NASKAH PUBLIKASI

PROYEK TUGAS AKHIR

**KRIPTOGRAFI CITRA DENGAN MENGGABUNGKAN**

**METODE RIVERST-SHAMIR-ADLEMAN (RSA) DAN METODE KOMPRESI HADAMARD**

Program Studi Informatika

Fakultas Teknologi Informasi dan Elektro



Disusun Oleh;

**Albertus Ndaru Krismandoko**

**5130411245**

**PROGRAM STUDI INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI DAN ELEKTRO**

**UNIVERSITAS TEKNOLOGI YOGYAKARTA**

**2018**

Naskah Publikasi

**PROYEK TUGAS AKHIR**

**KRIPTOGRAFI CITRA DENGAN MENGGABUNGKAN**

**METODE RIVERST-SHAMIR-ADLEMAN (RSA) DAN METODE KOMPRESI HADAMARD**

Disusun Oleh:

**Albertus Ndaru Krismandoko**

**5130411245**

Telah disetujui oleh pembimbing

Pembimbing

Dr. Erik Iman Heri Ujianto, S.T., M.Kom. Tanggal:.……Maret 2018

**KRIPTOGRAFI CITRA DENGAN MENGGABUNGKAN**

**METODE RIVERST-SHAMIR-ADLEMAN (RSA) DAN METODE KOMPRESI HADAMARD**

Albertus Ndaru Krismandoko

*Program Studi Informatika,Fakultas Teknologi Informasi dan Elektro  
Universitas Teknologi Yogykarta*

*Jl. Ringroad Utara Jombor Sleman Yogyakarta*

*E-mail : ndarualbert21@gmail.com*

## ABSTRAK

*Pada era teknologi yang sudah sangat maju saat ini, orang-orang dengan mobilitas yang sangat padat dituntut untuk bekerja dengan efektif dan efisien. Salah satu pengaruh citra digital dalam teknologi saat ini sangat besar karena semua sudah menggunakan teknologi digital dalam kehidupan saat ini. Ukuran citra digital dan keamanan citra dapat menjadi faktor yang sangat penting dalam kecepatan pengiriman citra atau dalam penyimpanan citra dan juga keamanan informasi dalam citra tersebut. Oleh sebab itu pengurangan ukuran citra digital dan pengaman data citra digital sangatlah membantu dalam memproses pengiriman dan perlindungan informasi dalam citra digital .Untuk mengurangi ukuran citra digital dan juga untuk mengamankan data citra tersebut tanpa menghilangkan informasi penting dapat dilakukan dengan teknik kompresi dan dengan kriptografi. Teknik kompresi sendiri terdapat 2 teknik yaitu teknik lossy dan lossless sedangkan kriptografi terdapat 2 algoritma yaitu algoritma Simetrik dan Asimetetrik .Saat ini sudah banyak metode dari kedua teknik tersebut digunakan dalam kompresi citra, dengan menggunakan salah satu metode atau dengan menggabungkan beberapa metode untuk memperoleh hasil yang maksimal. Penggabungkan metode Transformasi Hadamard dengan Metode Kriptografi RSA diusulkan untuk mmecahkan masalah tersebut. Penggabungan metode Transformasi Hadamard dengan Metode Kriptografi RSA dapat mengamankan dan mengkompresi citra dengan rata-rata CR = 1.89 , MSE = 0 dan PSNR ∞. Nilai MSE dan PSNR menunjukan bahwa hasil dekripsi dan rekonstruksi citra sama persis dengan citra sebelum dienkripsi,*

**Kata Kunci**: Kompresi, Transformasi Hadamard, Kriptografi, RSA

### 1. PENDAHULUAN

Pada saat ini teknologi sudah sangat maju, citra digital memegang peran penting dalam perkembangan teknologi saat ini. Mulai dari karya seni, mengabadikan moment penting, kepolisian, medis bahkan dalam dokumen penting sudah menggunakan citra digital untuk menyembunyikan informasi. Citra digital sendiri dapat disimpan dalam waktu yang cukup lama, seperti halnya moment penting yang diabadikan sampai dengan data penting. Selain hal tersebut saat ini pengiriman citra digital hampir selalu terjadi.

Metode kompresi yang ada saat ini pun juga sudah sangat banyak, beberapa diantaranya merupakan kompresi citra yang terkenal, contohnya seperti JPEG, GIF PNG dan lain sebagainnya. Metode metode tersebeut sebenarnya merupakan penggabungan dari beberapa metode atau teknik kompresi atau bahkan juga ada yang hanya menggunakan salah satu dari metode atau teknik kompresi yang ada. Misalnya JPEG, merupakan penggabungan dari metode *Discrete Cosinus Transform, Quantise,*  RLE, dan *Huffman Coding*.

Pada proses pengiriman citra terdapat beberapa hal yang harus diperhatikan yaitu : keamanan informasi data citra jika citra tersebut memiliki informasi yang penting, integritas data dan juga autentikasi. Oleh karena itu dibutuhkan pengkodean data sebelum dilakukan pengiriman, sehingga informasi dalam citra tersebut aman dan terjaga kerahasiaannya dan tidak mudah diubah untuk menjaga integritas data citra tersebut. Ilmu yang mempelajari tentang cara-cara pengamanan data dikenal dengan istilah Kriptografi.

Pada penelitian ini penggabungan metode kriptografi RSA dengan transformasi Hadamard akan diimplemenrasikan pada citra digital 8 bit greyscale dengan ukuran 256x256 pixel, kontras citra tidak dibatasi. Citra digital akan dienkripsi dan dikompresi untuk mengamankan data pada citra digital dan juga mengurangi ukuran bit citra digital secara efektif tanpa menghilakan informasi penting dalam citra.

.

### 2. LANDASAN TEORI

* 1. **Kriptografi**

Kriptografi berasal dari Bahasa Yunani, *crypto* dan *graphia. Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan data atau pesan ketika data atau pesan dikirim dari suatu tempat ke tempat lain. [1]

Algoritma kriptografi selalu terdiri dari dua bagian, yaitu enkripsi dan dekripsi. Enkripsi (encryption) adalah proses untuk menyandikan plaintext atau cleartext menjadi bentuk ciphertext. Sedangkan dekripsi (decryption) adalah proses mengembalikan ciphertext menjadi plaintext semula. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci. Kunci biasanya berupa string atau deretan bilangan.

* 1. **Kompresi**

Kompresi data ialah bagian dari ilmu pengetahuan dan seni dalam teknologi komputer yang merepresentasikan sebauh informasi, dalam hal ini berbentuk data, dalam suatu format yang lebih padat dan mampat. Hal inilah yang memungkin revolusi multimedia digital dalam 10 tahun terakhir. [2]

Data Gambar merupakan data yang secara aktual merepresentasikan real grafis kedalam bentuk digital yang dapat diproses dengan menggunkan komputer konvensional, yang dimaksud sebagai bentuk digital pada penjesan sebelumnya adalah data yang disajikan dalam bentuk diskrit yang biasa disebut pixel. Image Compression dibagi menjadi 2 yaitu lossless dan lossy .[2]

* 1. **RSA** [1]

RSA adalah sebuah algoritma kriptografi yang dibuat oleh 3 orang peneliti dari MIT pada tahun 1976. Algoritma RSA merupakan pemfaktoran bilangan prima yang cukup besar dengan memilih secara acak bilangan prima pertama (p), bilangan prima ke dua (q), dan bilangan prima ke tiga (e).

Besaran-besaran yang digunakan pada algoritma RSA:

1. p dan q bilangan prima (rahasia)

2. n = p ⋅ q (tidak rahasia)

3. φ(n) = (p – 1)(q – 1) (rahasia)

4. e (kunci enkripsi) (tidak rahasia)

5. d (kunci dekripsi) (rahasia)

6. m (plainteks) (rahasia)

7. c (cipherteks) (tidak rahasia)

Enkripsi RSA :

c=m^e Mod n

Dekripsi RSA :

m=c^d Mod n

* 1. **Transformasi Hadamard**

transformasi Hadamard merupakan transformasi non-sinusoidal, Fungsi basis transformasi hanya bernilai -1 dan 1. Transformasi hadamard mempunyai 2 macam yaitu transformasi Hadamard 1 dimensi dan transformasi Hadamard 2 dimensi. [3]

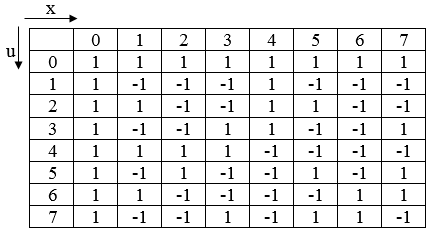
* + - 1. Transformasi Hadamard 1 dimensi dari citra

* + - 1. Transformasi Hadamard 1 dimensi balik

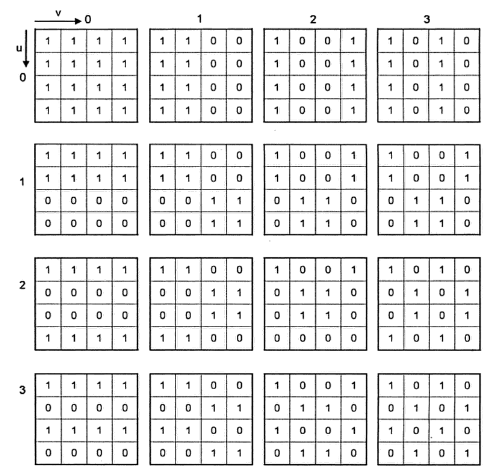
* + - 1. Fungsi Basis dari transformasi Hadamard 1D

* + - 1. Transformasi Hadamard 2 dimensi

* + - 1. Transformasi Hadamard 2 dimensi balik

* + - 1. Fungsi Basis dari transformasi Hadamard 2D

*Gambar 1. Fungsi Basis Hadamard 1D N=8*



*Gambar 2. Fungsi basis Transformasi Hadamard 2D*

*untuk N=4*

* 1. **Mean Square Error (MSE)**

MSE merupakan rata-rata dari kuadrat selisih dua pixel dua citra.

*n* merupakan jumlah pixel yang ada, *Pi* dan *Qi* merupakan nilai pixel dari kedua citra.[4]

* 1. **Compresion Rasio**

*Compression Ratio* adalah suatu metode untuk menghitung tingkat keefisienan suatu metode kompresi.

*C* adalah *Compression Ratio* sedangkan *b* adalah jumlah bit sebelum proses kompresi dan *b’* adalah jumlah bit setelah proses kompresi.[5]

* 1. **Peak Signal to Noise Ratio (PSNR)**

PSNR merupakan perkiraan hubungan antara berkurangnya kualitas dengan sistem penglihatan manusia. Semakin tinggi nilai PSNR, maka semakin mirip pula suatu citra.

*Pi* merupakan pixel dari citra, sehingga *maxi|Pi|* kuadrat merupakan kuadrat dari nilai pixel/ intensitas tertiggi dari citra, Contoh pada citra 8-bit yang memiliki range 0-255, nilai *maxi|Pi|* adalah 255.

### 3. METODOLOGI PENELITIAN

**3.1. Waterfall**

Dalam penelitian ini metode penelitian yang digunakan adalah Waterfall, dalam metode tersebut ada beberapa tahapan langkah yaitu komunikasi, perencanaan, pemodelan, konstruksi (implementasi), pemasangan. Dikarenakan penelitian yang dilakukan tidak berhubungan dengan user secara langsung (studi kasus) melainkan melakukan penelitian mengenai metode untuk kriptografi dan kompresi citra digital sehingga komunikasi dengan user tidak ada, untuk mengganti langkah tersebut dilakukan studi literatur mengenai teori-teori dan penelitian-penelitian yang terkait. Berikut penjelasan lebih detailnya,[6]

1. Pengumpulan data menggunakan studi literatur, dalam tahapan ini dilakukan riset mengenai metode-metode yang terkait dengan metode yang digunakan dalam penelitian ini, selain itu teori-teori yang terkait juga sangat penting untuk menunjang keberhasilan penelitian ini.
2. Perencanaan, dalam penelitian ini setelah melakukan studi literatur kemudian dipilih mana informasi yang bisa digunakan, dan mulai untuk mencoba menyusun algoritma yang akan digunakan.
3. Pemodelan, setelah melalui tahap perencanaan selanjutnya pemodelan dimana dilakukan analisis lebih mendalam mengenai algoritma yang sudah dibuat pada langkah perencanaan, apakah algoritma tersebut bisa digunakan atau tidak, jika tidak akan dilakukan analisis lebih mendalam. Setelah tahap analisis, dilanjutkan pemodelan sistem yang akan dibuat menggunakan UML. Dalam bagian pemodelan ini ada beberapa design yang harus dilakukan diantaranya design input, design output, design proses, design basis data.
   * + - 1. Design Input

Pada tahapan design input yang akan menjadi input ke sistem adalah citra digital. Master yang akan dibuat adalah Enkripsi-Kompresi dan Deskripsi-Dekompresi (Rekonstruksi) yang akan dipisah menjadi 2 interface .

* + - * 1. Design Proses

Pada design proses, seperti yang sudah dijelaskan pada skema proses sebelumnya, proses yang berlangsung sesuai dengan skema yang sudah dibuat. Untuk pemodelan terhadap penerapannya dalalm sistem akan dimodelkan menggunakan Use Case Diagram, Sequence Diagram, Activity Diagram, Class Diagram.

* + - * 1. Design Output

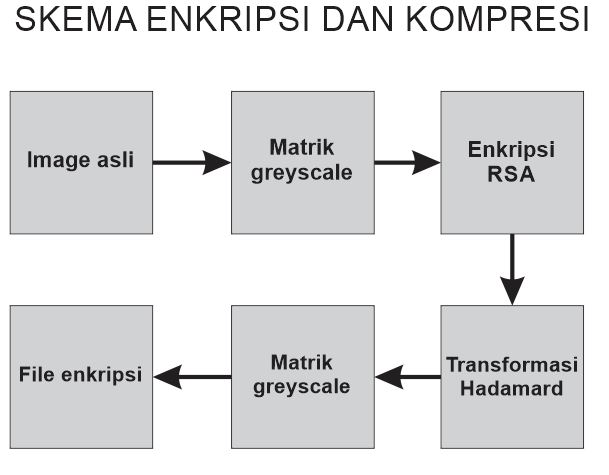
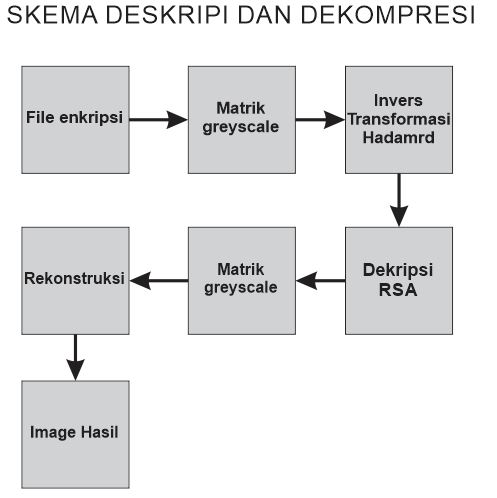
Output yang diharapkan dari sistem yang dibangun berupa kumpulan parameter-parameter hasil proses.

* + - * 1. ` Design Basis Data

Dalam sistem yang dibuat tidak membutuhkan basis data, karena hanya sebatas melakukan enkripsi, kompresi, deskripsi, dan dekompresi citra digital saja.

* + - * 1. Design Interface

Dalam design interface akan ditampilkan citra asli, Citra hasil proses enkripsi-kompresi dan deskripsi-dekompresi serta nilai-nilai PSNR, MSE, dan CR.

**3.2. Skema Enkripsi dan Dekripsi**

*Gambar 3. Skema Enkripsi-Kompresi*

*Gambar 4. Skema Dekripsi-Dekompresi*

**4. HASIL DAN PEMBAHASAN**



*Gambar 6. DSC01362\_Med\_C.bmp*



*Gambar 5. DSC01362.bmp*

*Gambar 7. DSC01362\_Higt\_C.bmp*



*Gambar 8. DSC\_2922.bmp*

*Gambar 9. DSC\_2922\_Med\_C.bmp*



*Gambar 10. DSC\_2922\_High\_C.bmp*

Hasil dari pengujian terhadap metode yang digunakan disajikan dalam juga table hasil uji dibawah ini,

1. Enkripsi dan Kompresi berdasarkan tingkat kecerahan citra.

*Tabel 1. Hasil uji dengan tingkat kecerahan*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Nama | Ukuran | Key | | CR |
| e | d |
| 1 | DSC01362.bmp | 256x256 | 13 | 757 | 1.86 |
| 2 | DSC01362\_medium\_bright.bmp | 256x256 | 13 | 757 | 1.88 |
| 3 | DSC01362\_high\_bright.bmp | 256x256 | 13 | 757 | 2.04 |
| 4 | DSC\_2922.bmp | 256x256 | 13 | 757 | 1.89 |
| 5 | DSC\_2922\_medium\_bright.bmp | 256x256 | 13 | 757 | 1.87 |
| 6 | DSC\_2922\_high\_bright.bmp | 256x256 | 13 | 757 | 1.9 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Nama | Key | | Waktu  (s) |
| e | d |
| 1 | DSC01362.bmp | 13 | 757 | 1.20 |
| 2 | DSC01362n\_medium\_contras.bmp | 13 | 757 | 1.20 |
| 3 | DSC01362\_hight\_contras.bmp | 13 | 757 | 1.27 |
| 4 | DSC01362\_medium\_bright.bmp | 13 | 757 | 1.21 |
| 5 | DSC01362\_high\_bright.bmp | 13 | 757 | 1.22 |
| 6 | DSC\_2922.bmp | 13 | 757 | 1.27 |
| 7 | DSC\_2922\_medium\_contras.bmp | 13 | 757 | 1.21 |
| 8 | DSC\_2922\_high\_contras.bmp | 13 | 757 | 1.23 |
| 9 | DSC\_2922\_medium\_bright.bmp | 13 | 757 | 1,21 |
| 10 | DSC\_2922\_high\_bright.bmp | 13 | 757 | 1.21 |

Hasil pengujian terhadap berbagai citra dengan tingkat kecerahan yang berbeda tetapi dengan kunci enkripsi dan ukuran yang sama menghasilkan rata-rata CR 1,91 seperti terlihat pada Tabel 1. Berdasarkan tingkat kecerahan, CR yang dihasilkan lebih besar pada citra dengan tingkat kecerahan yang tinggi. Berdasarkan pengujian yang dilakukan metode yang diusulkan sangat efektif bila digunakan pada citra dengan tingkat kecerahan tinggi jika ditinjau dari nilai CR nya, pengimplementasian terhadap citra berekstensi \*.bmp (citra yang belum terkompresi).

1. Berdasarkan tingkat kontras citra

*Tabel 2. Hasil uji dengan tingkat kontras*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Nama | Ukuran | Key | | CR |
| e | d |
| 1 | DSC01362.bmp | 256x256 | 13 | 757 | 1.86 |
| 2 | DSC01362\_medium\_contras.bmp | 256x256 | 13 | 757 | 1.88 |
| 3 | DSC01362\_hight\_contras.bmp | 256x256 | 13 | 757 | 1.89 |
| 4 | DSC\_2922.bmp | 256x256 | 13 | 757 | 1.89 |
| 5 | DSC\_2922\_medium\_contras.bmp | 256x256 | 13 | 757 | 1.89 |
| 6 | DSC\_2922\_high\_contras.bmp | 256x256 | 13 | 757 | 1.88 |

Hasil pengujian terhadap berbagai citra dengan tingkat kontras yang berbeda tetapi dengan kunci enkripsi dan ukuran yang sama menghasilkan rata-rata CR 1,89 seperti terlihat pada Tabel 2. Berdasarkan tingkat kecerahan, CR yang dihasilkan rata rata citra mempunyai nilai yang sama. Berdasarkan pengujian yang dilakukan metode yang diusulkan sangat efektif bila digunakan pada semua citra, karena jika ditinjau dari nilai CRnya rata-rata memiliki nilai yang sama, pengimplementasian terhadap citra berekstensi \*.bmp (citra yang belum terkompresi).

1. Berdasarkan waktu Enkripsi dan Kompresi

*Tabel 3. Hasil uji waktu Enkripsi dan Kompresi*

1. Berdasarkan waktu Enkripsi dan Kompresi dengan perubahan kunci

*Tabel 4. Hasil uji waktu Enkripsi dan Kompresi dengan perubahan kunci public dan privat*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Nama | Key | | Waktu  (s) |
| e | d |
| 1 | DSC01362.bmp | 23 (913) | 107 | 1.28 |
| 2 | DSC01362\_medium\_contras.bmp | 23 (913) | 107 | 1.26 |
| 3 | DSC01362\_hight\_contras.bmp | 23 (913) | 107 | 1.27 |
| 4 | DSC01362\_medium\_bright.bmp | 23 (913) | 107 | 1.28 |
| 5 | DSC01362\_high\_bright.bmp | 23 (913) | 107 | 1.26 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6 | DSC\_2922.bmp | 23 (913) | 107 | 1.26 |
| 7 | DSC\_2922\_medium\_contras.bmp | 23 (913) | 107 | 1.26 |
| 8 | DSC\_2922\_high\_contras.bmp | 23 (913) | 107 | 1.27 |
| 9 | DSC\_2922\_medium\_bright.bmp | 23 (913) | 107 | 1.27 |
| 10 | DSC\_2922\_high\_bright.bmp | 23 (913) | 107 | 1.27 |

1. Berdasarkan waktu dekripsi dan dekompresi

*Tabel 6. Hasil uji waktu dan kualitas kunci public 13*

*Tabel 5. Hasil uji waktu dan kualitas kunci public 23*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Nama | Kualitas | | Waktu(s) |
| MSE | PSNR |
| 1 | DSC01362.bmp | 0 | ∞ | 1.78 |
| 2 | DSC01362n\_medium\_contras.bmp | 0 | ∞ | 1.78 |
| 3 | DSC01362\_hight\_contras.bmp | 0 | ∞ | 1.74 |
| 4 | DSC01362\_medium\_bright.bmp | 0 | ∞ | 1.76 |
| 5 | DSC01362\_high\_bright.bmp | 0 | ∞ | 1.74 |
| 6 | DSC\_2922.bmp | 0 | ∞ | 1.77 |
| 7 | DSC\_2922\_medium\_contras.bmp | 0 | ∞ | 1.76 |
| 8 | DSC\_2922\_high\_contras.bmp | 0 | ∞ | 1.76 |
| 9 | DSC\_2922\_medium\_bright.bmp | 0 | ∞ | 1.76 |
| 10 | DSC\_2922\_high\_bright.bmp | 0 | ∞ | 1.77 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No | Nama | Kualitas | | Waktu(s) |
| MSE | PSNR |
| 1 | DSC01362.bmp | 0 | ∞ | 23.88 |
| 2 | DSC01362\_medium\_contras.bmp | 0 | ∞ | 24.44 |
| 3 | DSC01362\_hight\_contras.bmp | 0 | ∞ | 24.32 |
| 4 | DSC01362\_medium\_bright.bmp | 0 | ∞ | 24.38 |
| 5 | DSC01362\_high\_bright.bmp | 0 | ∞ | 22.83 |
| 6 | DSC\_2922.bmp | 0 | ∞ | 24.27 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 7 | DSC\_2922\_medium\_contras.bmp | 0 | ∞ | 23.59 |
| 8 | DSC\_2922\_high\_contras.bmp | 0 | ∞ | 24.39 |
| 9 | DSC\_2922\_medium\_bright.bmp | 0 | ∞ | 24.19 |
| 10 | DSC\_2922\_high\_bright.bmp | 0 | ∞ | 23.99 |

Hasil pengujian pada seluruh citra menunjukkan bahwa metode yang diusulkan sangat efektif baik terbukti kualitas tidak berubah sesuai dengan aslinya setelah proses rekonstruksi, semua MSE 0 dan PSNR ∞ . Melihat hasil pengujian waktu saat dekripsi dan dekompresi sangat berbedah jauh antara kunci publik 23(913), privat 107 dengan kunci publik 13(913), privat 757, ini dikarenakan semakin besar angka kunci privat maka semakin lama proses perhitungan dekripsinya, tetapi semakin besar angka kunci privatnya maka data yang ada pada citra digital semakin aman

**5. PENUTUP**

**5.1. Kesimpulan**

Dari hasil penelitian yang sudah dilakukan disimpulkan bahwa metode yang diusulkan mampu melakukan enkripsi, kompresi, deskripsi dan mampu merekonstruksi kembali citra. Metode yang diusulkan juga mempunyai performa yang baik, dilihat dari hasil rekonstruksi citra setelah mengalami enkripsi dan kompresi dengan kualitas citra yang sama persis dengan aslinya, dilihat dari MSE = 0 dan PSNR = ∞. Metode kriptografi dan kompresi yang diusulkan sangat efektif untuk keamanan data dan mengurangi bit citra saat enkripsi. Melihat dari waktu dekripsi dan dekompresi jika kunci privat semakin besar maka proses dekripsi semakin lama dikarenakan proses kalkulasi yang sangat besar tetapi data citra akan semakin aman.

**5.2. Saran**

Dari hasil penelititan yang dilakukan maka penulis memberikan beberapa saran untuk peneliti-peneliti selanjutnya dengan topik yang sama, berikut sarannya;

1. Gunakan metode kompresi lain pada saat kompresi citra setelah dienkripsi, contohnya metode *Walsh.*
2. Untuk mempercepat deskripsi gunakan metode enkripsi *Playfair Chiper.*
3. Tambahkan metode kuantisasi untuk kompresi citra dan mendapatkan *Compresion Ratio* yang lebih bagus.

**Daftar pustaka**

[1] Ariyus, D. (2008). *Pengeantar Ilmu KRIPTOGRAFI (Teori, Analisis, dan Implementasi)*. Yogyakarta: C.V Andi Offse.

[2] Pu, I. M. (2006). *Fundamental Data Compression*. Jordan Hill, Oxford OX2 8DP 30 Corporate Drive, Suite 400, Burlington, MA 01803: Elsevier..

[3] Putra, D. (2010). *Pengolahan Citra Digital*. Yogyakarta: C.V Andi Offset.

[4] Gonzalez, R. C., & Woods, R. E. (2008). *Digital Image Processing* (Third). New Jersey: Pearson Prentice Hall.

[5] Salomon, D. (2007). *Data Compression The Complete Reference FourthEdition*. *Journal of Chemical Information and Modeling* (Vol. 53).

[6] Pressman, R. S., & Maxim, B. R. (2015). *Software Engineering: a Practitioner’S Approach.* New York: Mc Graw Hill. Retrieved from Eighth Edition