IMPLEMENTASI ALGORITMA *HILL CIPHER* DAN *ARNOLD CAT MAP* DALAM PEMANFAATAN ENKRIPSI DAN DEKRIPSI CITRA DIGITAL BERBASIS *WEBSITE*

SKRIPSI

OLEH
MUHAMMAD LUQMAN HAKIM
NIM. 17610080

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

IMPLEMENTASI ALGORITMA *HILL CIPHER* DAN *ARNOLD CAT MAP* DALAM PEMANFAATAN ENKRIPSI DAN DEKRIPSI CITRA DIGITAL BERBASIS *WEBSITE*

SKRIPSI

Diajukan Kepada
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang
untuk Memenuhi Salah Satu Persyaratan dalam
Memperoleh Gelar Sarjana Matematika (S.Mat)

Oleh
Muhammad Luqman Hakim
NIM. 17610080

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2021

IMPLEMENTASI ALGORITMA *HILL CIPHER* DAN *ARNOLD CAT MAP* DALAM PEMANFAATAN ENKRIPSI DAN DEKRIPSI CITRA DIGITAL BERBASIS *WEBSITE*

SKRIPSI

Oleh
Muhammad Luqman Hakim
NIM. 17610080

Telah Diperiksa dan Disetujui untuk Diuji
Tanggal 16 Juni 2021

Pembimbing I,	Pembimbing II
Muhammad Khudzaifah, M.Si	Evawati Alisah, M.Pd
NIDT. 1990051120 160801 1 057	NIP. 19720604 199903 2 001

Mengetahui,
Ketua Program Studi Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

IMPLEMENTASI ALGORITMA *HILL CIPHER* DAN *ARNOLD CAT MAP* DALAM PEMANFAATAN ENKRIPSI DAN DEKRIPSI CITRA DIGITAL BERBASIS *WEBSITE*

SKRIPSI

Oleh
Muhammad Luqman Hakim
NIM. 17610080

Telah Dipertahankan di Depan Dewan Penguji Skripsi
dan Dinyatakan Diterima sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Matematika (S.Mat)
Tanggal 16 Juni 2021

Susunan Dewan Penguji:		Tanda Tangan
Penguji Utama	: Muhammad Nafie Jauhari, M.Si	(……)
Ketua Penguji	: Juhari, M.Si	(……)
Sekretaris Penguji	: Muhammad Khudzaifah, M.Si	(……)
Anggota Penguji	: Evawati Alisah, M.Pd	(……)

Mengetahui,
Ketua Program Studi Matematika

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001

PERNYATAAN KEASLIAN TULISAN

Saya yang bertandatangan di bawah ini:

Nama	:	Muhammad Luqman Hakim
NIM	:	17610080
Program Studi	:	Matematika
Fakultas	:	Sains dan Teknologi
Judul Skripsi	:	Implementasi Algoritma *Hill Cipher* dan *Arnold Cat Map* dalam Pemanfaatan Enkripsi dan Dekripsi Citra Digital Berbasis *Website*

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri, bukan merupakan pengambilan data, tulisan, atau pikiran orang lain yang saya akui sebagai hasil tulisan dan pikiran saya sendiri, kecuali dengan mencamtumkan sumber cuplikan atau daftar rujukan. Apabila di kemudian hari terbukti atau dapat dibuktikan skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 25 Juni 2021
Yang membuat pernyataan,

Muhammad Luqman Hakim
NIM. 17610080

MOTTO

"*Barangsiapa yang mengerjakan kebaikan seberat dzarrahpun, niscaya dia akan melihat (balasan)nya.*" – Q.S Az-Zalzalah ayat 7

"Jika tidak keras terhadap diri sendiri, maka hidup akan keras kepada diri sendiri."

PERSEMBAHAN

Skripsi ini penulis persembahkan untuk:
Kedua Orang tua penulis, adik penulis dan juga keluarga penulis
yang selalu menjadi motivasi dan semangat bagi penulis
dalam menuntut ilmu, mengabdi, dan berjuang di tanah rantau.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Segala puji bagi Allah Swt atas rahmat, taufik serta hidayah-Nya, sehingga penulis mampu menyelesaikan penyusunan skripsi dengan judul Implementasi Algoritma *Hill Cipher* dan *Arnold Cat Map* dalam Pemanfaatan Enkripsi dan Dekripsi Citra Digital Berbasis *Website*, sebagai salah satu syarat untuk memperoleh gelar sarjana dalam bidang matematika di Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang.

Dalam proses penyusunan skripsi ini, penulis banyak mendapat bimbingan dan arahan dari berbagai pihak. Untuk itu ucapan terima kasih yang sebesar-besarnya dan penghargaan yang setinggi-tingginya penulis sampaikan terutama kepada:

1. Prof. Dr. Abd. Haris M.Ag selaku Rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Dr. Sri Harini, M.Si selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang.
3. Dr. Usman Pagalay, M.Si selaku Ketua Program Studi Matematika Universitas Islam Negeri Maulana Malik Ibrahim Malang.
4. Muhammad Khudzaifah, M.Si, selaku dosen pembimbing I yang telah memberikan arahan dan berbagi ilmunya kepada penulis.

5. Evawati Alisah, M.Pd, selaku dosen pembimbing II yang telah banyak memberikan arahan, nasihat, motivasi dan berbagi pengalaman kepada penulis.
6. Muhammad Nafie Jauhari, M.Si, selaku dosen penguji I yang telah memberikan kritik dan pertanyaan yang membangun sehingga penulis lebih semangat dalam menyelesaikan skripsi ini.
7. Juhari, M.Si, selaku dosen penguji II yang telah memberikan kritik dan pertanyaan yang membangun sehingga penulis lebih semangat dalam menyelesaikan skripsi ini.

Semoga Allah Swt melimpahkan rahmat dan karunia-Nya kepada kita semua. Akhirnya penulis berharap semoga dengan rahmat dan izin-Nya mudah-mudahan skripsi ini bermanfaat bagi penulis dan bagi pembaca. Amiin.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 3 Mei 2021

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Hakim, Muhammad Luqman. 2021. **Implementasi Algoritma *Arnold Cat Map* dan *Hill Cipher* dalam Pemanfaatan Enkripsi dan Dekripsi Citra Digital Berbasis *Website***. Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (1) : M. Khudzaifah M.Si, Pembimbing (2) : Evawati Alisah, M.Pd.

Kata Kunci : Citra, Enkripsi, Dekripsi, Matriks, Hill, ACM.

Citra digital atau gambar merupakan salah satu data dalam bentuk informasi visual yang digunakan dalam perkembangan teknologi diberbagai bidang yang rawan untuk dicuri dan disalahgunakan pada jaringan komputer. Salah satu bidang kajian keamanan citra digital yang dapat digunakan sampai saat ini adalah kriptografi. Enkripsi dan dekripsi adalah dua fungsi yang ada dalam kriptografi. Enkripsi citra digital bertujuan menyandikan citra digital (*plain-image*) sehingga tidak dapat dikenali lagi (*cipher-image*). Pada penelitian ini dibahas mengenai proses enkripsi-dekripsi citra digital untuk keamanan citra digital dengan algoritma *Hill Cipher* dan *Arnold Cat Map* berbasis *website*. Sehingga diharapkan citra digital tersebut dapat diamankan dari kebocoran informasi visual yang bersifat rahasia. Tujuan dari penelitian ini adalah untuk mengetahui hasil dari enkripsi dan dekripsi citra digital dengan algoritma *Hill Cipher* dan *Arnold Cat Map* berbasis *website*. Setelah dilakukan uji coba, hasil yang didapatkan adalah citra digital dari proses enkripsi sangat berbeda dari pada citra digital awal. Hasil uji coba juga menunjukkan bahwa citra digital hasil enkripsi dengan menggunakan kombinasi algoritma *Hill Cipher* dan *Arnold Cat Map* memperoleh nilai *Structural Similarity Index Metrics* (SSIM) dengan rata-rata 0,027.

ABSTRACT

Hakim, Muhammad Luqman. 2021. **An Implementation of Hill Cipher and Arnold Cat Map Algorithm in Utilizing Digital Image Encryption and Decryption Website-Based**. Thesis. Department of Mathematics, Faculty of Science and Technology, Maulana Malik Ibrahim State Islamic University of Malang. Advisor (1) : Muhammad Khudzaifah, M.Si, Advisor (2) : Evawati Alisah, M.Pd

Keywords: Image, Encryption, Decryption, Matrix, Hill, ACM.

A digital image or image is one of the data in the form of visual information that is used in technological developments in various fields that are prone to being stolen and misused on computer networks. One of the fields of digital image security studies that can be used to date is cryptography. Encryption and decryption are two functions that exist in cryptography. Digital image encryption aims to encode a digital image (plain-image) so that it cannot be recognized again (cipher-image). This study discusses the process of digital image encryption-decryption for digital image security with Hill Cipher and Arnold Cat Map algorithms based on the website. So it is hoped that the digital image can be secured from leakage of confidential visual information. The purpose of this study was to determine the results of the encryption and decryption of digital images with Hill Cipher and Arnold Cat Map algorithms based on the website. After testing, the results obtained are that the digital image of the encryption process is very different from the initial digital image. The test results also show that the encrypted digital image using a combination of the Hill Cipher and Arnold Cat Map algorithms obtains a Structural Similarity Index Metrics (SSIM) value with an average of 0,027.

مستخلص البحث

حكيم، محمد لقمان. ٢٠٢١. **تطبيق *Algoritma Arnold Cat Map dan Hill Cipher* لأخذ الفوائد من إنكريبسي *(Enkripsi)* و ديكريبسي *(Dekripsi)* الصور الرقمية اسنادا على موقع الويب**. البحث الجامعي. قسم الرياضيات. كلية العلوم والتكنولوجيا. جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج. المشرف الأول (١) م. حذيفة، الماجيستير (٢) : إيفاواتي أليسة، الماجيستير.

الكلمات المفاتحة : الصور، إنكريبسي *(Enkripsi)*، ديكريبسي *(Dekripsi)*، ماتريك *(Matriks)*، Hiil، ACM

الصورة هي من المعلومات البصرية التي تستخدم لترقية التكنولوجيا في جميع المجال وسهولة في شرقتها وهي إساءة الاستخدام على شبكات الكمبيوتر. واحدى من مجال الأمن الذي يستخدم الآن هي التشفير. إن إنكريبسي *(Enkripsi)* و ديكريبسي *(Dekripsi)* من فوائد التشفير. إن الهدف تشفير الصور الرقمية هي لإقران صورة رقمية صورة عادية (*plain-image*) بحيث لا يمكن تعرفها صورة مشفرة (*cipher-image*). إن هذا البحث تبحث عن عملية التفشير–وصف صورة رقمية لأمان الصور الرقمية باستخدام خوارزمية Hill Cipher و Arnold Cat Map اسناد على موقع الويب. يأمل على صور الرقمية أن يؤمن من تسرب المعلومات المرئية السرية. إن الهدف هذا البحث لمعرفة نتائج إنكريبسي *(Enkripsi)* و ديكريبسي *(Dekripsi)* صور الرقمية باستخدام خوارزمية Hill Cipher و Arnold Cat Map اسناد على موقع الويب. بعد الإختبار، إن نتائجها هي أن الصورة الرقمية من عملية التشفير مختلفة تمامًا عن الصورة الرقمية الأولية. ونتائج الاختبار لصورة الرقمية المشفرة باستخدام مجموعة من خوارزميات Cipher Hill و Arnold Cat Map تحصل على قيمة مقاييس مؤشر التشابه الهيكلي (*Structural Similarity Index Metrics*) (SSIM) بمتوسط ٠،٠٢٧.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh yang mana salah satu media yang digunakan adalah *website.* Seiring dengan hal tersebut, tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan semakin meningkat, salah satunya adalah data dalam bentuk informasi visual yakni citra digital.

Citra digital atau gambar merupakan salah satu data dalam bentuk informasi visual yang digunakan dalam perkembangan teknologi diberbagai bidang. Contoh kasusnya dalam bidang keamanan yakni dalam melakukan verifikasi akun. Verifikasi akun pada *website* membutuhkan data diri yang valid salah satunya adalah foto kartu identitas pengguna. Di satu sisi, hal ini cukup berbahaya karena apabila foto kartu identitas tersebut dicuri dan disalahgunakan dapat merugikan pengguna. Sehingga, perlu untuk melindungi kerahasiaan dan keaslian citra digital karena kerahasiaan suatu informasi sangat penting dan bersifat pribadi.

Ajaran agama Islam mengajarkan tentang pentingnya menjaga amanah. Menjaga amanah merupakan tujuan dari merahasiakan pesan atau informasi yang diberikan. Dalam Al-Quran dijelaskan anjuran untuk bersikap amanah, yaitu terdapat di dalam surat an-Nisa’ ayat 58 yang berbunyi :

إِنَّ اللَّهَ يَأْمُرُكُمْ أَنْ تُؤَدُّوا الْأَمَانَاتِ إِلَى أَهْلِهَا وَإِذَا حَكَمْتُمْ بَيْنَ النَّاسِ أَنْ تَحْكُمُوا بِالْعَدْلِ إِنَّ اللَّهَ نِعِمَّا يَعِظُكُمْ بِهِ إِنَّ اللَّهَ كَانَ سَمِيعًا بَصِيرًا

"Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha mendengar lagi Maha Melihat" (QS. An-Nisa': 58).

Maka untuk menjalankan ajaran tersebut dalam proses pertukaran data atau informasi diperlukan solusi untuk menjaga amanah yang diberikan tetap terjaga dan dapat diterima oleh pihak yang dituju.

Salah satu bidang kajian keamanan citra digital yang dapat digunakan sampai saat ini adalah kriptografi. Enkripsi dan dekripsi adalah dua fungsi yang ada dalam kriptografi. Enkripsi citra digital bertujuan menyandikan citra digital (*plain-image*) sehingga tidak dapat dikenali lagi (*cipher-image*) (Munir, 2012). Metode enkripsi citra digital yang sekarang ini banyak dikembangkan adalah fungsi *Chaos*. *Chaos* digunakan didalam kriptografi karena tiga alasan : (1) sifat *chaos* yang sensitif terhadap nilai awal, (2) *chaos* berkelakuan acak, (3) Nilai-nilai *chaos* tidak mempunyai periode (Sharma, 2010). Algoritma *Arnold Cat Map* adalah salah satu algoritma kriptografi yang menggunakan skema transposisi berbasis fungsi *Chaos* dalam melakukan enkripsi citra digital. Teknik ini menggunakan kunci iterasi atau jumlah perulangan dalam menjalankan algoritma *Arnold Cat Map* dan dua variabel lainnya untuk membentuk suatu matriks.

Penelitian Ronsen Purba & Arwin Halim pada tahun 2014 menyatakan bahwa penggunaan algoritma *Arnold Cat Map* saja dalam melakukan enkripsi citra digital memiliki kelemahan dalam hal iterasi. Dalam penelitian Engelbert Eric Setiawan pada tahun 2016 menyatakan bahwa algoritma *Hill Cipher* cukup baik untuk

digunakan sebagai metode enkripsi citra digital. Karena sifat dasarnya sebagai linier kombinator, *Hill Cipher* mampu menyebarkan informasi (dalam hal ini, intensitas warna) sehingga cukup resisten terhadap *statistical attack.* Kemudian, pada penelitian Kromodimoeljo pada tahun 2010 menyatakan bahwa untuk menghasilkan algoritma enkripsi citra yang tangguh dari serangan kriptanalis tidak cukup hanya dengan menggunakan satu algoritma enkripsi. Hal ini dikarenakan kemampuan komputasi yang semakin meningkat, sehingga dibutuhkan algoritma tambahan untuk membuat hasil enkripsi yang tahan terhadap serangan atau kriptanalis.

Pada penelitian ini akan menggunakan dua algoritma enkripsi dan dekripsi citra digital berbasis invers dan tranposisi matriks dengan menggabungkan algoritma *Arnold Cat Map* dan *Hill Cipher*. Algoritma *Hill Cipher* merupakan salah satu teknik penyandian teks, tetapi dengan melakukan perubahan perhitungan pada nilai RGB (*Red Green Blue*) dalam citra digital maka *Hill Cipher* juga dapat dipakai untuk menyandikan citra digital. *Hill Cipher* menggunakan matriks persegi (*square*) sebagai kunci dalam proses penyandiannya, karena hanya melibatkan operasi matriks biasa sehingga prosesnya relatif cepat. Kemudian, algoritma *Arnold Cat Map* akan berperan sebagai enkripsi berbasis transposisi yang mana setiap piksel di koordinat (x, y) akan dipetakan pada koordinat baru (x', y').

Oleh karena itu, untuk melakukan enkripsi dan dekripsi citra digital dibutuhkan sebuah aplikasi keamanan informasi yang dapat digunakan secara umum. Aplikasi tersebut akan dibuat berbasis *website* yang akan dikembangkan dengan menggunakan Django. Django dipilih karena memiliki fitur yang dapat mempermudah pengembangan aplikasi, contohnya antarmuka admin yang otomatis

untuk mempermudah proses manipulasi data pada tabel basis data. Selain itu, Django dibangun dengan bahasa pemrograman Python, yang memiliki banyak *library* di dalamnya. Salah satu *library*-nya adalah Pillow yang akan digunakan juga untuk membantu dalam pemrosesan dan pembentukan citra digital. Sehingga dalam penelitian ini akan menjelaskan tentang enkripsi dan dekripsi citra digital menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* yang akan digunakan sebagai pengamanan sebuah informasi data berupa citra digital berbasis *website*.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang tersebut adapun permasalahan yang akan dibahas, yakni :

1. Bagaimana proses enkripsi dan dekripsi citra digital dengan algoritma *Hill Cipher* dan *Arnold Cat Map* ?
2. Bagaimana hasil enkripsi dan dekripsi citra digital dengan algoritma *Hill Cipher* dan *Arnold Cat Map* berbasis *website* ?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari tugas akhir ini, yaitu :

1. Mengetahui proses enkripsi dan dekripsi citra digital dengan algoritma *Hill Cipher* dan *Arnold Cat Map*.
2. Mengetahui hasil enkripsi dan dekripsi citra digital dengan algoritma *Hill Cipher* dan *Arnold Cat Map* berbasis *website.*

1.4 Batasan Masalah

Agar pembahasan dalam penelitian ini tidak meluas dan tidak menimbulkan permasalahan yang baru, maka peneliti memberi batasan sebagai berikut :

1. Kunci yang digunakan pada proses enkripsi dan dekripsi menggunakan algoritma *Hill Cipher* adalah matriks dengan ukuran 2×2.

1.5 Manfaat Penelitian

Hasil penelitian ini akan berupa aplikasi berbasis *website* yang diharapkan dapat memberikan manfaat di antaranya :

1. Bagi institusi pendidikan, penelitian ini bisa menjadi rujukan bagi penelitian-penelitian yang akan dikembangkan selanjutnya terutama pada bidang pengamanan data citra digital.
2. Bagi institusi yang membutuhkan pengamanan data citra digital, penelitian ini bisa menjadi salah satu alternatifnya.

1.6 Sistematika Penulisan

Dalam penulisan penelitian ini, penulis menggunakan sistematika yang terdiri dari empat bab, dan masing-masing bab dibagi ke dalam subbab dengan sistematika penulisan sebagai berikut.

Bab I Pendahuluan

Pada bab ini membahas tentang latar belakang, rumusan masalah, tujuan penelitan, batasan masalah, manfaat penelitian, metode penelitian, dan sistematika penulisan.

Bab II Kajian Pustaka

Bab ini menjelaskan tentang gambaran umum dari teori yang mendasari pada pembahasan. Teori-teori penunjang yang digunakan dalam bab ini meliputi citra digital, kriptografi, algoritma *Hill Cipher*, algoritma *Arnold Cat Map, Structural Similarity Index Metrics* (SSIM), Django, dan Pillow.

Bab III Metode Penelitian

Bab ini menjelaskan tentang langkah-langkah peneliti melakukan penelitian yaitu meliputi jenis penelitian, data dan sumber data, dan tahap penelitian.

Bab IV Pembahasan

Bab ini menjelaskan tentang pembahasan dari hasil enkripsi dan dekripsi citra digital menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* serta berisi implementasi algoritma tersebut ke dalam bentuk *website*.

Bab IV Penutup

Pada bab ini berisi kesimpulan dari pembahasan yang sesuai dengan hasil penelitian yang telah diperoleh, yang selanjutnya dapat digunakan sebagai saran untuk pembaca dan peneliti selanjutnya.

BAB II
KAJIAN PUSTAKA

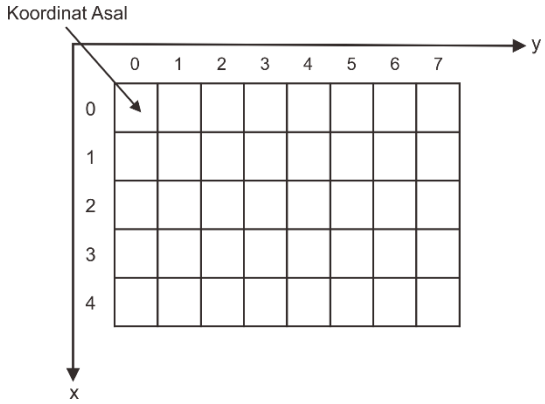
2.1 Citra Digital

Citra digital (*image*) adalah istilah lain untuk gambar. Sebagai salah satu komponen multimedia yang memegang peranan sangat penting dalam bentuk informasi visual, citra mempunyai karakteristik yang tidak dimiliki oleh data teks, yaitu kaya dengan informasi (Sutoyo, dkk., 2009).

Dalam konteks yang lebih luas, pengolahan citra digital mengacu pada pemrosesan setiap data 2 dimensi. Representasi citra dari fungsi kontinu menjadi nilai-nilai diskrit disebut pencitraan (*imaging*) atau digitalisasi. Untuk mengubah bentuk kontinu ke bentuk digital, memerlukan dua fungsi yaitu koordinat dan tingkat keabuhan (*gray-level*). Dikritisasi pada nilai koordinat disebut spasial (*sampling*) sedangkan pada tingkat keabuhan (*gray-level*) disebut kwantisasi (*quantization*) (Gonzales, 2002).

2.1.1 Matriks Citra Digital

Suatu citra digital dapat didefinisikan sebagai fungsi $f(x,y)$ berukuran M baris dan N kolom, dengan x dan y adalah koordinat spasial, dan amplitudo f di titik koordinat (x,y) dinamakan intensitas atau tingkat keabuan dari citra pada titik tersebut (Nafi'iyah, 2015). Gambar 2.1 menunjukkan posisi koordinat citra digital.



Gambar 2.1 Koordinat Citra Digital

Notasi Gambar 2.1 memungkinkan untuk ditulis dalam citra digital $M \times N$ sebagai berikut.

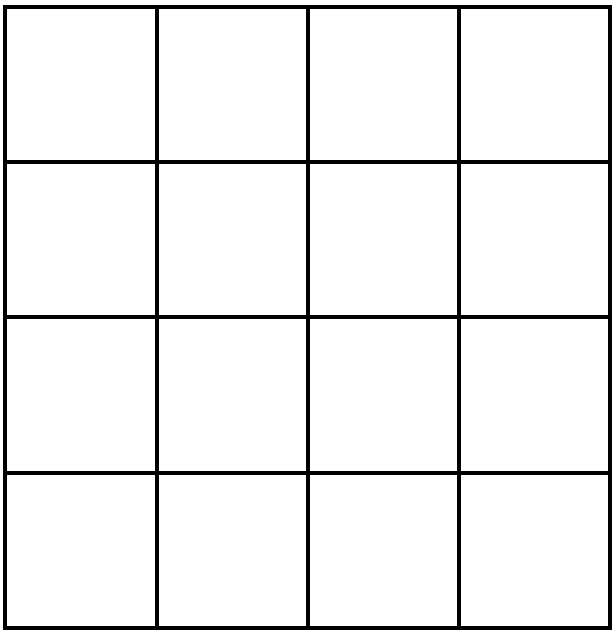
$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & f(1,1) & \dots & f(1,N-1) \\ \dots & \dots & \dots & \dots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{bmatrix}$$

Pada ruas kanan dari persamaan adalah definisi dari citra digital. Setiap elemen dari matriks tersebut disebut dengan elemen piksel. Beberapa notasi matriks menotasikan citra digital dan elemennya sebagai berikut.

$$\boldsymbol{A} = \begin{bmatrix} a_{0,0} & a_{0,1} & \dots & a_{0,N-1} \\ a_{1,0} & a_{1,1} & \dots & a_{1,N-1} \\ \dots & \dots & \dots & \dots \\ a_{M-1,0} & a_{M-1,1} & \dots & a_{M-1,N-1} \end{bmatrix}$$

Secara jelas, $a_{ij} = f(x = i, y = j) = f(i,j)$ jadi persamaan dari matriks $f(x,y)$ dan matriks $\boldsymbol{A}$ merupakan matriks identik.

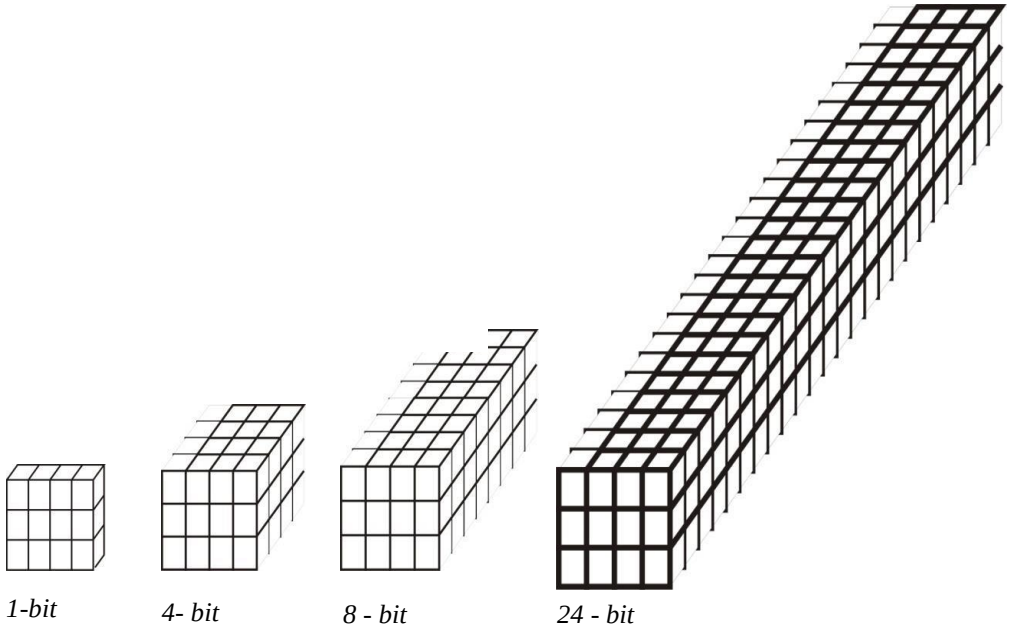
Untuk mempermudah penggambaran matriks citra dapat digunakan kumpulan persegi yang akan mewakili setiap entri dalam matriks citra seperti pada Gambar 2.2.



Gambar 2.2 Koordinat Citra Digital Berukuran 4 X 4 dalam Visualisasi Persegi

2.1.2 Jenis Citra Digital dan Komposisi Warna

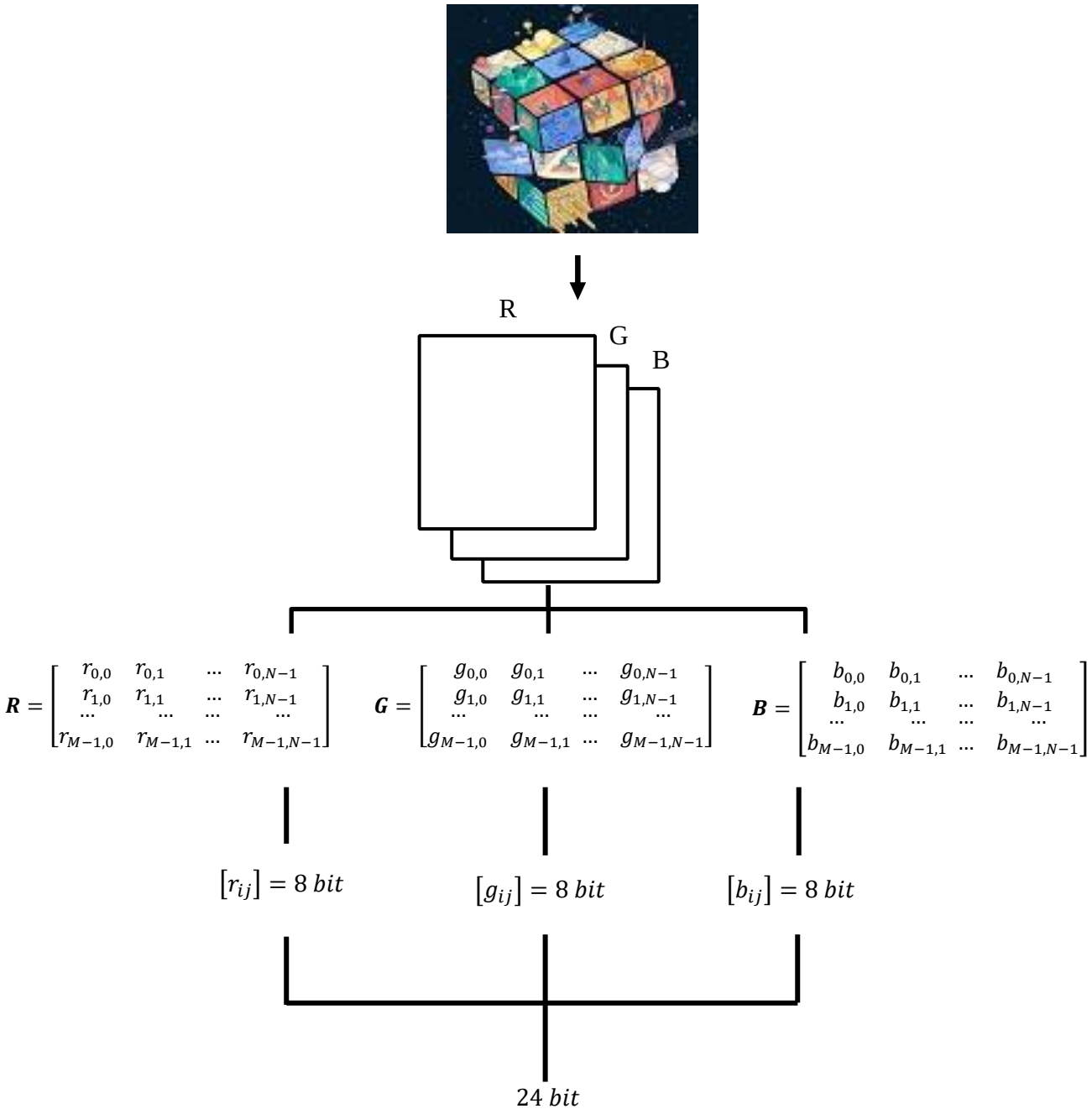
Dalam sebuah citra digital terdapat komposisi antara koordinat dan tingkat keabuhan (*Gray-Level*), pada Gambar 2.2 koordinat diartikan sebagai posisi entri dalam matriks citra digital maka tingkat keabuhan merupakan entri/nilai dari setiap entri/piksel citra digital yang akan menentukan warna pada tiap piksel. Tingkat keabuhan ini berkaitan dengan *binary digit* (bit) yang tersusun atas bilangan 0 dan 1. Semua varian warna untuk piksel diperoleh dari tiga warna dasar yaitu merah, hijau dan biru. Setiap warna dasar dipresentasikan dengan 1 *byte*; citra digital 24 bit menggunakan 3 *byte* per piksel untuk mempresentasikan suatu nilai (Ariyus, 2006). Hubungan antara koordinat citra digital dengan *gray -level* dapat dilihat pada gambar berikut.



Gambar 2.3 Visualisasi *Gray-level* dalam Citra Digital

Pada Gambar 2.3 masing-masing kubus mempresentasikan data dengan citra digital yang berukuran 4 × 3 piksel dengan bentuk kubus memanjang ke belakang yang mempresentasikan jumlah bit yang digunakan dalam tiap piksel. Kedalaman 8-bit atau kurang mempresentasikan citra digital *grayscale* sedangkan citra digital 24-bit mengandung warna RGB (*Red Green Blue*) (Binanto, 2010).

Berikut ini adalah penggambaran matriks citra digital yang memiliki warna RGB. Citra digital disebut citra digital RGB dikarenakan dalam citra digital tersebut ada tiga *layer* yang akan menciptakan lebih dari 16 juta jenis warna.



Gambar 2.4 Matriks dalam Citra Digital RGB

Setiap entri dalam matriks R, G atau B memiliki rentang nilai [0,255], di mana tiap nilai jika diubah kebentuk biner memiliki nilai tersusun atas 8 bit atau 8 susunan angka biner. Tiap entri tersebut dalam rentang nilai [0,255] memiliki tingkat keabuan tersendiri. Sedangkan pada citra digital *grayscale* hanya memiliki satu *layer*, sehingga warna yang dihasilkan hanya warna *gray* karena tidak ada susunan *layer* lain yang akan menciptakan kombinasi warna yang lebih banyak (Maulidah, 2018).

2.2 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (Munir, 2006). Kata "seni" di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (*plain-text*) menjadi suatu pesan dalam bahasa sandi (*cipher-text*).

$C = E(M)$.

di mana :

M = pesan asli

E = proses enkripsi

C = pesan yang telah dienkripsi

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

$M = D(C)$

D = proses dekripsi

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci (Muslimin, dkk., 2015).

2.2 *Hill Cipher*

Hill Cipher merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Hill Cipher* diciptakan oleh Lester S. Hill pada tahun 1929 (Forouzan, 2006). Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi. *Hill Cipher* tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

Dasar dari teknik *Hill Cipher* adalah aritmatika modulo terhadap matriks. Dalam penerapan pada citra digital, *Hill Cipher* menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Diberikan citra digital asli (*plain-image)* $\boldsymbol{P}$ dan kunci matriks $\boldsymbol{K} = \begin{bmatrix} k_{11} k_{12} \\ k_{21} k_{22} \end{bmatrix}$, dengan kondisi $\boldsymbol{K}$ harus memiliki *invers* matriks atau dapat disebut *invertible.* Enkripsi citra digital berdasarkan *Hill Cipher* bergantung pada pembagian piksel citra digital $\boldsymbol{P}$ menjadi matriks berukuran sama,

dan kemudian sandi *Hill Cipher* diterapkan pada masing-masing matriks tersebut. Berdasarkan matriks $\boldsymbol{P}$ dari dua piksel berturut-turut p_1, p_2 dari citra digital asli (*plain-image)* $\boldsymbol{P}$. Enkripsi dari matriks $\boldsymbol{P}$ adalah sama dengan matriks sandi $C = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$ berdasarkan persamaan berikut :

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} k_{11} k_{12} \\ k_{21} k_{22} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \ mod\ 256 \qquad (1)$$

Kemudian berdasarkan persamaan (1), citra digital sandi (*cipher-image*) dapat didefinisikan menjadi $\boldsymbol{C} = \boldsymbol{KP}\ mod\ 256$, di mana $\boldsymbol{C} = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$, $K = \begin{bmatrix} k_{11} k_{12} \\ k_{21} k_{22} \end{bmatrix}$, dan $\boldsymbol{P} = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$. Sedangkan untuk mengembalikan hasil dari enkripsi citra digital yakni dekripsi citra digital dapat didefinisikan menjadi $\boldsymbol{P} = \boldsymbol{K^{-1}C}\ mod\ 256$, di mana $\boldsymbol{K^{-1}}$ adalah invers matriks dari $\boldsymbol{K}$(Azza A. Abdo et al., 2020).

2.3 *Arnold Cat Map*

Algoritma *Arnold Cat Map* diperkenalkan pertama kali oleh seorang ahli matematika Rusia yang bernama Vladimir I. Arnold, pada tahun 1960 yang mendemonstrasikan algoritmanya tersebut dengan menggunakan citra digital kucing (Purba, 2014).

Arnold Cat Map adalah *chaotic* dua dimensi yang dapat digunakan untuk mengubah posisi piksel citra digital tanpa menghilangkan informasi apapun dari citra digital, posisi piksel dari citra digital dapat diasumsikan dengan $S = \{(x.y) \mid x.y = 0.1.2\ ,,, N-1\}$.

Sehingga algoritma *Arnold Cat Map* dapat dituliskan dengan persamaan berikut :

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = [A] \begin{bmatrix} x \\ y \end{bmatrix} \ (mod\ N)$$

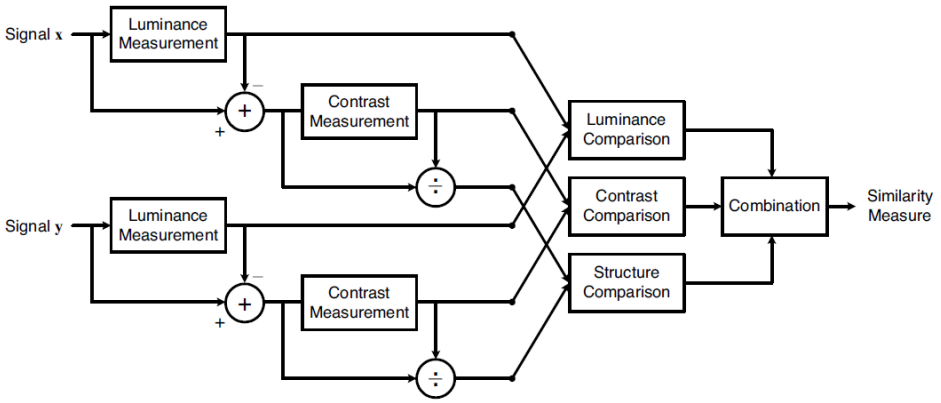
$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ (mod\ N)$$

Di mana a dan b adalah bilangan bulat positif sehingga determinan $[A] = 1$. $(x'.y')$ adalah posisi baru dari posisi piksel asli $(x.y)$ ketika algoritma *Arnold Cat Map* dilakukan satu kali. Hasil setelah penerapan *Arnold Cat Map* dengan jumlah iterasi dari iterasi d akan berupa citra digital acak yang berisi semua nilai piksel yang sama dari citra digital aslinya. Jumlah iterasi d yang harus diselesaikan tergantung pada parameter $a.b$ dan ukuran N citra digital asli (*plain-image*). Jadi algoritma *Arnold Cat Map* memiliki parameter $a.b.$ dan jumlah iterasi d, semuanya dapat digunakan sebagai kunci rahasia (Hariyanto, 2016).

2.4 *Structural Similarity Index Metrics* (SSIM)

SSIM dikenal sebagai kualitas metric yang digunakan untuk mengukur kemiripan diantara 2 buah citra dan dipercaya berkorelasi dengan kualitas persepsi Human Visual System (HVS) (Z. Wang, dkk., 2004). Model SSIM dibuat dengan memperhatikan 3 buah faktor yaitu *loss of correlation*, *luminance distortion* dan *contrast distortion*. Persamaan SSIM dapat dilihat pada (2).

$$SSIM(f.g) = l(f.g)c(f.g)s(f.g) \qquad (2)$$



Gambar 2.5 Diagram Sistem Pengukuran SSIM

Dengan faktor-faktor lainnya dapat dilihat pada (3)

$$\begin{cases} l(f.g) = \frac{2\mu_f\mu_g+C_1}{\mu_f^2+\mu_g^2+C_1} \\ c(f.g) = \frac{2\sigma_f\sigma_g+C_2}{\sigma_f^2+\sigma_g^2+C_2} \\ s(f.g) = \frac{2\sigma_{fg}+C_3}{\sigma_f\sigma_g+C_3} \end{cases} \quad (3)$$

$l(f.g)$ adalah perbandingan luminansi yang mengukur kemiripan nilai luminansi rerata 2 citra (μ_f dan μ_g). Nilai maksimal dari nilai $l(f.g)$ sama dengan 1. Nilai maksimal akan tercapai bila $\mu_f = \mu_g$.

$c(f.g)$ adalah perbandingan nilai kontras yang mengukur kemiripan nilai standar deviation 2 citra yaitu σ_f dan σ_g. Nilai maksimal dari nilai $c(f.g)$ sama dengan 1. Nilai maksimal akan tercapai bila $\sigma_f = \sigma_g$.

$s(f.g)$ adalah perbandingan struktur yang mengukur koefisien korelasi di antara 2 citra $(f.g), \sigma_{fg}$ adalah nilai kovarian antara f dan g.

Jangkauan nilai SSIM adalah 0 sampai dengan 1. Nilai "0" menunjukkan kedua citra yang dibandingkan tidak berkorelasi sedangkan nilai "1" menunjukkan kedua citra yang dibandingkan sama persis $f = g$.

$C_1. C_2.$ dan C_3 adalah suatu konstanta agar penyebut tidak sama dengan nol (Wulandari, 2017).

2.5 Django

Django adalah sebuah sebuah *high level web framework open source* yang menggunakan bahasa pemrograman Python, yang mengikuti pola arsitektur MVC (*Model-View-Controllers*). Django didukung oleh *the Django Software*

Foundation, sebuah organisasi independent yang didirikan sebagai sebuah perusahaan non-profit. Django diklaim sangat cepat, sangat memperhatikan keamanan (salah satunya- dengan fitur csrf_token), dan sangat *scalable* yakni mampu mengukur kecepatan dan fleksibilitas web dengan *traffic* tersibuk dan yang membutuhkan proses pengolahan data yang sangat besar (Cahyono, 2019).

2.6 Pillow (PIL)

Pillow (PIL) merupakan pustaka *Python Imaging* berbasis *Open Source* yang digagas oleh Fredrik Lundh. Pustaka *Python Imaging* ditujukan untuk menambahkan kemampuan pemrosesan citra digital ke interpreter *Python*. Pustaka ini menyediakan dukungan format file yang ekstensif, representasi internal yang efisien, dan kemampuan pemrosesan gambar yang cukup kuat (Alex Clark, 2010).

2.7 Kajian Keislaman

Secara bahasa, amanah berasal dari kata bahasa Arab : أَمِنَ يَأْمَنُ أَمْناً yang berarti aman/tidak takut. Dengan kata lain, aman adalah lawan dari kata takut. Dari sinilah diambil kata amanah yang merupakan lawan dari kata khianat. Dinamakan aman karena orang akan merasa aman menitipkan sesuatu kepada orang yang amanah.

Secara istilah, ada sebagian orang yang mengartikan kata amanah secara sempit yaitu menjaga barang titipan dan mengembalikannya dalam bentuk semula. Padahal sebenarnya hakikat amanah itu jauh lebih luas. Amanah menurut terminologi Islam adalah setiap yang dibebankan kepada manusia dari Allah *Ta'ala* seperti kewajiban-kewajiban agama, atau dari manusia seperti titipan harta.

Dalam Al-Quran dijelaskan anjuran untuk bersikap amanah, yaitu terdapat di dalam surat an-Nisa' ayat 58. Berdasarkan ayat tersebut, Al-Imam Ibnu Katsir memberikan penjelasan dalam tafsirnya, "Allah mengabarkan bahwa Dia memerintahkan untuk menunaikan amanah kepada yang berhak menerimanya". Dalam hadits al-Hasan dari Samurah, bahwa Rasulullah bersabda :

أَدِّ الْأَمَانَةَ إِلَى مَنِ ائْتَمَنَكَ، وَلاَ تَخُنْ مَنْ خَانَكَ

"Tunaikanlah amanah pada orang yang memberikan amanah itu kepadamu, dan jangan kau khianati orang yang pernah mengkhianatimu" (HR. Al-Imam Ahmad dan Ahlus Sunan).

Hal itu mencakup seluruh amanah yang wajib bagi manusia, berupa hak-hak Allah terhadap para hamba-Nya, seperti shalat, zakat, puasa, kafarat, nadzar dan selain dari itu, yang kesemuanya adalah amanah yang diberikan tanpa pengawasan hamba-Nya yang lain.

Serta amanah yang berupa hak-hak sebagian hamba dengan hamba lainnya, seperti titipan berupa pesan atau barang, yang kesemuanya adalah amanah yang dilakukan tanpa pengawasan saksi. Hal ini menandakan penting untuk menyampaikan pesan atau informasi hanya kepada orang yang berhak menerimanya seperti dengan menerapkan metode enkripsi pada pesan yang berbentuk citra digital.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Dalam penelitian ini jenis penelitian yang digunakan adalah metode eksperimen. Penelitian eksperimen diartikan sebagai pendekatan penelitian kuantitatif yang paling penuh, artinya memenuhi semua persyaratan untuk menguji hubungan sebab akibat. Alasan peneliti menggunakan metode eksperimen karena sejalan dengan rumusan masalah pada penelitian ini yaitu mengetahui hasil enkripsi dan dekripsi citra digital dengan algoritma *Hill Cipher* dan *Arnold Cat Map* berbasis *website*.

3.2 Data dan Sumber Data

Data yang digunakan dalam penelitian ini berupa data citra digital dengan ukuran $N \times N$ dengan N merupakan bilangan genap positif dan format *file *.jpg, *jpeg,* atau **.png* yang diperoleh dari *standard image test*.

3.3 Tahapan Penelitian

Pada penelitian ini proses enkripsi dan dekripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* dilakukkan dengan tahapan sebagai berikut.

1. Proses enkripsi dengan algoritma *Hill Cipher* dan *Arnold Cat Map* pada citra digital.
    a. Menentukan tiga bilangan bulat (a, b, d) yang akan digunakan sebagai kunci.
    b. Menyiapkan *plain-image* dalam bentuk citra digital berukuran $N \times N$ dengan N merupakan bilangan genap positif.

c. Mengubah *plain-image* ke dalam bentuk matriks *plain-image* yang mana setiap entri matriks tersebut terdiri dari nilai tingkat keabuan warna R (*Red*), G (*Green*) dan B (*Blue*) di setiap piksel pada *plain-image*.

d. Membuat kunci dalam bentuk matriks berukuran 2×2 dengan mensubstitusikan dua bilangan bulat (a, b) ke dalam formula matriks yang telah ditentukan.

e. Mengoperasikan matriks kunci dengan tiap dua entri pada matriks *plain-image* menggunakan operasi perkalian matriks. Kemudian, hasil dari setiap perkalian tersebut dimodulokan dengan 256 sehingga setiap entri pada matriks hasil enkripsi tetap berada pada interval nilai tingkat keabuan warna R (*Red*), G (*Green*) dan B (*Blue*).

f. Diperoleh matriks *cipher-image* (HC) atau matriks citra digital hasil enkripsi menggunakan algoritma *Hill Cipher*.

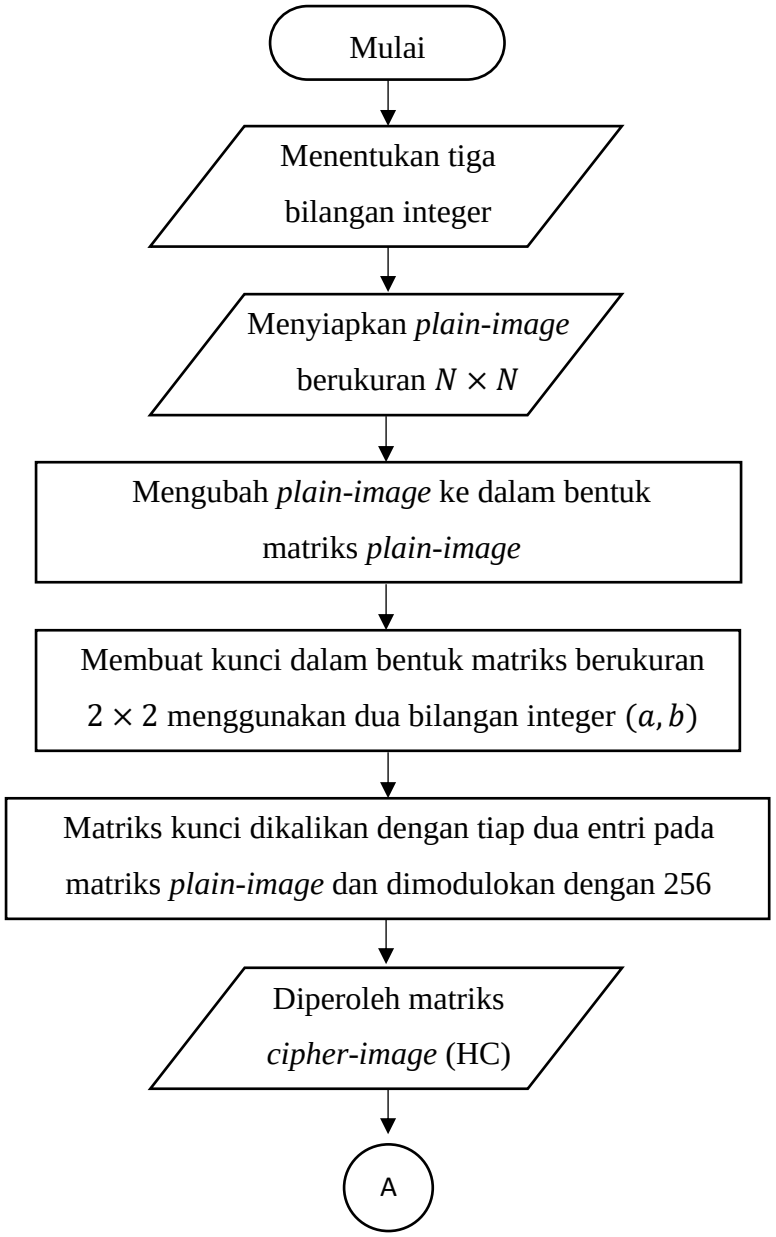
g. Mensubstitusikan dua bilangan bulat (a, b) yang telah ditentukan dan panjang matriks *cipher-image* (HC) (N) ke dalam persamaan *Arnold Cat Map.*

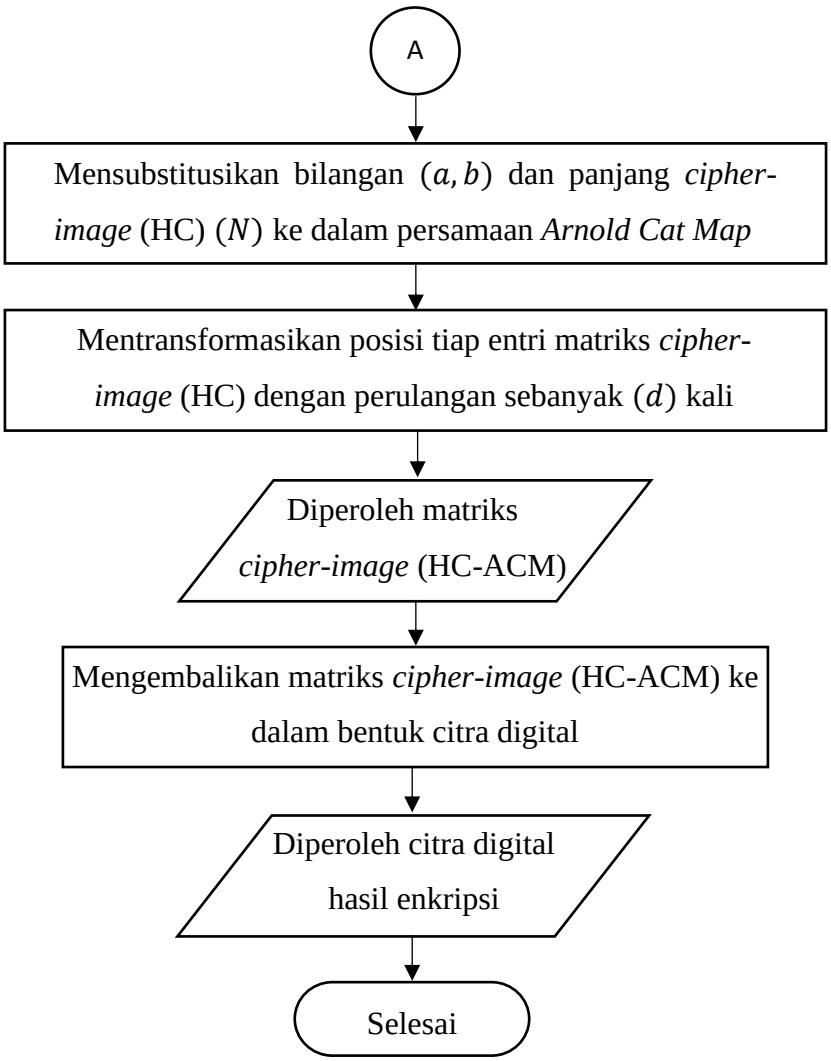
h. Mentransformasikan posisi tiap entri matriks *cipher-image* (HC) ke titik lain menggunakan persamaan *Arnold Cat Map* dengan perulangan sebanyak bilangan bulat (d) kali.

i. Diperoleh matriks *cipher-image* (HC-ACM) atau matriks citra digital hasil enkripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map*.

j. Mengembalikan matriks *cipher-image* (HC-ACM) ke dalam bentuk citra digital.

k. Diperoleh citra digital hasil enkripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* atau *cipher-image* (HC-ACM).





Gambar 3.1 *Flowchart* Proses Enkripsi Citra Digital Menggunakan Algoritma *Hill Cipher* dan *Arnold Cat Map*

2. Proses dekripsi dengan algoritma *Hill Cipher* dan *Arnold Cat Map* pada citra digital.
    a. Menentukan tiga bilangan bulat (a, b, d) yang sama dengan bilangan yang digunakan sebagai kunci pada proses enkripsi.
    b. Menyiapkan *cipher-image* (HC-ACM) atau citra digital hasil enkripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* berukuran $N \times N$ dengan N merupakan bilangan genap positif.

c. Mengubah *cipher-image* (HC-ACM) ke dalam bentuk matriks *cipher-image* (HC-ACM) yang mana setiap entri matriks tersebut terdiri dari nilai tingkat keabuan warna R (*Red*), G (*Green*) dan B (*Blue*) di setiap piksel pada *cipher-image (*HC-ACM*)*.

d. Mensubstitusikan dua bilangan bulat (a, b) dan panjang citra digital (N) dari *cipher-image* $(\mathrm{HC} - \mathrm{ACM})$ ke dalam persamaan *Arnold Cat Map.*

e. Mengembalikan posisi tiap entri matriks *cipher-image* (HC-ACM) ke posisi semula pada *cipher-image* (HC) dengan melakukan transformasi titik menggunakan persamaan *Arnold Cat Map* dengan perulangan sebanyak bilangan bulat (d) kali.

f. Diperoleh matriks *cipher-image* (HC) atau matriks citra digital hasil enkripsi menggunakan algoritma *Hill Cipher*.

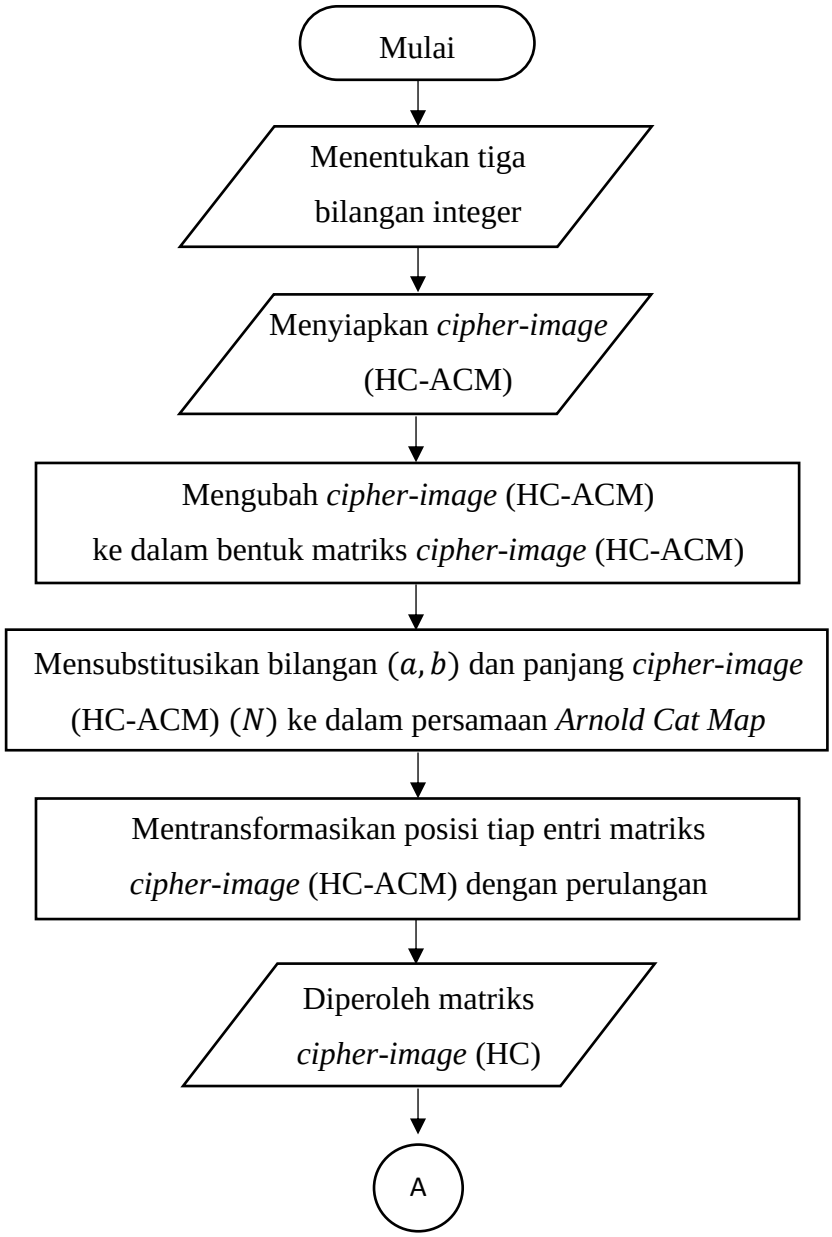
g. Membuat kunci dalam bentuk matriks berukuran 2×2 dengan mensubstitusikan dua bilangan bulat (a, b) ke dalam formula matriks yang telah ditentukan dan melakukan operasi *invers* matriks pada matriks kunci tersebut.

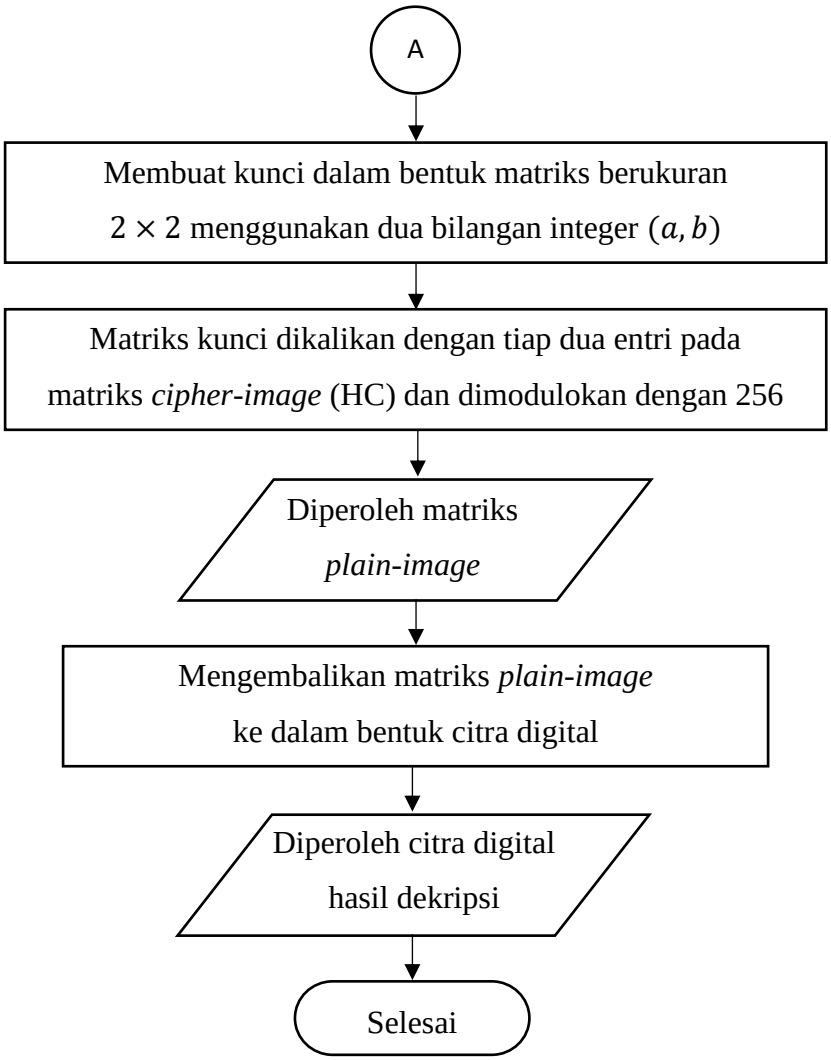
h. Mengoperasikan matriks kunci yang telah di-*invers* dengan tiap dua entri pada matriks *cipher-image* (HC) menggunakan operasi perkalian matriks. Kemudian, hasil dari setiap perkalian tersebut dimodulokan dengan 256 sehingga setiap entri pada matriks hasil dekripsi tetap berada pada interval nilai tingkat keabuan dari R (*Red*), G (*Green*) dan B (*Blue*).

i. Diperoleh matriks *plain-image* atau matriks citra digital hasil dekripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map.*

j. Mengembalikan matriks *plain-image* ke dalam bentuk citra digital.

k. Diperoleh citra digital hasil dekripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map*.





Gambar 3.2 *Flowchart* Proses Dekripsi Citra Digital Menggunakan Algoritma *Hill Cipher* dan *Arnold Cat Map*

BAB IV
PEMBAHASAN

4.1 Proses Enkripsi dan Dekripsi Citra Digital

4.1.1 Proses Enkripsi Citra Digital dengan Algoritma *Hill Cipher* dan *Arnold Cat Map*

Berikut ini contoh penerapan enkripsi dengan algoritma *Hill Cipher* dan *Arnold Cat Map* pada citra digital berukuran 4 × 4 piksel. Penerapan dilakukan pada *plain-image* RGB, sebuah citra digital RGB dapat tersusun dengan tiga *layer*.

1. Misalkan kunci yang digunakan adalah $a = 3$. $b = 4$ dan $d = 1$.
2. *Plain-image* RGB berukuran 4 × 4 piksel akan dienkripsi dengan kunci $\boldsymbol{K}$. Misalkan *plain-image* sebagai berikut.

Gambar 4.1 *Plain-image* RGB Ukuran 4 X 4

3. Selanjutnya *plain-image* berukuran 4 × 4 piksel dibaca sebagai matriks *plain-image* ($\boldsymbol{P}$) berordo 4 × 4 sebagai berikut.

$$\boldsymbol{P} = \begin{bmatrix} [48 & 49 & 110] & [44 & 135 & 118] & [19 & 78 & 49] & [117 & 42 & 167] \\ [69 & 17 & 17] & [200 & 57 & 50] & [175 & 118 & 44] & [137 & 59 & 206] \\ [98 & 84 & 24] & [59 & 135 & 104] & [55 & 152 & 164] & [96 & 108 & 128] \\ [56 & 71 & 102] & [20 & 39 & 77] & [36 & 36 & 36] & [48 & 49 & 110] \end{bmatrix}$$

4. Kunci $\boldsymbol{K}$ adalah kunci enkripsi dari algoritma *Hill Cipher* berbentuk matriks yang dibentuk dengan formula matriks $\boldsymbol{K} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix}$, Sehingga diperoleh matriks $\boldsymbol{K}$ sebagai berikut.

$$\boldsymbol{K} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}$$

5. Kemudian diambil masing-masing dua entri dalam matriks *plain-image* (***P***) yang didefinisikan dengan $\begin{bmatrix} \boldsymbol{p_{i.j}} \\ \boldsymbol{p_{i.j+1}} \end{bmatrix}$ ($i =$ indeks baris matriks *plain-image* (***P***) dan $j =$ indeks kolom matriks *plain-image* (***P***)) dan dibentuk dalam satu matriks dengan ukuran 2×3. Setelah itu, dilakukan operasi perkalian matriks dengan kunci matriks $\boldsymbol{K}$ yang mana hasil dari perkalian matriks tersebut dimodulokan dengan 256 sehingga dihasilkan dua entri yang dienkripsi $\begin{bmatrix} \boldsymbol{c_{i.j}} \\ \boldsymbol{c_{i.j+1}} \end{bmatrix}$.

6. Berikut proses perkalian masing-masing dua entri dalam matriks *plain-image* (***P***) dengan kunci matriks $\boldsymbol{K}$.

$$\begin{bmatrix} \boldsymbol{p_{0.0}} \\ \boldsymbol{p_{0.1}} \end{bmatrix} = \begin{bmatrix} 48 & 49 & 110 \\ 44 & 135 & 118 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{c_{0.0}} \\ \boldsymbol{c_{0.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{0.0}} \\ \boldsymbol{c_{0.1}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 48 & 49 & 110 \\ 44 & 135 & 118 \end{bmatrix} \ (mod\ 256)$$

$$= \begin{bmatrix} 180 & 198 & 208 \\ 252 & 159 & 182 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{0.2}} \\ \boldsymbol{p_{0.3}} \end{bmatrix} = \begin{bmatrix} 19 & 78 & 49 \\ 117 & 42 & 167 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{c_{0.2}} \\ \boldsymbol{c_{0.3}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{0.2}} \\ \boldsymbol{c_{0.3}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 19 & 78 & 49 \\ 117 & 42 & 167 \end{bmatrix} \ (mod\ 256)$$

$$= \begin{bmatrix} 114 & 204 & 38 \\ 61 & 90 & 63 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{1.0}} \\ \boldsymbol{p_{1.1}} \end{bmatrix} = \begin{bmatrix} 69 & 17 & 17 \\ 200 & 57 & 50 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{c_{1.0}} \\ \boldsymbol{c_{1.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{1.0}} \\ \boldsymbol{c_{1.1}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 69 & 17 & 17 \\ 200 & 57 & 50 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 157 & 188 & 167 \\ 60 & 41 & 206 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{1.2}} \\ \boldsymbol{p_{1.3}} \end{bmatrix} = \begin{bmatrix} 175 & 118 & 44 \\ 137 & 59 & 206 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{c_{1.2}} \\ \boldsymbol{c_{1.3}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{1.2}} \\ \boldsymbol{c_{1.3}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 175 & 118 & 44 \\ 137 & 59 & 206 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 74 & 39 & 150 \\ 177 & 215 & 38 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{2.0}} \\ \boldsymbol{p_{2.1}} \end{bmatrix} = \begin{bmatrix} 98 & 84 & 24 \\ 59 & 135 & 104 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{c_{2.0}} \\ \boldsymbol{c_{2.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{2.0}} \\ \boldsymbol{c_{2.1}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 98 & 84 & 24 \\ 59 & 135 & 104 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 19 & 233 & 80 \\ 135 & 43 & 168 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{2.2}} \\ \boldsymbol{p_{2.3}} \end{bmatrix} = \begin{bmatrix} 55 & 152 & 164 \\ 96 & 108 & 128 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{c_{2.2}} \\ \boldsymbol{c_{2.3}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{2.2}} \\ \boldsymbol{c_{2.3}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 55 & 152 & 164 \\ 96 & 108 & 128 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 87 & 220 & 36 \\ 188 & 220 & 16 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{3.0}} \\ \boldsymbol{p_{3.1}} \end{bmatrix} = \begin{bmatrix} 56 & 71 & 102 \\ 20 & 39 & 77 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{c_{3.0}} \\ \boldsymbol{c_{3.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{3.0}} \\ \boldsymbol{c_{3.1}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 56 & 71 & 102 \\ 20 & 39 & 77 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 116 & 188 & 77 \\ 228 & 23 & 129 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{3.2}} \\ \boldsymbol{p_{3.3}} \end{bmatrix} = \begin{bmatrix} 36 & 36 & 36 \\ 48 & 49 & 110 \end{bmatrix} \rightarrow \begin{bmatrix} c_{3.2} \\ c_{3.3} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{3.2}} \\ \boldsymbol{c_{3.3}} \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 36 & 36 & 36 \\ 48 & 49 & 110 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 180 & 183 & 110 \\ 0 & 13 & 38 \end{bmatrix}$$

7. Setelah semua entri dikalikan dengan kunci matriks $\boldsymbol{K}$, hasil dari setiap dua entri yang dienkripsi $\begin{bmatrix} \boldsymbol{c_{i.j}} \\ \boldsymbol{c_{i.j+1}} \end{bmatrix}$ dimasukkan ke dalam matriks *cipher-image* ($\boldsymbol{C}$) maka diperoleh.

$\boldsymbol{C}$

$$= \begin{bmatrix} [180 & 198 & 208] & [252 & 159 & 182] & [114 & 204 & 38] & [61 & 90 & 63] \\ [157 & 188 & 167] & [60 & 41 & 206] & [74 & 39 & 150] & [177 & 215 & 38] \\ [19 & 233 & 80] & [135 & 43 & 168] & [87 & 220 & 36] & [188 & 220 & 16] \\ [116 & 188 & 77] & [228 & 23 & 129] & [180 & 183 & 110] & [0 & 13 & 38] \end{bmatrix}$$

8. Memasukkan kunci $a = 3$ dan $b = 4$ serta $N = 4$ ke dalam persamaan enkripsi *Arnold Cat Map*.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ (mod\ N)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 3 & 13 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ (mod\ 4)$$

9. Berikut proses transformasi titik matriks awal ($\boldsymbol{C}$) pada matriks transpose ($\boldsymbol{C^T}$).

Jika $\boldsymbol{c_{x.y}} \in \boldsymbol{C}$ dan $\boldsymbol{c^T_{x.y}} \in \boldsymbol{C^T}$ dengan titik $x = 0.1.2.3$ dan $y = 0.1.2.3$

untuk baris $x = 0$ dan kolom $y = 0$, dengan entri

$\boldsymbol{c_{0.0}} = [180 \quad 198 \quad 208]$

$$\boldsymbol{c_{0.0}} = [180 \quad 198 \quad 208] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \ (mod\ 4)$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c^T_{0.0}}$$

untuk baris $x = 0$ dan kolom $y = 1$, dengan entri

$\boldsymbol{c_{0.1}} = [252 \quad 159 \quad 182]$

$$\boldsymbol{c_{0.1}} = [252 \quad 159 \quad 182] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \ (mod\ 4)$$

$$= \begin{bmatrix} 3 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{3.1}^{T}}$$

untuk baris $x = 0$ dan kolom $y = 2$, dengan entri

$$\boldsymbol{c_{0.2}} = [114 \quad 204 \quad 38]$$

$$\boldsymbol{c_{0.2}} = [114 \quad 204 \quad 38] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} \ (mod\ 4)$$

$$= \begin{bmatrix} 2 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{2.2}^{T}}$$

untuk baris $x = 0$ dan kolom $y = 3$, dengan entri

$$\boldsymbol{c_{0.3}} = [61 \quad 90 \quad 63]$$

$$\boldsymbol{c_{0.3}} = [61 \quad 90 \quad 63] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 0 \\ 3 \end{bmatrix} \ (mod\ 4)$$

$$= \begin{bmatrix} 1 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{1.3}^{T}}$$

untuk baris $x = 1$ dan kolom $y = 0$, dengan entri

$$\boldsymbol{c_{1.0}} = [157 \quad 188 \quad 167]$$

$$\boldsymbol{c_{1.0}} = [157 \quad 188 \quad 167] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \ (mod\ 4)$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c_{1.0}^{T}}$$

untuk baris $x = 1$ dan kolom $y = 1$, dengan entri

$$\boldsymbol{c_{1.1}} = [60 \quad 41 \quad 206]$$

$$\boldsymbol{c_{1.1}} = [60 \quad 41 \quad 206] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \ (mod\ 4)$$

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{0.1}^{T}}$$

untuk baris $x = 1$ dan kolom $y = 2$, dengan entri

$$\boldsymbol{c_{1.2}} = [74 \quad 39 \quad 150]$$

$\boldsymbol{c_{1.2}} = [74 \quad 39 \quad 150] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \ (mod\ 4)$

$= \begin{bmatrix} 3 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{3.2}^{T}}$

untuk baris $x = 1$ dan kolom $y = 3$, dengan entri

$\boldsymbol{c_{1.3}} = [177 \quad 215 \quad 38]$

$\boldsymbol{c_{1.3}} = [177 \quad 215 \quad 38] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix} \ (mod\ 4)$

$= \begin{bmatrix} 2 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{2.3}^{T}}$

untuk baris $x = 2$ dan kolom $y = 0$, dengan entri

$\boldsymbol{c_{2.0}} = [19 \quad 233 \quad 80]$

$\boldsymbol{c_{2.0}} = [19 \quad 233 \quad 80] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} \ (mod\ 4)$

$= \begin{bmatrix} 2 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c_{2.0}^{T}}$

untuk baris $x = 2$ dan kolom $y = 1$, dengan entri

$\boldsymbol{c_{2.1}} = [135 \quad 43 \quad 168]$

$\boldsymbol{c_{2.1}} = [135 \quad 43 \quad 168] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} \ (mod\ 4)$

$= \begin{bmatrix} 1 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{1.1}^{T}}$

untuk baris $x = 2$ dan kolom $y = 2$, dengan entri

$\boldsymbol{c_{2.2}} = [87 \quad 220 \quad 36]$

$\boldsymbol{c_{2.2}} = [87 \quad 220 \quad 36] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} \ (mod\ 4)$

$= \begin{bmatrix} 0 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{0.2}^{T}}$

untuk baris $x = 2$ dan kolom $y = 3$, dengan entri

$\boldsymbol{c_{2.3}} = [188 \quad 220 \quad 16]$

$$\boldsymbol{c_{2.3}} = [188 \quad 220 \quad 16] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 3 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{3.3}^{T}}$$

untuk baris $x = 3$ dan kolom $y = 0$, dengan entri

$$\boldsymbol{c_{3.0}} = [116 \quad 188 \quad 77]$$

$$\boldsymbol{c_{3.0}} = [116 \quad 188 \quad 77] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 3 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c_{3.0}^{T}}$$

untuk baris $x = 3$ dan kolom $y = 1$, dengan entri

$$\boldsymbol{c_{3.1}} = [228 \quad 23 \quad 129]$$

$$\boldsymbol{c_{3.1}} = [228 \quad 23 \quad 129] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 2 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{2.1}^{T}}$$

untuk baris $x = 3$ dan kolom $y = 2$, dengan entri

$$\boldsymbol{c_{3.2}} = [180 \quad 183 \quad 110]$$

$$\boldsymbol{c_{3.2}} = [180 \quad 183 \quad 110] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 1 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{1.2}^{T}}$$

untuk baris $x = 3$ dan kolom $y = 3$, dengan entri

$$\boldsymbol{c_{3.3}} = [0 \quad 13 \quad 38]$$

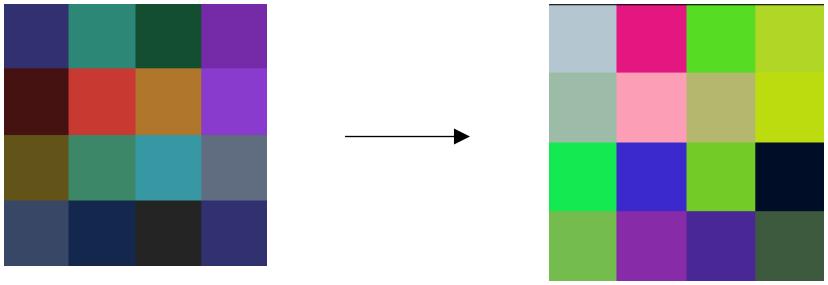
$$\boldsymbol{c_{3.3}} = [0 \quad 13 \quad 38] \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 0 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{0.3}^{T}}$$

10. Karena iterasi d = 1 maka proses transformasi hanya dilakukan satu kali, Sehingga hasil transformasi menghasilkan matriks $\boldsymbol{C^T}$ dengan entri sebagai berikut.

$$\boldsymbol{C^T} = \begin{bmatrix} [180 & 198 & 208] & [228 & 23 & 129] & [87 & 220 & 36] & [177 & 215 & 38] \\ [157 & 188 & 167] & [252 & 159 & 182] & [180 & 183 & 110] & [188 & 220 & 16] \\ [19 & 233 & 80] & [60 & 41 & 206] & [114 & 204 & 38] & [0 & 13 & 38] \\ [116 & 188 & 77] & [135 & 43 & 168] & [74 & 39 & 150] & [61 & 90 & 63] \end{bmatrix}$$

Setelah semuanya ditranspose, langkah selanjutnya adalah membaca kembali nilai RGB dari setiap piksel yang telah dienkripsi dengan algoritma *Hill Cipher* dan letak posisinya telah ditranspose dengan algoritma *Arnold Cat Map* untuk diubah ke dalam bentuk citra digital. Maka dapat dilihat bahwa citra digital telah berubah dari citra digital aslinya.

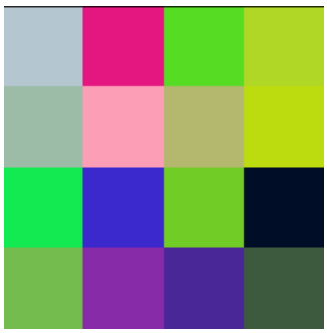


Gambar 4.2 Hasil dari Enkripsi Citra Digital Menggunakan Algoritma *Hill Cipher* dan *Arnold Cat Map*

4.1.2 Proses Dekripsi Citra Digital dengan Algoritma *Hill Cipher* dan *Arnold Cat Map*

Berikut ini contoh penerapan dekripsi dengan algoritma *Hill Cipher* dan *Arnold Cat Map* pada citra digital berukuran 4 × 4 piksel. Penerapan dilakukan pada *cipher-image* (HC-ACM) yang merupakan hasil enkripsi dari contoh penerapan sebelumnya menggunakan algoritma Hill Cipher dan Arnold Cat Map.

1. Diketahui kunci yang digunakan pada enkripsi algoritma Arnold Cat Map sebelumnya adalah $a = 3$. $b = 4$ dan $d = 1$. Dengan *cipher-image* diambil dari *cipher-image* (HC-ACM) berukuran 4 × 4 sebagai berikut.



Gambar 4.3 *Cipher-image* RGB Ukuran 4 X 4

2. Selanjutnya *cipher-image* (citra sandi) dimisalkan ($\boldsymbol{C^T}$) berukuran 4 × 4 akan dibaca sebagai matriks 4 × 4. Berikut entri dari matriks *cipher-image* (citra sandi).

$$\boldsymbol{C^T} = \begin{bmatrix} [180 & 198 & 208] & [228 & 23 & 129] & [87 & 220 & 36] & [177 & 215 & 38] \\ [157 & 188 & 167] & [252 & 159 & 182] & [180 & 183 & 110] & [188 & 220 & 16] \\ [19 & 233 & 80] & [60 & 41 & 206] & [114 & 204 & 38] & [0 & 13 & 38] \\ [116 & 188 & 77] & [135 & 43 & 168] & [74 & 39 & 150] & [61 & 90 & 63] \end{bmatrix}$$

3. Memasukkan kunci $a = 3$ dan $b = 4$ serta $N = 4$ ke dalam persamaan dekripsi *Arnold Cat Map*.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} (mod\ N)$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} (mod\ 4)$$

$$= \frac{1}{1 \cdot 13 - 4 \cdot 3} \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} (mod\ 4)$$

4. Berikut proses transformasi titik matriks ($\boldsymbol{C^T}$) pada matriks transpose ($\boldsymbol{C}$).

Jika $\boldsymbol{c^T_{x.y}} \in \boldsymbol{C^T}$ dan $\boldsymbol{c_{x.y}} \in \boldsymbol{C}$ dengan titik $x = 0.1.2.3$ dan $y = 0.1.2.3$

untuk baris $x' = 0$ dan kolom $y' = 0$, dengan entri

$\boldsymbol{c^T_{0.0}} = [180 \quad 198 \quad 208]$

$\boldsymbol{c^T_{0.0}} = [180 \quad 198 \quad 208] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} (mod\ 4)$

$= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c_{0.0}}$

untuk baris $x' = 0$ dan kolom $y' = 1$, dengan entri

$\boldsymbol{c^T_{0.1}} = [228 \quad 23 \quad 129]$

$\boldsymbol{c^T_{0.1}} = [228 \quad 23 \quad 129] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} (mod\ 4)$

$= \begin{bmatrix} 1 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{1.1}}$

untuk baris $x' = 0$ dan kolom $y' = 2$, dengan entri

$\boldsymbol{c^T_{0.2}} = [87 \quad 220 \quad 36]$

$\boldsymbol{c_{0.2}^T} = [87 \quad 220 \quad 36] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} (mod\ 4)$

$= \begin{bmatrix} 2 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{2.2}}$

untuk baris $x' = 0$ dan kolom $y' = 3$, dengan entri

$\boldsymbol{c_{0.3}^T} = [177 \quad 215 \quad 38]$

$\boldsymbol{c_{0.3}^T} = [177 \quad 215 \quad 38] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 3 \end{bmatrix} (mod\ 4)$

$= \begin{bmatrix} 3 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{3.3}}$

untuk baris $x' = 1$ dan kolom $y' = 0$, dengan entri

$\boldsymbol{c_{1.0}^T} = [157 \quad 188 \quad 167]$

$\boldsymbol{c_{1.0}^T} = [157 \quad 188 \quad 167] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} (mod\ 4)$

$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c_{1.0}}$

untuk baris $x' = 1$ dan kolom $y' = 1$, dengan entri

$\boldsymbol{c_{1.1}^T} = [252 \quad 159 \quad 182]$

$\boldsymbol{c_{1.1}^T} = [252 \quad 159 \quad 182] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} (mod\ 4)$

$= \begin{bmatrix} 2 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{2.1}}$

untuk baris $x' = 1$ dan kolom $y' = 2$, dengan entri

$\boldsymbol{c_{1.2}^T} = [180 \quad 183 \quad 110]$

$\boldsymbol{c_{1.2}^T} = [180 \quad 183 \quad 110] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} (mod\ 4)$

$= \begin{bmatrix} 3 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{3.2}}$

untuk baris $x' = 1$ dan kolom $y' = 3$, dengan entri

$\boldsymbol{c_{1.3}^T} = [188 \quad 220 \quad 16]$

$$\boldsymbol{c_{1.3}^T} = [188 \quad 220 \quad 16] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 0 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{0.3}}$$

untuk baris $x' = 2$ dan kolom $y' = 0$, dengan entri

$$\boldsymbol{c_{2.0}^T} = [19 \quad 233 \quad 80]$$

$$\boldsymbol{c_{2.0}^T} = [19 \quad 233 \quad 80] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 2 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c_{2.0}}$$

untuk baris $x' = 2$ dan kolom $y' = 1$, dengan entri

$$\boldsymbol{c_{2.1}^T} = [60 \quad 41 \quad 206]$$

$$\boldsymbol{c_{2.1}^T} = [60 \quad 41 \quad 206] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 3 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{3.1}}$$

untuk baris $x' = 2$ dan kolom $y' = 2$, dengan entri

$$\boldsymbol{c_{2.2}^T} = [114 \quad 204 \quad 38]$$

$$\boldsymbol{c_{2.2}^T} = [114 \quad 204 \quad 38] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 0 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{0.2}}$$

untuk baris $x' = 2$ dan kolom $y' = 3$, dengan entri

$$\boldsymbol{c_{2.3}^T} = [0 \quad 13 \quad 38]$$

$$\boldsymbol{c_{2.3}^T} = [0 \quad 13 \quad 38] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 1 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{1.3}}$$

untuk baris $x' = 3$ dan kolom $y' = 0$, dengan entri

$$\boldsymbol{c_{3.0}^T} = [116 \quad 188 \quad 77]$$

$$\boldsymbol{c_{3.0}^{T}} = [116 \quad 188 \quad 77] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 3 \\ 0 \end{bmatrix} \rightarrow \boldsymbol{c_{3.0}}$$

untuk baris $x' = 3$ dan kolom $y' = 1$, dengan entri

$$\boldsymbol{c_{3.1}^{T}} = [135 \quad 43 \quad 168]$$

$$\boldsymbol{c_{3.1}^{T}} = [135 \quad 43 \quad 168] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \boldsymbol{c_{0.1}}$$

untuk baris $x' = 3$ dan kolom $y' = 2$, dengan entri

$$\boldsymbol{c_{3.2}^{T}} = [74 \quad 39 \quad 150]$$

$$\boldsymbol{c_{3.2}^{T}} = [74 \quad 39 \quad 150] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 1 \\ 2 \end{bmatrix} \rightarrow \boldsymbol{c_{1.2}}$$

untuk baris $x' = 3$ dan kolom $y' = 3$, dengan entri

$$\boldsymbol{c_{3.3}} = [61 \quad 90 \quad 63]$$

$$\boldsymbol{c_{3.3}^{T}} = [61 \quad 90 \quad 63] \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix} (mod\ 4)$$

$$= \begin{bmatrix} 2 \\ 3 \end{bmatrix} \rightarrow \boldsymbol{c_{2.3}}$$

5. Karena iterasi d = 1 maka proses transformasi hanya dilakukan satu kali, Sehingga hasil transformasi menghasilkan matriks $\boldsymbol{C}$ dengan entri sebagai berikut.

$$\boldsymbol{C} = \begin{bmatrix} [180 \quad 198 \quad 208] & [252 \quad 159 \quad 182] & [114 \quad 204 \quad 38] & [61 \quad 90 \quad 63] \\ [157 \quad 188 \quad 167] & [60 \quad 41 \quad 206] & [74 \quad 39 \quad 150] & [177 \quad 215 \quad 38] \\ [19 \quad 233 \quad 80] & [135 \quad 43 \quad 168] & [87 \quad 220 \quad 36] & [188 \quad 220 \quad 16] \\ [116 \quad 188 \quad 77] & [228 \quad 23 \quad 129] & [180 \quad 183 \quad 110] & [0 \quad 13 \quad 38] \end{bmatrix}$$

6. Kunci $\boldsymbol{K^{-1}}$ berupa matriks yang dibentuk dengan formula matriks $\boldsymbol{K^{-1}} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix}^{-1}$ untuk melakukan dekripsi, kunci yang digunakan harus sama dengan kunci saat melakukan enkripsi yakni $a = 3$ dan $b = 4$. Sehingga diperoleh matriks $\boldsymbol{K^{-1}}$ sebagai berikut.

$$\boldsymbol{K^{-1}} = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}^{-1}$$

$$\boldsymbol{K^{-1}} = \frac{1}{1 \cdot 13 - 4 \cdot 3} \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix}$$

$$\boldsymbol{K^{-1}} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix}$$

7. Kemudian diambil masing-masing dua entri dalam matriks *cipher-image* (***C***) yang didefinisikan dengan $\begin{bmatrix} c_{i.j} \\ c_{i.j+1} \end{bmatrix}$ ($i =$ indeks baris matriks *cipher-image* (***C***) dan $j =$ indeks kolom matriks *cipher-image* (***C***)) dan dibentuk dalam satu matriks dengan ukuran 2×3. Setelah itu, dilakukan operasi perkalian matriks dengan kunci matriks $\boldsymbol{K^{-1}}$ yang mana hasil dari perkalian matriks tersebut dimodulokan dengan 256 sehingga dihasilkan dua entri yang didekripsi $\begin{bmatrix} \boldsymbol{p_{i.j}} \\ \boldsymbol{p_{i.j+1}} \end{bmatrix}$.

8. Berikut proses perkalian masing-masing dua entri dalam matriks *cipher-image* (***C***) dengan kunci matriks $\boldsymbol{K^{-1}}$.

$$\begin{bmatrix} \boldsymbol{c_{0.0}} \\ \boldsymbol{c_{0.1}} \end{bmatrix} = \begin{bmatrix} 180 & 198 & 208 \\ 252 & 159 & 182 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{0.0}} \\ \boldsymbol{p_{0.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{0.0}} \\ \boldsymbol{p_{0.1}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 180 & 198 & 208 \\ 252 & 159 & 182 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 48 & 49 & 110 \\ 44 & 135 & 118 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{0.2}} \\ \boldsymbol{c_{0.3}} \end{bmatrix} = \begin{bmatrix} 114 & 204 & 38 \\ 61 & 90 & 63 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{0.2}} \\ \boldsymbol{p_{0.3}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{0.2}} \\ \boldsymbol{p_{0.3}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 19 & 78 & 49 \\ 117 & 42 & 167 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 19 & 78 & 49 \\ 117 & 42 & 167 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{1.0}} \\ \boldsymbol{c_{1.1}} \end{bmatrix} = \begin{bmatrix} 157 & 188 & 167 \\ 60 & 41 & 206 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{1.0}} \\ \boldsymbol{p_{1.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{1.0}} \\ \boldsymbol{p_{1.1}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 157 & 188 & 167 \\ 60 & 41 & 206 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 69 & 17 & 17 \\ 200 & 57 & 50 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{1.2}} \\ \boldsymbol{c_{1.3}} \end{bmatrix} = \begin{bmatrix} 74 & 39 & 150 \\ 177 & 215 & 38 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{1.2}} \\ \boldsymbol{p_{1.3}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{1.2}} \\ \boldsymbol{p_{1.3}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 74 & 39 & 150 \\ 177 & 215 & 38 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 175 & 118 & 44 \\ 137 & 59 & 206 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{2.0}} \\ \boldsymbol{c_{2.1}} \end{bmatrix} = \begin{bmatrix} 98 & 84 & 24 \\ 59 & 135 & 104 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{2.0}} \\ \boldsymbol{p_{2.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{2.0}} \\ \boldsymbol{p_{2.1}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 98 & 84 & 24 \\ 59 & 135 & 104 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 19 & 233 & 80 \\ 135 & 43 & 168 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{2.2}} \\ \boldsymbol{c_{2.3}} \end{bmatrix} = \begin{bmatrix} 87 & 220 & 36 \\ 188 & 220 & 16 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{2.2}} \\ \boldsymbol{p_{2.3}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{2.2}} \\ \boldsymbol{p_{2.3}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 87 & 220 & 36 \\ 188 & 220 & 16 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 55 & 152 & 164 \\ 96 & 108 & 128 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{3.0}} \\ \boldsymbol{c_{3.1}} \end{bmatrix} = \begin{bmatrix} 116 & 188 & 77 \\ 228 & 23 & 129 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{3.0}} \\ \boldsymbol{p_{3.1}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{3.0}} \\ \boldsymbol{p_{3.1}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 56 & 71 & 102 \\ 20 & 39 & 77 \end{bmatrix} (mod\ 256)$$

$$= \begin{bmatrix} 56 & 71 & 102 \\ 20 & 39 & 77 \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{c_{3.2}} \\ \boldsymbol{c_{3.3}} \end{bmatrix} = \begin{bmatrix} 180 & 183 & 110 \\ 0 & 13 & 38 \end{bmatrix} \rightarrow \begin{bmatrix} \boldsymbol{p_{3.2}} \\ \boldsymbol{p_{3.3}} \end{bmatrix}$$

$$\begin{bmatrix} \boldsymbol{p_{3.2}} \\ \boldsymbol{p_{3.3}} \end{bmatrix} = \begin{bmatrix} 13 & -3 \\ -4 & 1 \end{bmatrix} \begin{bmatrix} 180 & 183 & 110 \\ 0 & 13 & 38 \end{bmatrix} (mod\ 256)$$

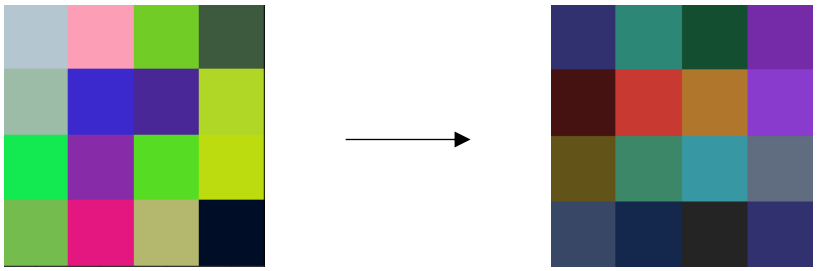
$$= \begin{bmatrix} 36 & 36 & 36 \\ 48 & 49 & 110 \end{bmatrix}$$

9. Setelah semua entri dikalikan dengan kunci matriks K^{-1}, hasil dari setiap dua entri yang didekripsi $\begin{bmatrix} \boldsymbol{p_{i.j}} \\ \boldsymbol{p_{i.j+1}} \end{bmatrix}$ dimasukkan ke dalam matriks *plain-image* (***P***) maka diperoleh.

P

$$= \begin{bmatrix} [48 & 49 & 110] & [44 & 135 & 118] & [19 & 78 & 49] & [117 & 42 & 167] \\ [69 & 17 & 17] & [200 & 57 & 50] & [175 & 118 & 44] & [137 & 59 & 206] \\ [98 & 84 & 24] & [59 & 135 & 104] & [55 & 152 & 164] & [96 & 108 & 128] \\ [56 & 71 & 102] & [20 & 39 & 77] & [36 & 36 & 36] & [48 & 49 & 110] \end{bmatrix}$$

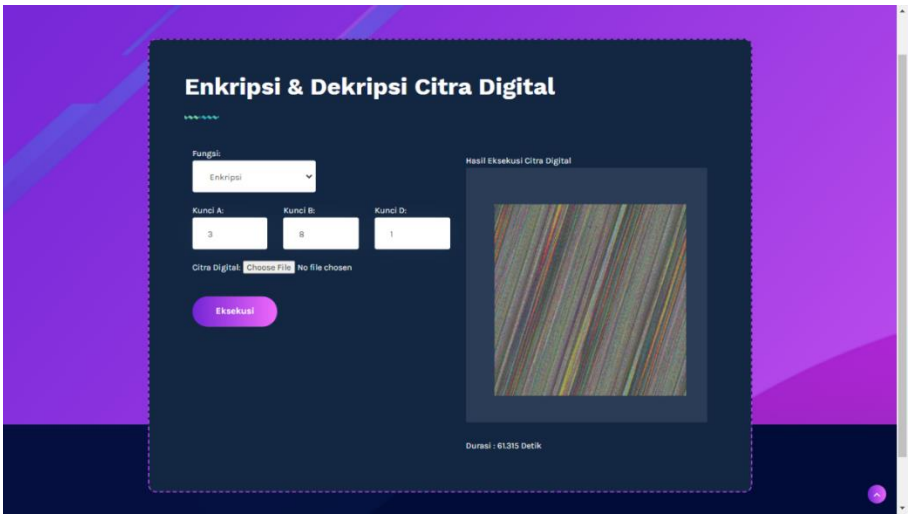
Matriks ***P*** inilah yang merupakan citra digital asli yang telah didekripsi dengan algoritma *Hill Cipher*. Maka dapat dipertunjukkan bahwa citra digital yang dienkripsi sebelumnya telah kembali ke dalam bentuk citra digital aslinya.



Gambar 4.4 Hasil dari Dekripsi Citra Digital Menggunakan Algoritma *Hill Cipher* dan *Arnold Cat Map*

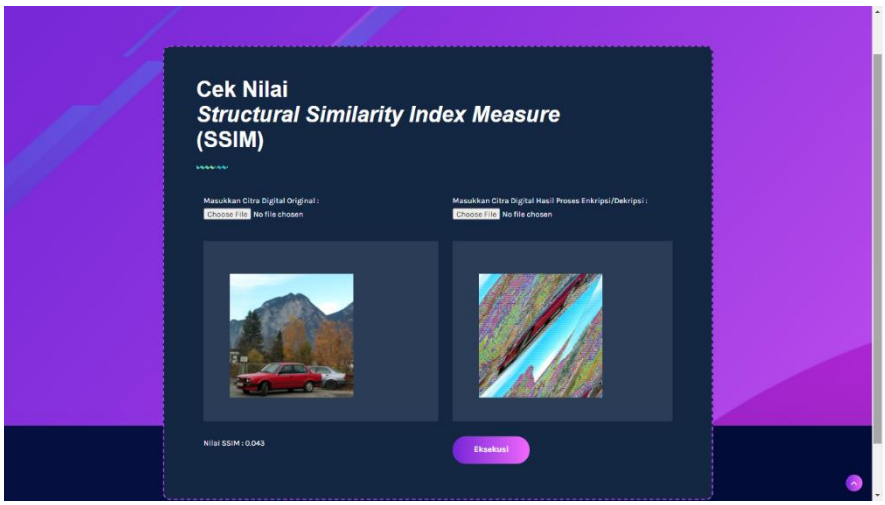
4.2 Pembahasan Hasil Enkripsi dan Dekripsi Citra Digital

Dalam bagian ini, sebelumnya telah dilakukan pengujian enkripsi dan dekripsi dengan menggunakan program *python* berbasis *website.* Pengujian dilakukan dengan memasukkan citra digital dan kunci ke halaman *website* seperti Gambar 4.5 untuk memperoleh hasil citra digital yang telah diproses dan waktu yang dibutuhkan untuk menjalankan proses tersebut.



Gambar 4.5 Tampilan Antarmuka Halaman *Website* Enkripsi dan Deksripsi Citra Digital

Kemudian, memasukkan citra digital asli dan citra digital yang telah diproses pada halaman *website* untuk dibandingkan seperti pada Gambar 4.6 sehingga diperoleh nilai *Structural Similarity Index Metrics* (SSIM).

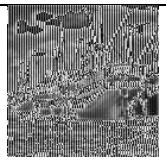
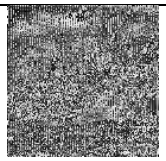
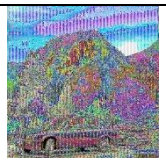
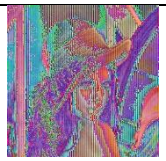
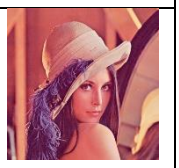
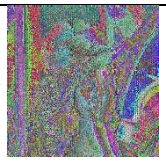
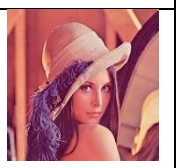


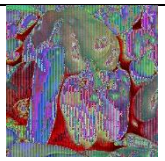
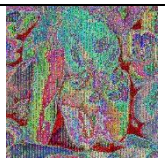
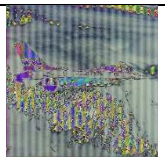
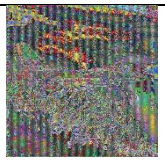
Gambar 4.6 Tampilan Antarmuka Halaman *Website* Cek Nilai *Structural Similarity Index Metrics* (SSIM)

4.2.1 Pembahasan Hasil Enkripsi dan Dekripsi Citra Digital dengan Algoritma *Hill Cipher*

Berikut pengujian menggunakan algoritma *Hill Cipher* terhadap 5 citra digital dengan ukuran yang berbeda dan menggunakan variasi 2 kunci yang berbeda. Hasil pengujian dapat dilihat pada Tabel 4.1.

Tabel 4.1 Hasil Pengujian Enkripsi dan Dekripsi dengan Algoritma *Hill Cipher*

No	Citra Digital Awal	Ukuran (Piksel)	Kunci	Waktu Proses Enkripsi (Detik)	Nilai SSIM Enkripsi	Hasil Enkripsi	Waktu Proses Dekripsi (Detik)	Nilai SSIM Dekripsi	Hasil Dekripsi
1.		128 X 128	a = 1 b = 1	0,225	0,038		0,215	1	
2.		128 X 128	a = 3 b = 8	0,175	0,011		0,142	1	
3.		256 X 256	a = 1 b = 1	0,476	0,175		0,864	1	
4.		256 X 256	a = 3 b = 8	0,522	0,052		0,812	1	
5.		512 X 512	a = 1 b = 1	2,526	0,127		2,414	1	
6.		512 X 512	a = 3 b = 8	2,163	0,039		2,418	1	

7.		800 X 800	a = 1 b = 1	5,435	0,217		5,902	1	
8.		800 X 800	a = 3 b = 8	5,366	0,043		6,162	1	
9.		1080 X 1080	a = 1 b = 1	10,26	0,082		10,381	1	
10.		1080 X 1080	a = 3 b = 8	10,499	0,027		10,638	1	

Dapat dilihat pada Tabel 4.1, pengujian dilakukan dengan total 10 kali percobaan dengan ukuran citra digital dan kunci yang berbeda. Untuk proses enkripsi dengan ukuran citra yang kecil membutuhkan waktu enkripsi yang relatif cepat. Sedangkan untuk proses enkripsi dengan ukuran citra yang besar membutuhkan waktu yang lebih lama. Kasus yang sama terjadi juga pada proses dekripsi citra digital.

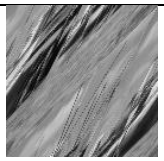
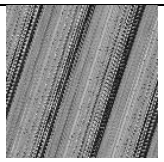
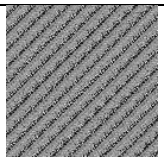
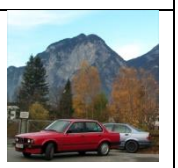
Selanjutnya, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses enkripsi menggunakan citra digital yang sama tetapi bilangan a dan b yang digunakan sebagai kunci lebih besar maka dapat menghasilkan nilai *Structural Similarity Index Metrics* (SSIM) yang lebih kecil. Rata-rata nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan pada pengujian ini adalah 0,081. Hal tersebut menunjukkan bahwa citra digital yang dihasilkan dari proses enkripsi tidak identik dengan citra digital awal. Kemudian, untuk nilai *Structural Similarity Index Metrics*

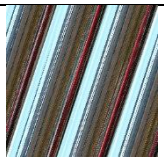
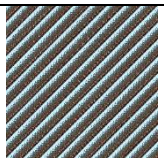
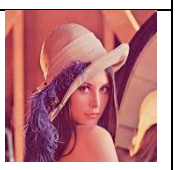
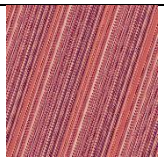
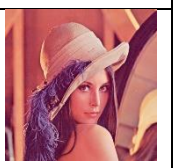
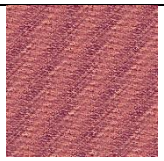
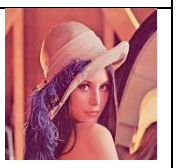
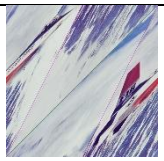
(SSIM) yang dihasilkan dari proses dekripsi menggunakan citra digital hasil enkripsi menghasilkan nilai 1 untuk semua pengujian. Hal tersebut menunjukkan bahwa citra digital yang dihasilkan identik atau sama dengan citra digital awal.

4.2.2 Pembahasan Hasil Enkripsi dan Dekripsi Citra Digital dengan Algoritma *Arnold Cat Map*

Berikut pengujian menggunakan algoritma *Arnold Cat Map* terhadap 5 citra digital dengan ukuran yang berbeda dan menggunakan variasi 3 kunci yang berbeda. Hasil pengujian dapat dilihat pada Tabel 4.2.

Tabel 4.2 Hasil Pengujian Enkripsi dan Dekripsi dengan Algoritma *Arnold Cat Map*

No	Citra Digital Awal	Ukuran (Piksel)	Kunci	Waktu Proses Enkripsi (Detik)	Nilai SSIM Enkripsi	Hasil Enkripsi	Waktu Proses Dekripsi (Detik)	Nilai SSIM Dekripsi	Hasil Dekripsi
1.		128 X 128	a = 1 b = 1 d = 1	0,267	0,075		0,296	1	
2.		128 X 128	a = 3 b = 8 d = 1	0,289	0,053		0,268	1	
3.		128 X 128	a = 3 b = 8 d = 99	25	0,03		25,276	1	
4.		256 X 256	a = 1 b = 1 d = 1	0,904	0,155		1,189	1	

5.		256 X 256	a = 3 b = 8 d = 1	0,907	0,063		0,887	1	
6.		256 X 256	a = 3 b = 8 d = 99	107,135	0,024		106	1	
7.		512 X 512	a = 1 b = 1 d = 1	4,288	0,213		4,357	1	
8.		512 X 512	a = 3 b = 8 d = 1	4,463	0,037		4,223	1	
9.		512 X 512	a = 3 b = 8 d = 99	483,991	0,021		476,263	1	
10.		800 X 800	a = 1 b = 1 d = 1	10,526	0,322		11,099	1	
11.		800 X 800	a = 3 b = 8 d = 1	11,38	0,05		10,775	1	
12.		800 X 800	a = 3 b = 8 d = 99	1073,351	0,017		1239,992	1	
13.		1080 X 1080	a = 1 b = 1 d = 1	19,818	0,433		19,464	1	
14.		1080 X 1080	a = 3 b = 8 d = 1	20,659	0,254		20,742	1	

15.		1080 X 1080	a = 3 b = 8 d = 99	2159,882	0,028		2231,322	1	

Dapat dilihat pada Tabel 4.2, pengujian dilakukan dengan total 15 kali percobaan dengan ukuran citra digital dan kunci yang berbeda. Untuk proses enkripsi dengan ukuran citra digital dan nilai kunci d yang kecil membutuhkan waktu enkripsi yang relatif cepat. Sedangkan untuk proses enkripsi dengan ukuran citra digital dan nilai kunci d yang besar membutuhkan waktu yang lama. Kasus yang sama terjadi juga pada proses dekripsi citra digital.

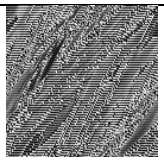
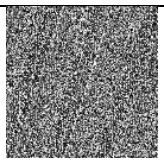
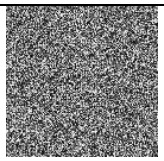
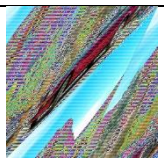
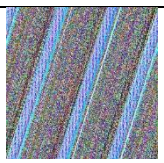
Selanjutnya, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses enkripsi menggunakan citra digital yang sama tetapi nilai kunci a dan b yang digunakan sebagai kunci yang lebih besar maka dapat menghasilkan nilai *Structural Similarity Index Metrics* (SSIM) yang lebih kecil. Dalam pengujian ini juga terdapat kunci d yang mana walaupun menggunakan citra digital dan nilai kunci a dan b yang sama tetapi nilai kunci d yang digunakan lebih besar dapat menghasilkan nilai *Structural Similarity Index Metrics* (SSIM) yang lebih kecil. Rata-rata nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan pada pengujian ini adalah 0,118. Hal tersebut menunjukkan bahwa citra digital yang dihasilkan dari proses enkripsi tidak identik dengan citra digital awal. Kemudian, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses dekripsi menggunakan citra digital hasil enkripsi menghasilkan nilai 1 untuk semua pengujian. Hal tersebut menunjukkan

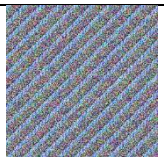
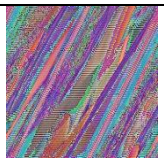
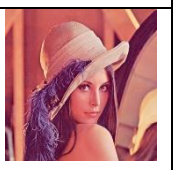
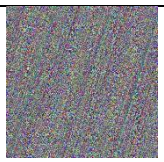
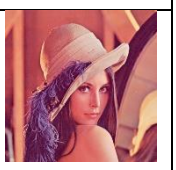
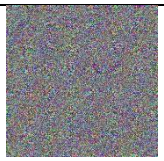
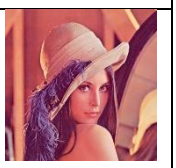
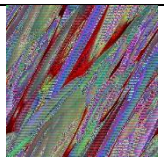
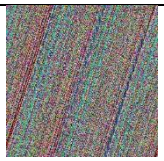
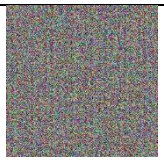
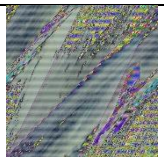
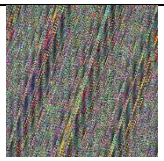
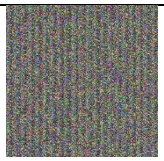
bahwa citra digital yang dihasilkan identik atau sama dengan citra digital awal.

4.2.3 Pembahasan Hasil Enkripsi dan Dekripsi Citra Digital dengan Algoritma *Hill Cipher* dan *Arnold Cat Map*

Berikut pengujian menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* terhadap 5 citra digital dengan ukuran yang berbeda dan menggunakan variasi 3 kunci yang berbeda. Hasil pengujian dapat dilihat pada Tabel 4.3.

Tabel 4.3 Hasil Pengujian Enkripsi dan Dekripsi dengan Algoritma *Hill Cipher* dan *Arnold Cat Map*

No	Citra Digital Awal	Ukuran (Piksel)	Kunci	Waktu Proses Enkripsi (Detik)	Nilai SSIM Enkripsi	Hasil Enkripsi	Waktu Proses Dekripsi (Detik)	Nilai SSIM Dekripsi	Hasil Dekripsi
1.		128 X 128	a = 1 b = 1 d = 1	0,341	0,013		0,424	1	
2.		128 X 128	a = 3 b = 8 d = 1	0,625	0,011		0,385	1	
3.		128 X 128	a = 3 b = 8 d = 99	27,297	0,012		27,111	1	
4.		256 X 256	a = 1 b = 1 d = 1	1,875	0,043		2,162	1	
5.		256 X 256	a = 3 b = 8 d = 1	2,205	0,017		1,717	1	

6.		256 X 256	a = 3 b = 8 d = 99	115,15	0,016		113,195	1	
7.		512 X 512	a = 1 b = 1 d = 1	7,125	0,039		7,054	1	
8.		512 X 512	a = 3 b = 8 d = 1	6,821	0,022		7,509	1	
9.		512 X 512	a = 3 b = 8 d = 99	485,395	0,021		461,485	1	
10.		800 X 800	a = 1 b = 1 d = 1	17,881	0,086		18,27	1	
11.		800 X 800	a = 3 b = 8 d = 1	16,621	0,02		17,336	1	
12.		800 X 800	a = 3 b = 8 d = 99	1033,259	0,019		1021,483	1	
13.		1080 X 1080	a = 1 b = 1 d = 1	29,705	0,052		32,693	1	
14.		1080 X 1080	a = 3 b = 8 d = 1	33,526	0,02		32,628	1	
15.		1080 X 1080	a = 3 b = 8 d = 99	3392,19	0,017		1907,56	1	

Dapat dilihat pada Tabel 4.3, pengujian dilakukan dengan total 15 kali percobaan dengan ukuran citra digital dan kunci yang berbeda. Untuk proses enkripsi dengan ukuran citra digital dan nilai kunci d yang kecil membutuhkan waktu enkripsi yang relatif cepat. Sedangkan untuk proses enkripsi dengan ukuran citra digital dan nilai kunci d yang besar membutuhkan waktu yang lama. Kasus yang sama terjadi juga pada proses dekripsi citra digital.

Selanjutnya, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses enkripsi menggunakan citra digital yang sama tetapi nilai kunci a dan b yang digunakan sebagai kunci yang lebih besar maka dapat menghasilkan nilai *Structural Similarity Index Metrics* (SSIM) yang lebih kecil. Dalam pengujian ini juga terdapat kunci d yang mana walaupun menggunakan citra digital dan nilai kunci a dan b yang sama tetapi nilai kunci d yang digunakan lebih besar dapat menghasilkan nilai *Structural Similarity Index Metrics* (SSIM) yang lebih kecil. Rata-rata nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan pada pengujian ini adalah $0{,}027$. Hal tersebut menunjukkan bahwa citra digital yang dihasilkan dari proses enkripsi tidak identik dengan citra digital awal. Kemudian, untuk nilai *Structural Similarity Index Metrics* (SSIM) yang dihasilkan dari proses dekripsi menggunakan citra digital hasil enkripsi menghasilkan nilai 1 untuk semua pengujian. Hal tersebut menunjukkan bahwa citra digital yang dihasilkan identik atau sama dengan citra digital awal.

4.3 Kajian Keislaman

Penyandian pesan atau yang disebut proses enkripsi, bertujuan untuk melindungi pesan dari orang yang tidak mempunyai hak mengetahui isi pesan yang kemudian dilakukan proses pembacaan pesan kembali atau dekripsi oleh orang yang menerima pesan. Hal tersebut memiliki kesamaan dengan definisi amanah secara sempit yaitu menjaga barang titipan dan mengembalikannya dalam bentuk semula.

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan sebelumnya, maka dapat diambil kesimpulan sebagai berikut :

1. Proses enkripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* dimulai dengan proses perubahan nilai tingkat keabuan pada setiap piksel dari citra digital asli. Kemudian, dilanjutkan dengan proses transformasi posisi setiap piksel dari citra digital yang telah diproses sebelumnya. Sehingga diperoleh citra digital hasil enkripsi. Pada proses dekripsi menggunakan algoritma *Hill Cipher* dan *Arnold Cat Map* berkebalikan dengan proses enkripsi, pada proses ini citra digital yang akan didekripsi akan dilakukan transformasi posisi setiap piksel dari citra digital terlebih dahulu. Kemudian, dilanjutkan dengan perubahan nilai tingkat keabuan pada setiap piksel dari citra digital yang telah diproses sebelumnya. Sehingga diperoleh citra digital hasil dekripsi yang sama dengan citra digital asli.

2. Berdasarkan pembahasan terhadap hasil pengujian enkripsi dan dekripsi citra digital, maka dapat diambil kesimpulan bahwa waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dipengaruhi oleh ukuran citra digital dan besaran nilai kunci d yang dimasukkan dengan menggunakan algoritma *Arnold Cat Map*. Semakin besar ukuran citra digital dan nilai kunci d yang dimasukkan dengan menggunakan algoritma *Arnold Cat Map* maka membutuhkan waktu yang lebih lama untuk melakukan proses enkripsi dan dekripsi citra digital. Kemudian, hasil enkripsi citra digital yang diperoleh dari penerapan algoritma

Hill Cipher dan *Arnold Cat Map* berhasil menghasilkan suatu citra digital yang lebih acak dan hampir tidak dikenali lagi jika dibandingkan dengan penerapan yang hanya menggunakan algoritma *Hill Cipher* atau *Arnold Cat Map* saja. Hal tersebut dibuktikan dengan rata-rata nilai *Structural Similarity Index Metrics* (SSIM) yang diperoleh dalam proses pengujian dengan penerapan algoritma *Hill Cipher* dan *Arnold Cat Map* adalah 0,027 yang bernilai lebih kecil dari hasil yang diperoleh dengan algoritma *Hill Cipher* atau *Arnold Cat Map* saja yang masing-masing nilainya adalah 0,081 dan 0,118. Selanjutnya, untuk hasil dekripsi yang dihasilkan dari setiap pengujian diperolah nilai *Structural Similarity Index Metrics* (SSIM) sama dengan 1 yang mana hal tersebut membuktikan bahwa dekripsi yang dilakukan berhasil mengembalikan citra digital hasil enkripsi ke citra digital awal.

5.2 Saran

Dengan melihat hasil yang dicapai pada penelitian ini, terdapat saran untuk pengembangan penelitian selanjutnya yakni terkait kunci yang digunakan dalam proses enkripsi dan dekripsi tersebut agar dapat diberikan pengamanan khusus karena mengingat untuk menyampaikan suatu citra digital ke tujuan harus menyertakan kunci agar penerima citra digital dapat melakukan proses dekripsi terhadap citra digital yang telah diberikan sebelumnya.

DAFTAR PUSTAKA

Abdo, Azza A., Hanaa F. Morse dan Maissa A. El-Mageed. (2020). *An Efficient Color Image Encryption Scheme Based On Combination Of Hill Cipher And Cellular Neural Network*. Indian Journal o Computer Science and Engineering (IJCSE) Vol. 11 No. 2.

Ariyus, Doni. (2006). *Kriptografi Keamanan Data dan Komunikasi.* Yogyakarta: Graha Ilmu.

Binanto, Iwan. (2010). *Multimedia Digital Dasar Teori + Pengembangannya.* Yogyakarta: Andi Offset.

Cahyono, Hary. (2019). *Membangun Aplikasi Web Data Analysis Dengan Framework Django.* Jakarta : Google Play Book.

Clark, Alex dan kontributor. (2010). *Pillow (PIL Fork) Documentation.* https://pillow.readthedocs.io/en/stable/.

Django Software Foundation. (2019). *Django makes it easier to build better web apps more quickly and with less code.* https://www.djangoproject.com/.

Forouzan, Behrouz. (2006).*Cryptography and Network Security*. McGraw-Hill.

Gonzales, R. C. dan Richard E. Woods. (2002). *Digital Image Processing*. New Jersey : Prentice Hall.

Hariyanto, Eko dan Robbi Rahim. (2016). *Arnold's Cat Map Algorithm in Digital Image Encryption*. International Journal of Science and Research (IJSR) Volume 5 Issue 10.

Kementrian Agama RI (2011), *Al-Qur'an Dan Tafsirnya Edisi Yang Disempurnakan*, Jakarta: Widya Cahaya.

Kromodimoeljo, Sentot. 2010. *Teori dan Aplikasi Kriptografi*. Jakarta : SPK IT.

Maulidah, Cici Erisa. (2018). *Implementasi Metode Super Enkripsi (Vinegere Cipher – Arnold Cat Map) Pada Matriks Citra*. Skripsi. Universitas Islam Negeri Maulana Malik Ibrahim Malang. Malang.

Munir, Rinaldi. (2006). *Diktat Kuliah IF5054 Kriptografi*.Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika.

Munir, Rinaldi. (2012). *Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold*

Cat Map dan Logistic Map. ISSN : 2087-2658.

Muslimin, Irkham dan Ir. Sumarno, MM. (2015). *Kriptografi Pada File Gambar Menggunakan Metode Hill Cipher dan Transposisi*. Universitas Muhammadiyah Sidoarjo. Sidoarjo

Nafi'iyah, Nur. (2015). *Algoritma Kohonen dalam Mengubah Citra Graylevel Menjadi Citra Biner*. Jurnal Ilmiah Teknologi dan Informasia ASIA (JITIKA) Vol.9, No.2.

Purba, R. Arwin Halim dan Indra Syahputra. (2014). *Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm*. ISSN : 1412-0100.

Setiawan, Engelbert Eric. (2016). *Analisis Performa Metode Hill Cipher Sebagai Algoritma Penyandian Citra*. Skripsi. Universitas Sanata Dharma. Yogyakarta.

Sharma, M. (2010). *Image Encryption Techniques Using Chaotic Schemes: A Review. International Journal of Engineering Science and Technology 2(6),* pp. *2359-2363.*

Sutoyo, T., Mulyanto, E., Suhartono, V., Nurhayati, Oky D., dan Wijanarto. (2009). *Teori Pengolahan Citra Digital*. Yogyakarta: Andi Offset.

Wulandari, Meirista. (2017). *Index Quality Assesment Citra Terinterpolasi (SSIM dan FSIM)*. JUTEI Volume.1 No.1.

Z. Wang, A. C. Bovik, H. R. Sheikh, dan E. P. Simoncelli (2004). *Image Quality Assessment: From Error Visibility to Structural Similarity* IEEE *Transactions on Image Processing*, vol. 13, pp. 600-612.

LAMPIRAN

1. Pembacaan Piksel Citra Digital pada *Website*

```
.............................................................
pil_img=Image.open(self.image)

if pil_img.mode == 'CMYK' or 'P' or 'RGBA' or 'HSV' or 'LAB'
or 'YCbCr':
    pil_img = pil_img.convert('RGB')

pil_img=np.array(pil_img)
if pil_img.shape[0]!=pil_img.shape[1]:
    jumBaris=round(pil_img.shape[0])
    jumKolom=round(pil_img.shape[1])

    size=0

    if jumBaris%2!=0 or jumKolom%2!=0:
        size=1

    if jumBaris>jumKolom:
        size+=jumKolom
        rasio=jumKolom/jumBaris
        kolom=int(rasio*size)
        baris=size
    else :
        size+=jumBaris
        rasio=jumBaris/jumKolom
        kolom=size
        baris=int(rasio*size)
    bg=cv2.resize(pil_img, (size, size))
    image_square=cv2.GaussianBlur(bg, (45, 45), 0)

    pil_img=cv2.resize(pil_img, (kolom, baris))
    jumBaris=pil_img.shape[0]
    jumKolom=pil_img.shape[1]
    kiri=jumBaris//4
    kanan=jumBaris-(jumBaris//4)
    image_square[0:jumBaris, 0:jumKolom, 0:3]=pil_img[:, :,
0:3]
    pil_img=image_square

if pil_img.shape[0]%2!=0:
    jumBaris=round(pil_img.shape[0])
    jumKolom=round(pil_img.shape[1])
    size=1+pil_img.shape[0]
    bg=cv2.resize(pil_img, (size, size))
    image_square_genap=cv2.GaussianBlur(bg, (45, 45), 0)
    image_square_genap[0:jumBaris, 0:jumKolom,
0:3]=pil_img[:, :, 0:3]
    pil_img=image_square_genap

img=get_secured_image(pil_img, self.action, self.kunci_a,
self.kunci_b, self.kunci_d)
```

2. Proses Enkripsi dan Dekripsi Citra Digital pada *Website*

```
.............................................................
import cv2
import numpy as np
from PIL import Image
from mpmath import log10

def get_secured_image(img, action, a, b, d):
#---------------Membaca Citra Digital dan Kunci--------------
    Mod = 256
    a=int(a)
    b=int(b)
    d=int(d)
    rows, cols, ch = img.shape
    q = np.zeros([rows, cols, ch])
    key = np.array([[1,a],[b,a*b+1]])
    keyinvers=np.linalg.inv(key)
    keyinvers = keyinvers.astype(int)
    i=0
    if action == 'ENKRIPSI':
        # Enkripsi Hill Cipher
        for x in range (0, rows):
            for y in range (0, cols, 2):
                m=img[x,y:y+2,:]
                n=(np.matmul(key,m % Mod)) % Mod
                q[x,y:y+2,:]=n
        img=q.astype(np.uint8)
        #Enkripsi Arnold Cat Map
        while i<d:
            rows, cols, ch = img.shape
            if (rows == cols):
                n = rows
                img2 = np.zeros([rows, cols, ch])
                for x in range(0, rows):
                    for y in range(0, cols):
                        k=[x,y]
                        l=np.matmul(key,k)%n
                        img2[x,y] = img[l[0],l[1]]
                img=img2
                i=i+1
        encrypted=img.astype(np.uint8)
        return encrypted
    elif action == 'DEKRIPSI':
        #Dekripsi Arnold Cat Map
        while i<d:
            rows, cols, ch = img.shape
            if (rows == cols):
                n = rows
                img2 = np.zeros([rows, cols, ch])
                for x in range(0, rows):
                    for y in range(0, cols):
                        k=[x,y]
                        l=np.matmul(keyinvers,k)%n
                        img2[x,y] = img[l[0],l[1]]
```

```
.....................................................................
            img=img2
            i=i+1
        img2=img.astype(np.uint8)
        #Dekripsi Hill Cipher
        rows, cols, ch = img.shape
        p = np.zeros([rows, cols, ch])
        for x in range (0, rows):
            for y in range (0, cols, 2):
                m=img[x,y:y+2,:]
                n=(np.matmul(keyinvers,m % Mod)) % Mod
                p[x,y:y+2,:]=n
        decrypted=p.astype(np.uint8)
        return decrypted
```

RIWAYAT HIDUP

Muhammad Luqman Hakim lahir di Kota Palangka Raya pada 3 Agustus 1999. Memiliki nama panggilan Luqman. Tempat tinggal di Perumahan Bumi Palangka 2, Jln. Pinguin V No.384, Kel. Bukit Tunggal, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah. Merupakan anak pertama dari Bapak Sutomo dan Ibu Dahniar Astuti.

Pendidikan yang pernah ditempuh yaitu TK. Kemudian melanjutkan sekolahnya di MIN Langkai Palangka Raya dan lulus pada tahun 2011. Menempuh pendidikan SMP di Sekolah Menengah Pertama Negeri 1 Kota Palangka Raya lulus pada tahun 2014. Melanjutkan pendidikan SMA di Sekolah Menengah Atas Negeri 2 Kota Palangka Raya lulus pada tahun 2017.

Tahun 2017 melanjutkan studi ke jenjang pendidikan strata 1 di Universitas Islam Negeri Maulana Malik Ibrahim Malang mengambil jurusan Matematika Fakultas Sains dan Teknologi. Aktif mengikuti kegiatan organisasi serta komunitas yang ada di dalam dan di luar (intra atau ekstra) kampus, seperti menjadi Pengurus HMJ Matematika UIN Malang (2017-2019), Anggota GenBI Malang (2018-2019), dan Pengurus GenBI Malang (2019-2020).

Kegiatan-kegiatan yang pernah diikuti yaitu GenBI Leadership Camp Jawa Timur tahun 2019, GenBI Leadership Camp Nasional tahun 2019 dan 2020, Kuliah Kerja Mahasiswa (KKM) UIN Malang mengabdi tahun 2020, Praktek Kerja Lapangan (PKL) di Dinas Komunikasi dan Informatika Kota Malang tahun 2020, dan Mahasiswa Cloud Computing di Bangkit Academy yang diselenggarakan oleh Google, Tokopedia, Gojek, & Traveloka.

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jalan Gajayana No 50 Dinoyo Malang Telp/Fax. (0341)588933

BUKTI KONSULTASI SKRIPSI

Nama : Muhammad Luqman Hakim
NIM : 17610080
Fakultas/ Program Studi : Sains dan Teknologi/ Matematika
Judul Skripsi : Implementasi Algoritma *Hill Cipher* dan *Arnold Cat Map* dalam Pemanfaatan Enkripsi dan Dekripsi Citra Digital Berbasis *Website*
Pembimbing I : Muhammad Khudzaifah, M.Si
Pembimbing II : Evawati Alisah, M.Pd

No	Tanggal	Hal	Tanda Tagan
1	9 Maret 2021	Konsultasi Bab I, II, III	1.
2	11 Maret 2021	Konsultasi Bab I dan Kajian Keislaman	2.
3	22 Maret 2021	Konsultasi Bab I, II, III	3.
4	23 Maret 2021	Konsultasi Bab I dan Kajian Keislaman	4.
5	15 April 2021	Simulasi Seminar Proposal	5.
6	15 April 2021	Simulasi Seminar Proposal	6.
7	27 April 2021	Konsultasi Bab I, II, III	7.
8	1 Mei 2021	Konsultasi Kajian Keislaman	8.
9	6 Mei 2021	Konsultasi Bab IV (Kajian Keislaman)	9.
10	7 Mei 2021	Konsultasi Bab IV	10.
11	15 Juni 2021	Konsultasi Keseluruhan	11.
12	16 Juni 2021	ACC Keseluruhan	12.

Malang, 16 Juni 2021
Mengetahui,
Ketua Program Studi

Dr. Usman Pagalay, M.Si
NIP. 19650414 200312 1 001