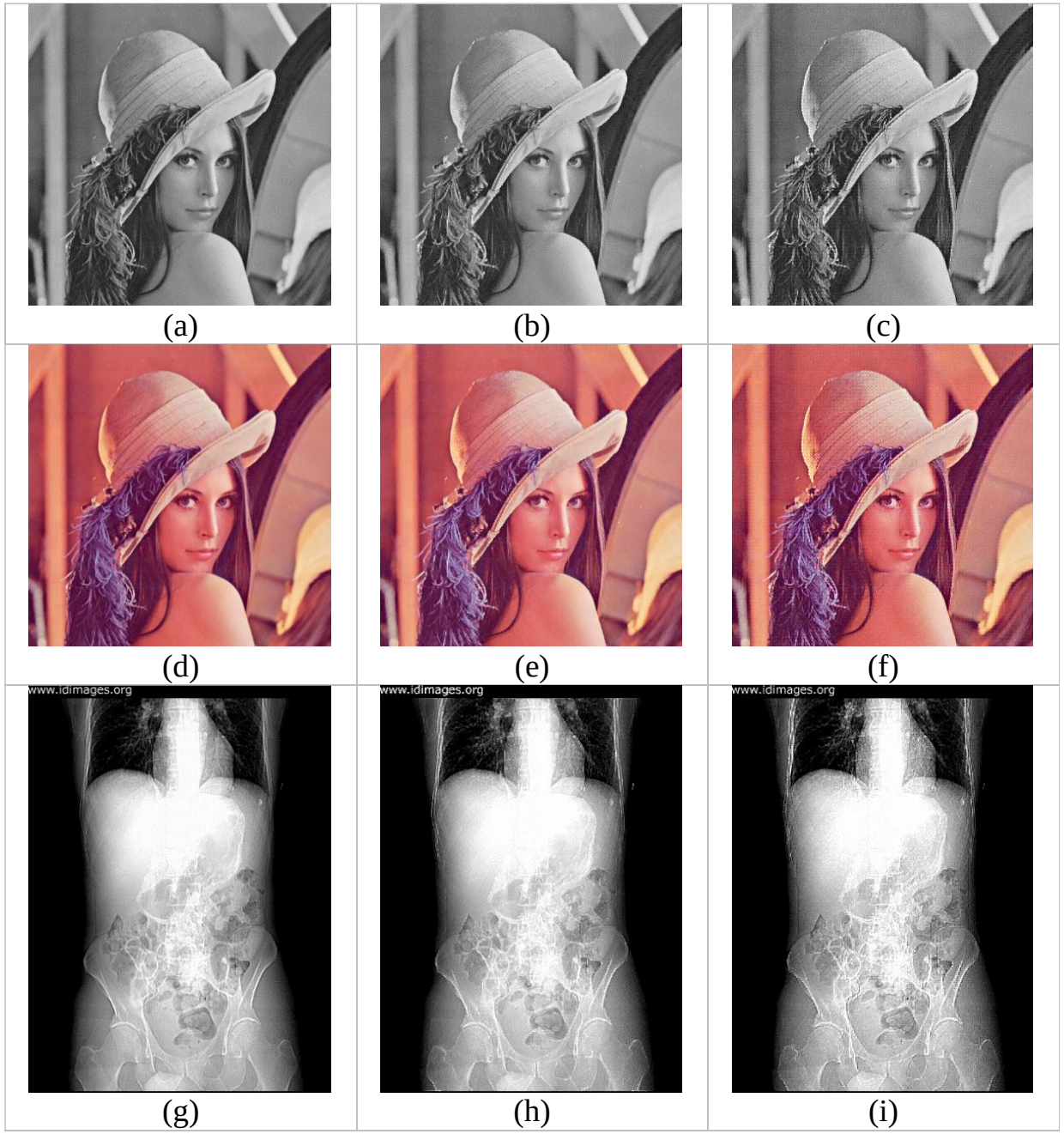


- Hanya pada metode (Alattar, 2014) pada citra baboon yang dapat mengimbangi nilai tersebut.
- Selain itu pada metode yang diusulkan (Holil & Ahmad, 2014) dengan citra mandril keseluruhan nilainya berada diatas 0,5

KOMPARASI RATA RATA P-VALUE CHI SQUARE ATTACK



- model histogram dari citra medis yang memiliki nilai besar pada ujung kiri dan kanan,
- pergerakan histogram kearah mendekati tengah sehingga membuat nilai P-value yang kurang baik



- Gambar (a),(d), dan (g) merupakan hasil citra pada metode yang diusulkan.
- Gambar (b),(e), dan (h) merupakan hasil penyisipan dengan metode yang diusulkan oleh (Holil & Ahmad, 2014).
- Gambar (c),(f), dan (i) adalah hasil citra ketika dilakukan penyisipan dengan metode yang diusulkan oleh (Alattar, 2014).

Kesimpulan

- Penggunaan fungsi modulo dalam penyembunyian data dapat meningkatkan kualitas citra yang dihasilkan
- Penggunaan bilangan 3 pada pesan yang akan disisipkan juga dapat meningkatkan kapasitas maksimal dari sebuah citra
- Pada citra yang memiliki variasi pixel cukup tinggi memiliki tingkat keamanan yang lebih baik. Terlihat dari kecilnya hasil KL Divergence dan Chi Square Attack.

Saran

- Diperlukan penelitian lebih lanjut tentang penyimpanan location map yang terintegrasi dengan media penyimpanan.
- Diperlukan penelitian lebih lanjut pada citra yang memiliki histogram yang hampir seragam
- Peningkatan penggunaan fungsi modulus pada metode penyembunyian data.

Rangkuman Kontribusi

	Holil dan Ahmad 2014	Propose
Proses Penyisipan	Pesan dikonversi dalam angka bilangan 2 (0,1) U0 = median dari block V1= U0- U1 V2= U0- U2 V3= U0- U3 Selisih direduksi $\begin{cases} V_N, jika -2 < V_N < 2 \\ V_N + 2^{\lfloor \log V_N \rfloor - 1}, jika -2 \leq V_N \\ V_N - 2^{\lfloor \log V_N \rfloor - 1}, jika\ V_N \geq 2 \end{cases}$ Penyisipan RDE dan Non RDE $\tilde{V} = 2x\ v + b$ Changeable $\tilde{V} = 2x \left\lfloor \frac{v}{2} \right\rfloor + b$	Pesan dikonversi dalam angka bilangan 3 (0,1,2) U0 = nilai pixel ujung kiri atas V1= U0- U1 V2= U0- U2 V3= U0- U3 Penyisipan $\tilde{V} \begin{cases} Vn, jika\ Vn\ mod 3 = M\ mod\ 3 \\ Vn + 1, jika\ Vn\ mod 3 = M\ mod\ 3 + 1 \\ Vn - 1, jika\ Vn\ mod 3 = M\ mod\ 3 + 2\ \ dan\ d > 0 \\ Vn + 2, jika\ Vn\ mod 3 = M\ mod\ 3 + 2\ \ dan\ d = 0 \end{cases}$ If 1<Un<254

Rangkuman Kontribusi

	Holil dan Ahmad 2014	Propose
Extract Data	U0 = median dari block V1= U0- U1 V2= U0- U2 V3= U0- U3 M = Vn mod 2	U0 = nilai pixel ujung kiri atas V1= U0- U1 V2= U0- U2 V3= U0- U3 M = Vn mod 3 If 0<Un<255
Recovery Cover	Expandable Non RDE $\ddot{Vn} = \left\lfloor \frac{Vn}{2} \right\rfloor$ Exampandable RDE $\ddot{Vn} = \left\lfloor \frac{Vn}{2} \right\rfloor$ $Vi = \begin{cases} \ddot{Vn} - 2^{log_2\lvert\ddot{Vn}\rvert - 1}, if\ LM = 0 \\ \ddot{Vn} - 2^{log_2\lvert\ddot{Vn}\rvert}, if\ LM = 1 \end{cases}$	(+) region Ganjil Un=2 x $\left\lfloor \frac{V}{2} \right\rfloor$ Genap Un=2 x $\left\lfloor \frac{V-2}{2} \right\rfloor + 1$ (-) region Ganjil Un=2 x $\left\lfloor \frac{V+2}{2} \right\rfloor$ Genap Un=2 x $\left\lfloor \frac{V}{2} \right\rfloor + 1$ If 0<Un<255

Rangkuman Kontribusi

	Holil dan Ahmad 2014	Propose
Location Map	Expandable RDE 1 1 Expandable non-RDE 1 0 Changeable 0 1 Unchangeable 0 0 Digabung dengan pesan sebelum dilakukan proses Embbed	Plus Region 1 | 0 Minus Region 0 | 1 Unchange 0 | 0 Region d=0 1 | 1 Location map akan dibagi menjadi 2 bagian bagian pertama akan disimpan pada sebuah file Bagian yang lain dilakukan Diembed pada titik referensi dengan fungsi modulus 8 $U_m mod\ 8 + n = LM_2 \quad \widetilde{U_m} = U_m + n$ Kemudian n disimpan pada file untuk proses recoveri. Untuk blok lebih dari 2x2 embedding dilakukan penambahan dan pengurangan secara bergantian. Setiap proses disimpan pada file.

Rangkuman Kontribusi

	Pambudi dan Ahmad 2015	Propose
Pengamanan Location map	Pertukaran kunci dengan deffie-helma Terdapat 3 IV 1. IV 2. IV' 3. IV client IV ' diacak dengan metode dengan bilangan kunci s IV=26 huruf+10 angka l=s mod length(IV) count=1 while count <=length(IV) if IV[i] telah ada pada IV' i=(i+1) mod length(IV) IV'[count++]=IV[i] i=(i+s) mod length(IV) IV client diacak bebas transformasi IV client IV client dikirimkan ke penerima ddetransformasiIV client dilanutkan dengan ddetransformasipesan	Pertukaran kunci dengan deffie-helman Terdapat 3 IV 1. IV 2. IV' 3. IV transport IV' diacak dengan bilangan B dari penerima IV=26 huruf+10 angka l=s mod length(IV) count=1 a=0 while count <=length(IV) if IV[i] telah ada pada IV' i=(i+1) mod length(IV) IV'[count]=IV[i] i=(i+a+s) mod length(IV) a++ count++ IV transport diacak dengan metode diatas dengan bilangan kunci s IV transport tidak dikirimkan karena penerima juga mengacak dengan metode yang sama ddetransformasipesan dengan IV transport yang diacak oleh penerima