IMPLEMENTASI ALGORITMA SUPER ENKRIPSI *ARNOLD'S CAT MAP* DAN *AFFINE CIPHER* DENGAN PEMBANGKITAN KUNCI MENGGUNAKAN PERSAMAAN *LOGISTIC MAP*

SKRIPSI

OLEH:
Egi Novaldi
NIM. 18610039

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI *ARNOLD'S CAT MAP* DAN *AFFINE CIPHER* DENGAN PEMBANGKITAN KUNCI MENGGUNAKAN PERSAMAAN *LOGISTIC MAP*

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
Egi Novaldi
NIM. 18610039

PROGRAM STUDI MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM
MALANG
2023

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI *ARNOLD'S CAT MAP* DAN *AFFINE CIPHER* DENGAN PEMBANGKITAN KUNCI MENGGUNAKAN PERSAMAAN *LOGISTIC MAP*

SKRIPSI

Oleh
Egi Novaldi
NIM. 18610039

Telah Disetujui Untuk Diuji

Malang, 22 Desember 2023

Dosen Pembimbing I	Dosen Pembimbing II
Muhammad Khudzaifah, M.Si	Erna Herawati, M.Pd.
NIP. 19900511 202321 1 029	NIP. 19760723 202321 2 006

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, S.Pd., M.Sc
NIP. 19741129 200012 2 005

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI *ARNOLD'S CAT MAP* DAN *AFFINE CIPHER* DENGAN PEMBANGKITAN KUNCI MENGGUNAKAN PERSAMAAN *LOGISTIC MAP*

SKRIPSI

Oleh
Egi Novaldi
NIM. 18610039

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

Tanggal 27 Desember 2023

Ketua Penguji	: Prof. Dr. H. Turmudi, M.Si, Ph.D	.....
Anggota Penguji I	: Intan Nisfulaila, M.Si	.....
Anggota Penguji II	: Muhammad Khudzaifah, M.Si	.....
Anggota Penguji III	: Erna Herawati, M.Pd	.....

Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, S.Pd., M.Sc
NIP. 19741129 200012 2 005

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan di bawah ini:

Nama	: Egi Novaldi
NIM	: 18610039
Program Studi	: Matematika
Fakultas	: Sains dan Teknologi
Judul Skripsi	: Implementasi Algoritma Super Enkripsi *Arnold's Cat Map* Dan *Affine Cipher* Serta Implementasi Persamaan *Logistic Map* Dalam Pembangkitan Kunci

Menyatakan dengan sebenarnya bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilan data, tulisan atau pikiran orang lain yang saya akui sebagai hasil tulisan dna pikiran saya sendiri, kecuali dengan mencantumkan 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, 27 Desember 2023

Yang membuat pernyataan,

Egi Novaldi

MOTTO DAN PERSEMBAHAN

"Mulailah segala sesuatu dengan bismillah, apapun hasil yang diperoleh setidaknya itu bukti kamu telah berjuang"

Skripsi ini penulis persembahkan untuk:

Kedua orang tua penulis, saudara penulis, seluruh keluarga penulis, dan sahabat yang senantiasa memberi dukungan dan semangat.

KATA PENGANTAR

Assalamualaikum Warohmatullah Wabarakatuh

Segala puji bagi Allah SWT. yang telah melimpahkan rahmat, taufik, dan hidayah-Nya, sehingga penulis mampu menyelesaikan skripsi dengan judul "Implementasi Algoritma Super Enkripsi *Arnold's Cat Map* Dan *Affine Cipher* Serta Pembangkitan Kunci Pada *Affine Cipher* Menggunakan *Logistic Map*". sebagai salah satu syarat untuk memperoleh gelar Sarjana Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Shalawat serta salam yang senantiasa kita curahkan kepada baginda Rasulullah SAW, semoga kita semua mendapatkan syafaatnya di *yaumul* akhir nanti, *Aamiin.*

Dalam proses penyusunan skripsi ini, penulis telah banyak mendapat bimbingan dan masukan serta semangat dari berbagai pihak. Untuk itu dengan kerendahan hati, penulis mengucapkan terima kasih kepada yang terhormat:

1. Prof. Dr. H. M. Zainuddin, M.A., selaku rektor Universitas Islam Negeri Maulana Malik Ibrahim.
2. Prof. Dr. Hj. Sri Harini, M.Si., selaku dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim.
3. Dr. Elly Susanti, S.Pd., M.Sc., selaku ketua Program Studi Matematika, Universitas Islam Negeri Maulana Malik Ibrahim.
4. Muhammad Khudzaifah, M.Si., selaku dosen pembimbing I yang telah memberikan arahan dan berbagi ilmu kepada penulis.
5. Erna Herawati, M.Pd., selaku dosen pembimbing II yang telah memberikan arahan, nasihat, dan berbagi banyak pengalaman kepada penulis.

6. Prof. Dr. H. Turmudi, M.Si., selaku penguji utama yang telah memberikan arahan dan saran yang membangun kepada penulis.
7. Intan Nisfulaila, M.Si., selaku dosen penguji yang telah banyak memberikan arahan dan saran yang membangun kepada penulis.
8. Fachrur Rozi, M.Si., selaku dosen wali yang senantiasa memberikan motivasi, semangat, serta arahan kepada penulis selama menyelesaikan studi.
9. Seluruh dosen Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim.
10. Kedua orang tua saya yaitu Bapak Efendi dan Ibu Almh. Erniwati serta seluruh keluarga yang senantiasa mendoakan dan memberi dukungan penuh kepada penulis selama menempuh studi.
11. Seluruh mahasiswa matematika angkatan 2018 Program Studi Matematika yang senantiasa memberikan support dan energi positif untuk membantu penulis menyelesaikan skripsi ini.

Penulis menyadari bahwa penulisan proposal skripsi ini masih terdapat banyak kekurangan. Oleh karena itu, penulis sangat berharap diberikan kritik dan saran yang dapat membangun sehingga dapat dijadikan bahan perbaikan bagi penulis terkait penelitian selanjutnya. Mohon maaf atas segala kelebihan dan kekurangan pada penulisan skripsi ini.

Wassalamu'alaikum Warahmatullahi Wabarakatuh

Malang, 27 Desember 2023

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

ABSTRAK

Novaldi, Egi. 2023. **Implementasi Algoritma Super Enkripsi Arnold's Cat Map Dan Affine Cipher Dengan Pembangkitan Kunci Menggunakan Persamaan Logistic Map.** Skripsi. Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing (1): Muhammad Khudzaifah, M.Si., Pembimbing (2): Erna Herawati, M.Pd.

Kata Kunci: Super Enkripsi, Citra Digital, Enkripsi, Dekripsi, Algoritma *Arnold's Cat Map*, Algoritma *Affine Cipher*, Pembangkit Kunci, Persamaan *Logistic Map.*

Kemudahan dalam berkomunikasi dan saling berbagi informasi tidak lepas munculnya kejahatan seperti pembajakan, pencurian data, dan penyebaran informasi yang tidak seharusnya. Ada berbagai jenis data penting yang dapat diamankan salah satunya yaitu data visual (citra digital). Kriptografi memiliki banyak algoritma dan metode penyandian pesan dan data. Pada penelitian ini dibahas mengenai metode super enkripsi dengan mengkolaborasikan algoritma *Arnold's Cat Map* dan *Affine Cipher*. Setiap algoritma penyandian memiliki kunci yang mempengaruhi kualitas proses enkripsi. Dalam penelitian ini pembangkitan kunci pada *Affine Cipher* dilakukan menggunakan persamaan *Logistic Map*. *Logistic Map* menghasilkan deret bilangan acak yang bersifat *chaos*. Tujuan penelitian ini adalah untuk mengetahui hasil dari enkripsi dan dekripsi terhadap data visual (citra digital) dengan algoritma super enkripsi dengan menggunakan algoritma *Arnold's Cat* dan *Affine Cipher* serta pembangkitan kunci dengan persamaan *Logistic Map* yang akan dimanfaatkan pada *Affine Cipher*. Hasil percobaan menunjukan citra hasil proses enkripsi memiliki tingkat similaritas yang rendah dari citra aslinya yang dapat dilihat dari nilai *Mean Square Error* (MSE) yang besar dengan rata-rata 105,3873 dan tingkat noise yang tinggi berdasarkan nilai *Peak Signal-to-Noise Ratio* (PSNR) yang rata-rata nilainya di bawah 30 db.

ABSTRACT

Novaldi, Egi. 2023. **Implementation of Super Encryption Algorithm Arnold's Cat Map and Affine Cipher with key Generator Using Logistic Map Equation.** Thesis. Mathematics Study Program, Faculty of Science dan Technology, Universitas Islam Negeri Maulana Malik Ibrahim Malang. Supervisor (1): Muhammad Khudzaifah, M.Si., Supervisor (2): Erna Herawati, M.Pd.

Keywords: Super Encryption, Digital Image, Encryption, Decryption, Arnold's Cat Map Algorithm, Affine Cipher Algorithm, Key Generator, Logistic Map Equation.

The ease of communicating and sharing information cannot be separated from the emergence of crimes such as hacking, data theft, and the spread of information that should not be. There are various types of important data that can be protected, one of which is visual data (digital images). Cryptography has many algorithms and methods of encrypting messages and data. This research discusses the super encryption method by collaborating Arnold's Cat Map and Affine Cipher algorithms. Each encryption algorithm has a key that influences the quality of the encryption process. In this paper, the key generator for Affine Cipher is generated using the Logistic Map equation. Logistic Map generates a chaotic sequence of random numbers. The goal of this research is to determine the results of encryption and decryption of visual data (digital images) with super encryption algorithms using Arnold's Cat and Affine Cipher algorithms and key generation with Logistic Map equations that will be used in Affine Cipher. The experimental results show that the image resulting from the encryption process has a low level of similarity to the original image which can be seen from the value of Mean Square Error (MSE) which is large with an average of 105.3873 and a high level of noise based on the value of Peak Signal-to-Noise Ratio (PSNR) whose average value is below 30 db.

مستخلص البحث

نوفالدي،إيجي.٢٠٢٣. **تنفيذ طريقة التشفير الفائق *Arnold's Cat Map* و تشفير أفيني مع توليدالمفتاح يستخدم معادلة الخريطة اللوجستية**. البحث الجامعي. قسم الرياضيات ، كلية العلوم والتكنولوجيا، جامعة مولانا مالك إبراهيم الإسلامية الحكومية مالانج . المشرف الأول: محمد خذيفة ، الماجستير، المشرف الثاني : إيرنا هيراواتي ، الماجستيرة.

الكلمات الرئيسية : تشفير فائق، صورة رقمية، التشفري، فك التشفر، خوارزمية *arnold's cat map*، خوارزمية تشفير أفيني، توليدالمفتاح، الخريطة اللوجستية.

سهولة التواصل وتبادل المعلومات لا تنفصل عن ظهور جرائم مثل الاختراق وسرقة البيانات ونشر المعلومات التي لا ينبغي نشرها. هناك أنواع مختلفة من البيانات المهمة التي يمكن حمايتها، ومنها البيانات المرئية (الصور الرقمية). يحتوي تشفير على العديد من الخوارزميات والطرق لتشفير الرسائل والبيانات. يبحث هذا البحث عن طريقة التشفير الفائق من خلال بمع *Arnold's Cat Map* و تشفير أفيني. تحتوي كل خوارزمية تشفير على مفتاح يؤثر على جودة عملية التشفير. يمكن تحديد المفتاح بشكل مباشر أو عن طريق توليده. بالطبع، فإن عملية التوليد ستحسن جودة عملية التشفير. يمكن استخدام معادلة الخريطة اللوجستية ، وهي أيضًا تقنية فوضوية مثل *Arnold's Cat Map*، لتوليد المفاتيح. في هذا البحث، تم تنفيذ توليد المفاتيح في تشفير أفيني باستخدام معادلة الخريطة اللوجستية.تنتج *Logistic map* سلسلة فوضوية من الأرقام العشوائية. هدف هذا البحث هو تحديد نتائج تشفير وفك تشفير البيانات المرئية (الصور الرقمية) باستخدام خوارزميات التشفير الفائق باستخدام خوارزميتي *Arnold's Cat Map* و تشفير أفيني وتوليد المفتاح باستخدام معادلة الخريطة اللوجستية التي سيتم استخدامها في تشفير أفيني أظهرت نتائج التجارب أن الصورة الناتجة عن عملية التشفير لها مستوى منخفض من التشابه مع الصورة الأصلية كما يظهر من قيمة متوسط مربعا الخطإ الكبيرة والتي يبلغ متوسطها ١٠٥,٣٨٧٣ ومستوى عالٍ من الضوضاء بناءً على قيمة نسبة ذروة الإشارة إلى الضوضاء التي يبلغ متوسط قيمتها أقل من ٣٠ ديسيبل.

.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Revolusi industri merupakan awal dari dimulainya perubahan tatanan teknologi dunia, dimana perkerjaan yang dahulu dilakukan oleh tenaga konvensional atau tangan manusia perlahan tergantikan oleh tenaga mesin (teknologi). Teknologi terus mengalami perkembangan pesat hingga sampai saat ini. Pada era modern saat ini, teknologi yang dikembangkan sangat bermanfaat bagi kehidupan sehari-hari manusia. hal itu dapat dilihat dari kemudahan manusia berkomunikasi dan saling bertukar informasi atau data jarak jauh. Dahulu seseorang ingin mengirim informasi atau data penting harus menggunakan jasa pengantar khusus agar informasi yang dikirim sampai kepada penerima, sekarang informasi dapat dikirim melalui perangkat komunikasi digital. Perangkat komunikasi digital ini dapat membuat seseorang berkomunikasi dan bertukar informasi dengan orang yang jaraknya ribuan kilometer dengan waktu singkat serta pesan yang disampaikan tidak hanya berupa pesan teks saja tapi juga sudah dapat mengirim pesan suara, video maupun gambar (citra digital).

Kemudahan dalam berkomunikasi dan saling bertukar informasi atau data yang yang lebih efisien tersebut tidak lepas dari munculnya tindak kejahatan. Sehingga menyebabkan tingkat permintaan terhadap keamanan informasi yang dipertukarkan mengalami peningkatan, salah satunya adalah keamanan data berbentuk informasi visual (citra digital). Informasi visual yang disampaikan bisa saja merupakan informasi rahasia, tentu hal ini dapat merugikan pihak pemilik informasi tersebut.

Informasi sama halnya seperti amanah dan aib yang salah satu tujuannya ialah untuk dirahasiakan sehingga hal itu hanya boleh diketahui oleh pemilik aib itu sendiri ataupun pihak-pihak tertentu saja. Al-Quran juga menjelaskan di dalam surah ke delapan yaitu surah Al-Anfal pada ayat ke-27 berbunyi.

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَخُوْنُوا اللّٰهَ وَالرَّسُوْلَ وَتَخُوْنُوْٓا اَمٰنٰتِكُمْ وَاَنْتُمْ تَعْلَمُوْنَ ﴿٢٧﴾

Artinya*:"Wahai orang-orang yang beriman! Janganlah kamu mengkhianati Allah dan Rasul dan (juga) janganlah kamu mengkhianati amanat yang dipercayakan kepadamu, sedangkan kamu mengetahui."* (Al-Anfal/8:27).

Dalam tafsir Ibnu Katsir surah tersebut merujuk pada kejadian Abu Lubabah dimana Rasulullah mengutus kepada Bani Quraizhah untuk menyampaikan pesan agar mereka tunduk pada hukum Rasulullah SAW. Namun Abu Lubabah mengisyaratkan tangan dileher yang berarti mati. Kemudian beliau sadar atas perilaku khianat dirinya dan akhirnya beliau bertobat dengan mengikat dirinya pada tiang sampai hingga taubatnya diterima dan yang melepaskan ikatannya adalah Rasulullah SAW sendiri.

Dalam surah di atas Allah SWT. memerintahkan kita agar menjaga amanah dalam hal ini amanah dapat kita pahami juga sebagai informasi atau data. Selain menjaga informasi atau data yang kita jaga juga harus disampaikan kepada orang yang seharusnya menerima informasi tersebut tanpa diketahui orang yang tidak seharusnya mengetahui sehingga tidak terjadi kesalahpahaman. Untuk menghindari informasi yang seharusnya rahasia tidak tersebar atau diketahui orang lain maka diperlukan solusi agar informasi atau pesan citra digital tetap aman terjaga hingga sampai kepada tujuan atau orang yang dituju.

Bidang ilmu yang membahas tentang tentang bagaimana mengamankan data citra digital yang umum digunakan saat ini ialah ilmu kriptografi. Kriptografi

memiliki tiga fungsi dasar untuk melakukan pengamanan terhadap pesan dan data informasi yaitu enkripsi, dekripsi dan kunci. Enkripsi berperan dalam mengamankan pesan dan data. Enkripsi citra bertujuan untuk menyandikan citra (*plain-image*) sehingga sulit bahkan tidak dapat dikenali lagi. (Munir, Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map, 2012)

Algoritma enkripsi memiliki kekuatan pengamanan berdasarkan seberapa besar perbedaan dari pesan yang telah disandi dengan pesan asli. Salah satu algoritma penyandian adalah algoritma *Arnold's Cat Map*. Algoritma *Arnold's Cat Map* merupakan algoritma tranformasi dimana piksel diacak dari posisi semula ke posisi yang berbeda berdasarkan iterasinya. Algoritma ini termasuk algoritma yang sangat baik dalam melakukan proses penyandian citra digital. Dikarenakan algoritma *Arnold's Cat Map* merupakan salah satu dari fungsi *chaos*. Dimana akan menghasil pesan citra yang akan bersifat sangat acak dan sulit dikenali. Namun, algoritma *Arnold's Cat Map* memiliki kelemahan yaitu seperti dalam penelitian Ronsen Purba dkk (2014), yang menyebutkan algoritma tersebut memiliki kelemahan dalam hal iterasi. Oleh karena itu, untuk menghadapi hal tersebut dibutuhkan suatu metode yaitu salah satunya dengan mengkolaborasikan algoritma *Arnold's Cat Map* tersebut dengan algoritma kedua atau yang biasa disebut dengan *super-encryption* (Super Enkripsi).

Super encryption merupakan salah satu metode penyandian pesan (enkripsi) dengan menggunakan dua algoritma berbeda dalam proses penyandian pesan. Metode ini umumnya menggabungkan metode tranposisi dan substitusi. Pada tahun 2012, Rinaldi Munir melakukan penelitian menggunakan metode *super encryption*

dengan menggunakan dua metode *chaotic* yaitu *Chaotic Arnold's Cat Map* dan *chaotic Logistic Map*. Ada banyak algoritma yang dapat dijadikan sebagai algoritma kedua untuk meningkatkan proses enkripsi sebuah citra digital salah satunya adalah algoritma *Affine Cipher*. *Affine Cipher* cukup baik dijadikan algoritma kedua dalam *super encryption* dikarenakan termasuk dalam cipher yang sederhana dan efisien sehingga tidak membebani dalam proses penyandiannya.

Affine Cipher termasuk *cipher* substitusi dimana setiap karakter akan diganti dengan karakter lain. *Affine Cipher* juga sudah lazim dikombinasikan dengan algoritma lain untuk meningkatkan keamanan dalam proses penyandian data dan pesan. *Affine Cipher* selain cipher sederhana dengan hasil enkripsi yang baik, dimana setiap piksel dari citra digital akan dilakukan perhitungan dengan persamaan enkripsi-nya.Umumnya, *Affine Cipher* menggunakan dua kunci yang bersifat tunggal, hal itu dapat menjadi kekurangan yang dapat dipecahkan salah satunya dengan *exhaustive key search.* Sehingga untuk menutupi kekurangan tersebut dibutuhkan kunci dengan nilai yang beragam yang dapat dilakukan dengan pembangkitan kunci bernilai acak (*Pseudorandom generator*). Berdasarkan penelitian Rini Arianty dan Diana Tri Susetianingtias (2020), menunjukan *Logistic Map* dapat dimanfaatkan sebagai generator pembangkit kunci. Kunci yang dibangkitkan dengan *Logistic Map* akan menghasilkan deretan bilangan acak. Oleh karena itu, peneliti ingin memanfaatkan *Logistic Map* sebagai pembangkit kunci untuk mengatasi kekurangan tersebut.

Berdasarkan penelitian terdahulu dan penjelasan diatas, penelitian ini akan meneliti bagaimana proses penyandian pesan gambar (citra digital) dengan menggunakan algoritma *super encryption* yaitu dengan mengkolaborasikan

algoritma *Arnold's Cat Map* dan *Affine Cipher* serta dengan melakukan pembangkitan kunci bilangan acak dengan menggunakan *Logistic Map.*

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan dapat diketahui beberapa rumusan masalah sebagai berikut.

1. Bagaimana proses enkripsi menggunakan algoritma super enkripsi dengan menggunakan algoritma *Arnold's Cat Map* dan *Affine Cipher* dengan pembangkitan kunci menggunakan persamaan *Logistic Map.*
2. Bagaimana proses dekripsi menggunakan algoritma super enkripsi dengan menggunakan algoritma *Arnold's Cat Map* dan *Affine Cipher* dengan pembangkitan kunci menggunakan persamaan *Logistic Map.*

1.3 Tujuan Penelitian

Penelitian ini memiliki tujuan untuk mengetahui bagaimana proses enkripsi dan proses dekripsi pada citra digital dengan menggunakan metode super enkripsi yaitu metode dengan menggunakan dua algoritma penyandian yaitu algoritma *Arnold's Cat Map* dan *Affine Cipher* yang kemudian pada algoritma *Affine Cipher* terdapat perubahan dimana kunci pada *Affine Cipher* akan menggunakan kunci hasil pembangkitan dengan menggunakan persamaan *Logistic Map.*

1.4 Manfaat Penelitian

Beberapa manfaat yang dapat diperoleh dari hasil penelitian ini yaitu sebagai berikut.

1. Memperoleh dan menambah wawasan keilmuan dan pegetahuan tentang algoritma kriptografi yang digunakan dalam penelitian ini (*Arnold's Cat*

Map dan *Affine Cipher*).

2. Penelitian dapat menjadi rujukan dalam perkembangan penelitian-penelitian selanjutnya terkait pengamanan pesan gambar (citra digital).
3. Kode program pengamanan dapat dimanfaatkan sebagai salah satu metode pengamanan untuk berbagai media berkomunikasi.

1.5 Batasan Penelitian

Penelitain ini memiliki beberapa batasan masalah sebagai berikut.

1. Penggunaan Persamaan *Logistic Map* untuk Pembangkitan kunci dilakukan pada algoritma *Affine Cipher.*
2. Penelitian ini membatasi citra yang digunakan dengan format ekstensi bmp (bitmap) dan PNG (*Portable Network Graphics*).
3. Citra digital yang digunakan berupa citra digital berwarna (RGB) dengan berukuran 512×512 piksel.

Proses enkripsi dan dekripsi citra akan dilakukan dengan Bahasa pemograman python dengan *Visual Studio Code* sebagai *text-editor.*

BAB II
KAJIAN TEORI

2.1 Keterbagian

Keterbagian bilangan adalah bagian mendasar dari berbagai sifat-sifat pada teori bilangan. Sehingga keterbagian harus dipahami terlebih dahulu.

Definisi 1:

Misalkan $p, q \in \mathbb{Z}$, dengan $p \neq 0$, maka p disebut membagi q ditulis sebagai $p|q$ apabila $q = px$, untuk suatu $x \in \mathbb{Z}$. (Irawan, Hijriyah, & Habibi, 2014)

Berdasarkan definisi, suatu bilangan bulat p dengan $p \neq 0$, dikatakan membagi bilangan bulat q bila terdapat suatu bilangan bulat x sedemikian sehingga $q = px$. Notasi $p|q$ dibaca "p membagi q" atau juga bisa dibaca "q habis dibagi p" atau "p pembagi q". Jika p tidak membagi q, maka ditulis sebagai $p \nmid q$.

Contoh :

1. $4|20$, karena terdapat $x = 5 \in \mathbb{Z}$ sehingga $20 = 4 \cdot 5$
2. $7|28$, karena terdapat $x = 4 \in \mathbb{Z}$ sehingga $28 = 7 \cdot 4$
3. $5 \nmid 16$, karena tidak terdapat $x \in \mathbb{Z}$ sehingga $16 = 5 \cdot x$

2.2 Greatest Common Divisor

Himpunan pembagi dari 12 adalah 1, 2, 3, 4, 6 dan 12. Himpunan pembagi dari 18 adalah 1, 2, 3, 6, 9, dan 18. Kemudian {1, 2, 3, 6} adalah himpunan pembagi yang sama dari 12 dan 18. Perhatikan bahwa himpunan tersebut memiliki nilai terbesar yaitu 6. Konsep tersebutlah yang disebut dengan perseketuan terbesar bersama.

Definisi 2 :

Misalkan bahwa c dan d adalah bilangan bulat dan keduanya tak-nol. Kemudian terdapat element r merupakan element terbesar dari himpunan persekutuan bersama, element tersebut disebut *greatest common divisor* dari p dan q. Dapat ditulis $r = \gcd(c, d)$. (Kraft & Washington, 2013)

Contoh :

1. $\gcd(24,52) = 4$
2. $\gcd(9,27) = 9$
3. $\gcd(15,28) = 1$

2.3 Relatif Prima

Relatif Prima atau yang disebut juga *co-prime numbers* merupakan penyebutan terhadap dua bilangan bulat yang tidak memiliki faktor persekutuan terbesar bersama selain 1.

Definisi 3 :

Dua bilangan c dan d adalah bilangan bulat positif, dikatakan relatif prima apabila pembagi bersama terbesarnya $\gcd(c, d)$ = 1.

Contoh :

Diketahui c = 31 dan d = 212, buktikan dua bilangan bulat tersebut relatif prima.

Berikut faktor pembagi dari masing-masing bilangan bulat:

Faktor pembagi 31 = 1,31;

Faktor pembagi 212 = 1,2,4,53,106,212;

Diketahui pembagi yang sama diantara kedua bilangan bulat tersebut adalah 1 dan merupakan pembagi terbesar yang sama.

Jadi, $\gcd(31,212) = 1$, dan kedua bilangan bulat tersebut relatif prima.

2.4 Kongruensi

Pembicaraan tentang kongruensi tidak terlepas dari masalah keterbagian. Karena konsep keterbagian dan sifat-sifatnya merupakan pengkajian secara lebih dalam dengan menggunakan konsep kongruensi. Sehingga kongruensi adalah cara lain untuk mengkaji keterbagian dalam himpunan bilangan bulat. (Irawan, Hijriyah, & Habibi, 2014)

Definisi 4 :

Misalkan m adalah bilangan bulat lebih dari 0, membagi selisih $p - q$, maka kita katakana p kongruen dengan q Modulo M, dan ditulis :

$$p \equiv q (\text{mod } M)$$

Jika $p - q$ tidak dibagi M, maka kita katakan tidak kongruen dengan q Mod M dan dituliskan:

$$p \not\equiv q (\text{mod } M)$$

2.5 Aritmatika Modulo

Aritmatika modulo adalah bagian dari ilmu matematika yang berperan penting dalam matematika komputasi, terkhususnya pada penerapan kriptografi. Aritmatika modulo menggunakan operator mod (modulo).

Definisi 5 :

Misalkan p adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi $p \bmod m$ (dibaca"p modulo m") memberikan sisa apabila p dibagi dengan m. Bilangan m disebut "modulus" atau "modulo", dan hasil operasi modulo m terletak di dalam himpunan $\{0, 1, 2, \dots, m - 1\}$. (Munir, Kriptografi, 2019)

2.6 Balikan Modulo (*Modulo Invers*)

Aritmatika bilangan riil memperkenalkan tentang balikan perkalian (*Invers*). Seperti balikan perkalian dari p yaitu $1/p$ sedemikian hingga $p \times 1/p = 1$. Konsep balikan juga terdapat pada aritmatika modulo (*modulo invers*), apabila diberikan $p(\mathrm{mod}\, m)$, Bilangan bulat p memiliki *invers* dalam modulus m hanya jika p dan m relatif prima dan $m > 1$. *Invers dari* $p(\mathrm{mod}\, m)$ adalah sebuah bulangan bulat p^{-1} sedemikian sehingga (Munir, Kriptografi, 2019)

$$p \times p^{-1} \equiv 1(\mathrm{mod}\, m)$$

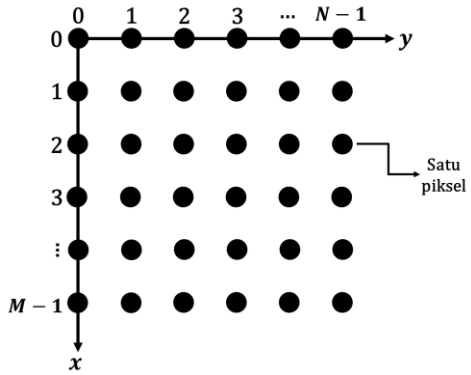
2.7 Citra Digital

Citra merupakan suatu gambaran atau kemiripan dari suatu objek. Citra analog tidak dapat direpresentasikan di dalam komputer, sehingga citra analog tidak bisa diproses oleh komputer secara langsung. Tentu agar citra bisa diproses di komputer, citra analog harus dikonversi kedalam citra digital. Citra digital merupakan citra yang dapat diolah oleh komputer (Andono, Sutojo, & Muljono, 2017). Citra digital dapat di proses di komputer karena citra analog dirubah menjadi citra kontinu dengan nilai M baris dan N kolom, sehingga menjadi citra diskrit. Nilai pada titik pertemuan baris dan kolom inilah yang disebut sebagai piksel.

Titik koordinat dan nilai intensitas adalah parameter yang dimiliki oleh sebuah piksel. Nilai pada koordinat (x, y) adalah $f(x, y)$, yaitu besar nilai intensitas atau warna pada piksel tersebut. Umumnya nilai pada citra warna atau RGB (*Red, Green, and Blue*) dan *grayscale* berada pada rentang nilai 0 – 255. Pada citra hitam putih intesitas hanya terdiri dari dua angka 0 dan 1, dimana 0 mewujudkan warna hitam dan 1 mewujudkan warna putih. Piksel dapat di gambar sebagai sistem

koordinat berikut.

Berdasarkan Gambar 2.1, citra digital dapat dituliskan dalam bentuk matriks dengan ordo $M \times N$ berikut.



Gambar 2.1 Skema Sistem Koordinat pada Citra Digital

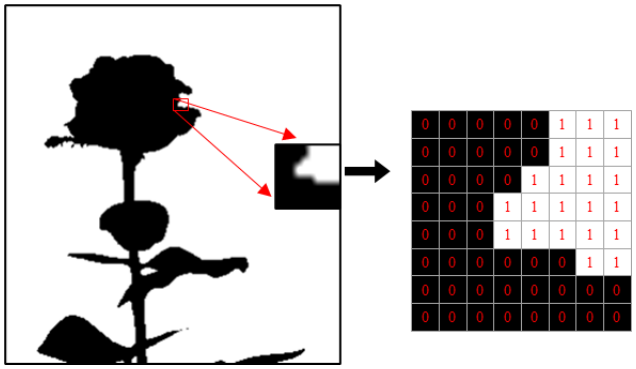
$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,N-1) \\ f(1,0) & \cdots & \cdots & f(1,N-1) \\ \dots & \dots & \dots & \dots \\ f(M-1,0) & f(M-1,1) & \dots & f(M-1,N-1) \end{bmatrix}$$

Dari gambar matriks di atas dapat diketahui $f(x,y)$ adalah fungsi intensitas dimana nilai *x* (baris) dan *y* (kolom) sebagai koordinat posisi.

Ada tiga jenis citra digital yang banyak digunakan dalam berbagai penelitian dan pengolahan citra yaitu sebagai berikut.

2.7.1 Citra Biner

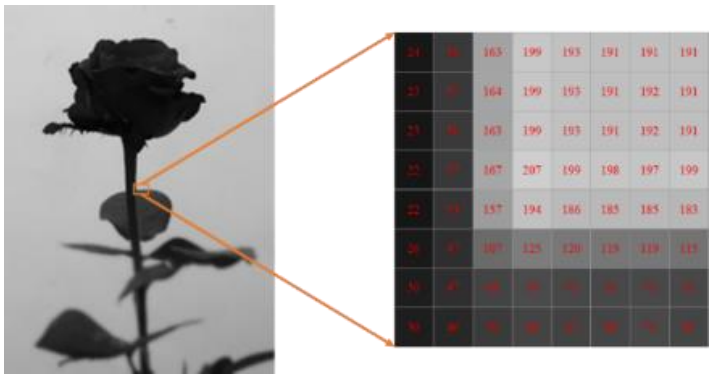
Citra biner atau yang sering dikenal sebagai gambar (citra) hitam putih merupakan jenis citra yang nilai intensitas $(f(x,y))$ setiap piksel terdiri dua indeks intensitas yaitu 0 dan 1, dimana nilai 0 akan menghasilkan warna piksel hitam dan nilai 1 akan menghasilkan warna piksel putih.



Gambar 2.2 Bentuk Nilai Piksel pada Citra Hitam-Putih

2.7.2 Citra Skala Abu-Abu

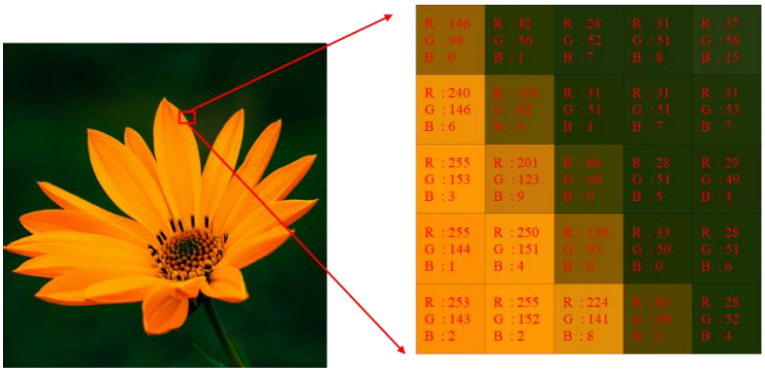
Citra Skala Abu-Abu (*Grayscale*) adalah jenis citra dimana nilai intensitas matriks setiap pikselnya berada pada rentang nilai 0 – 255 sehingga setiap piksel membutuh 8-bit memori. Nilai 0 – 255 menunjukan skala dari kegelapan dan kecerahan piksel tersebut.



Gambar 2.3 Bentuk Nilai Piksel pada Citra *Grayscale*

2.7.3 Citra Warna

Citra Warna merupakan jenis citra yang setiap titik pikselnya terdapat tiga komponen intensitas yang berbeda yaitu *Red* (merah), *Green* (hijau), dan *Blue* (biru). Seperti halnya citra *grayscale* setiap komponen memiliki nilai dalam rentang 0 – 255. Karena citra warna memiliki 3 komponen berbeda sehingga setiap pikselnya membutuhkan 24-bit memori.



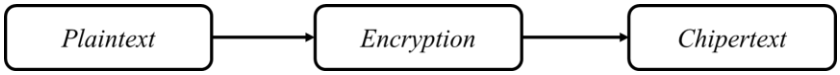
Gambar 2.4 Bentuk Nilai Piksel pada Citra RGB

2.8 Kriptografi

Menurut bahasa kata kriptografi terbagi menjadi dua kata yaitu kripto yang berarti rahasia dan graphia berarti tulisan, apabila kedua kata disatukan maka bermakna tulisan atau pesan rahasia. Kriptografi merupakan ilmu mengenai metode enkripsi dimana data diproses dengan menggunakan kunci enkripsi menjadi sesuatu data yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi (Kromodimoeljo, 2010). Sejarah mencatat, kriptografi telah digunakan oleh bangsa Mesir kuno tapatnya sekitar 4000 tahun yang lalu, yang mana kriptografi dipergunakan sebagai pesan rahasia yang dikirimkan kepada pasukan militer agar pesan tidak diketahui oleh pihak musuh walaupun sang kurir pesan tertangkap.

Kriptografi merupakan ilmu tentang metode-metode berkomunikasi secara aman antara dua pihak. Spesifiknya, ada dua pihak yang ingin saling mengirim pesan tetapi mereka ingin menghindari kemungkinan pihak ketiga memahami pesan ini jika jatuh ke tangan yang salah (Rubinstein-Salzedo, 2018). Kedua pihak dapat mengirim pesan secara aman dengan melakukan penyandian pesan dengan suatu algoritma kriptografi. Tiga fungsi dasar yang dimiliki algoritma kriptografi yaitu enkripsi, dekripsi, dan kunci.

1. **Enkripsi** adalah sebuah operasi yang merubah pesan generik (*plaintext*) ke pesan sandi (*Ciphertext*).

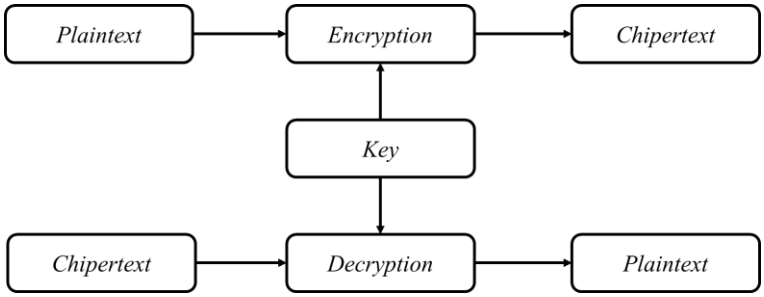


Gambar 2.5 Gambaran Alur Sederhana Proses Enkripsi

2. **Dekripsi** adalah sebuah operasi yang mengembalikan pesan sandi (*Ciphertext*) ke dalam bentuk pesan semula (*Plaintext*).

Gambar 2.6 Gambaran Alur Sederhana Proses Dekripsi

3. **Kunci** adalah komponen penting dalam sebuah algoritma penyandian tanpa sebuah kunci algoritma tidak dapat berjalan. Ada dua jenis kunci pada proses penyandian yaitu kunci publik dan kunci pribadi (*private*) atau rahasia.



Gambar 2.7 Gambaran Alur Sederhana Penggunaan *Key*

2.9 *Arnold's Cat Map*

Vladimit I. Arnold adalah seorang ahli matematika yang berasal dari Rusia memperkenalkan pertama kali sebuah algoritma enkripsi dengan mendemonstrasikan algoritma miliknya dengan menggunakan citra kucing (Purba, Halim, & Syahputra, 2014). *Arnold's Cat Map* bekerja dengan memetakan setiap titik dalam gambar ke koordinat baru dengan cara mengalikan koordinat asli dengan sebuah matriks transformasi linier dan kemudian mengambil nilai hasil modulo pada batas gambar. Proses ini diulang sejumlah iterasi tertentu untuk menciptakan

efek "campuran" yang kuat pada piksel gambar, sehingga sulit untuk membaca atau mengidentifikasi gambar asli.

Metode enkripsi *Arnold's Cat Map* akan mentrasformasikan setiap titik piksel pada matriks asal $(M \times M)$ yang dipresentasikan dengan (x, y) menjadi (x', y') yang menunjukan hasil transformasi dari titik asal matriks. Sehingga semua titik piksel pada matriks akan teracak berdasarkan iterasi yang ditentukan.

Algoritma *Arnold's Cat Map* memiliki persamaan enkripsi sebagai berikut.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = [A] \begin{bmatrix} x \\ y \end{bmatrix} \bmod(M) \tag{2.1}$$

Keterangan:

1. (x, y) : Titik baris dan kolom awal matriks
2. (x', y') : Titik baris dan kolom baru matriks
3. $[A]$: Matriks transformasi *Arnold's Cat Map*
4. mod : Modulo
5. M : Banyaknya kolom/baris matriks
6. c : Kunci (rahasia)
7. d : Kunci (rahasia)

$[A]$ adalah sebuah matriks transformasi yang digunakan untuk mentranformasikan nilai piksel pada matriks. Matriks $[A]$ didefinisikan sebagai $\begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}$ dimana nilai c dan d bilangan bulat positif sehingga nilai determinan yang diperoleh matriks $[A] = 1$. Hasil setelah pemrosesan dengan persamaan *Arnold's Cat Map* dengan jumlah iterasi d akan berbentuk citra digital teracak yang nilai piksel pada matriksnya sama dari citra digital asal namun dengan koordinat yang berbeda. Jumlah pengulangan (iterasi) yang harus diselesaikan di dasarkan

pada parameter *c*. *d* dan ukuran *M* citra digital asli (*plain-image*). Jadi algoritma *Arnold's Cat Map* mempunyai parameter *c, d,* dan banyaknya iterasi , semua parameter tersebut dapat digunakan sebagai kunci rahasia (Hariyanto & Rahhim, 2016).

Proses dekripsi algoritma *Arnold's Cat Map* sedikit berbeda dari persamaan enkripsinya. Tepatnya pada nilai matriks [*A*] akan dirubah kedalam bentuk matriks *invers* $[A]^{-1} = \begin{bmatrix} cd+1 & -c \\ -d & 1 \end{bmatrix}$, sehingga persamaan dekripsinya sebagai berikut.

$$\begin{bmatrix} x \\ y \end{bmatrix} = [A]^{-1} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod(M) \tag{2.2}$$

2.10 *Logistic Map*

Logistic Map (Peta Logistik) merupakan salah satu jenis *non-linear dynamic map* yang diperkenalkan oleh ahli matematika Robert May pada tahun 1976. *Logistic Map* merupakan salah satu dari metode *chaos* yang sederhana berbentuk persamaan iterative.

Dari parameter di atas, dapat dipahami variabel yang digunakan dalam persamaan *Logistic Map,* Adapun persamaan *Logistic Map* sebagai berikut.

$$x_{n+1} = r x_n (1 - x_n) \tag{2.3}$$

Keterangan :

1. x_n : Nilai awal pada saat n
2. x_{n+1} : Nilai pada saat $n + 1$
3. r : parameter
4. n : Moment/waktu

Dimana x_n adalah bilangan antara 0 dan 1 ($0 \leq x_n \leq 1$) yang mempresetasikan ukuran populasi pada waktu n. Sedangkan r (kadang dimisalkan sebagai μ) adalah parameter fungsi yang menunjukan laju pertumbuhan dengan nilainya $0 \leq r \leq 4$. *Logistic Map* akan memiliki sifat *chaos* (kacau) apabila nilai $3.569946 \leq r \leq 4$.

Akhir 1940-an, John Von Neumann Menyarankan untuk menggunakan persamaan logistik tersebut sebagai generator bilangan acak (*Keystream*). Nilai – nilai acak yang dihasilkan dari persamaan *Logistic Map* tidak dapat langsung dioperasi modulokan dalam penggunaannya sebagai kunci persamaan *Affine Cipher* karena masih berupa bilangan riil antara 0 sampai 1. Nilai tersebut harus ditransformasikan menjadi nilai bilangan bulat (*integer*).

2.11 *Affine Cipher*

Affine Cipher merupakan sebuah penyandian substitusi, yang mana setiap huruf dalam alfabet dikonversikan ke dalam persamaan numerik, dienkripsikan dengan sebuah persamaan aritmatika dan dikonversikan kembali kedalam huruf (Mezaal & Abdulkareem, 2017). Kunci pada *Affine Cipher* adalah algoritma enkripsi perluasan dari algoritma *Caesar Cipher,* dengan melakukan operasi perkalian pada *plaintext* dengan sebuah nilai konstanta *m* kemudian menjumlahkan hasilnya dengan kunci *b*.

Selain diterapkan dalam pengamanan pesan teks, *Affine Cipher* juga dapat diterapkan pada enkripsi citra digital dengan mengubah nilai piksel dalam citra menjadi nilai yang terenkripsi menggunakan fungsi matematika sederhana. Sebagai contoh, jika citra digital menggunakan ruang warna *grayscale* maka setiap piksel

akan direpresentasikan oleh sebuah bilangan bulat yang berkisar dalam rentang 0 hingga 255.

Berdasarkan parameter di atas berikut persamaan yang digunakan dalam algoritma *Affine Cipher*.

$$C = (mP + b)\ mod(M) \tag{2.4}$$

Keterangan :

1. C : Chipertext (pesan rahasia)
2. P : Plaintext (pesan asli)
3. m : Konstanta
4. b : Kunci (rahasia)
5. mod : Modulo
6. M : Ukuran matriks
7. m^{-1} : Invers dari konstanta

Dimana nilai *m* adalah bilangan bulat yang harus relatif prima terhadap *M*, serta *b* adalah kunci enkripsi. Persamaan dekripsi pada algoritma *Affine Cipher* tidak terlalu jauh berbeda dari persamaan enkripsi nya dimana nilai *m* pada persamaan akan dirubah dalam bentuk *invers* (m^{-1}(mod (M) serta kode pesan (*cipher-image*) akan dikurangi dengan nilai kunci.

$$P = m^{-1}(\ C - b\ )\text{mod}(M) \tag{2.5}$$

2.12 *Super Encryption*

Proses enkripsi dengan menggunakan suatu algoritma tertentu memiliki kelemahan tersendiri, baik dari iterasi, kunci, bahkan persamaan yang digunakan. Oleh karena itu untuk meningkatkan kesulitan suatu proses enkripsi maka

dibutuhkannya peningkatan, salah satu cara untuk meningkatkan kesulitan proses enkripsi yaitu dengan menggunakan metode enkripsi super.

Enkripsi Super (*Super Encryption*) merupakan salah satu kriptografi berbasis karakter yang menggabungkan dua algoritma cipher. Hal tersebut memiliki tujuan untuk mendapatkan cipher yang lebih kuat sehingga tidak mudah untuk dipecahkan, dan juga untuk mengatasi penggunaan cipher tunggal yang secara komparatif lemah. (Setyaningsih, Iswahyudi, & Widyastuti, 2011)

Enkripsi super umumnya menggunakan satu cipher transposisi dan satu cipher substitusi. Bersamaan dengan hal tersebut pada penelitian ini menggunakan algoritma *Arnold's Cat Map* sebagai cipher transposisi dan *Caesar Cipher* sebagai cipher substitusi.

2.13 *Mean Square Error*

Mean Square Error merupakan salah satu jenis pengukuran berdasarkan kesalahan statistik. Dimana MSE termasuk dalam pengukuran kualitas citra secara objektif. Secara objektif artinya pengukuran dilakukan tanpa campur tangan manusia. MSE digunakan untuk mengukur nilai tingkat kesamaan antara citra sebelum diproses dengan citra sesudah diproses. MSE adalah ukuran yang digunakan untuk menilai seberapa baik sebuah metode dalam melakukan rekonstruksi atau restorasi citra relatif terhadap citra originalnya.

Untuk menentukan nilai MSE dengan menggunakan persamaan sebagai berikut.

$$\text{MSE} = \frac{1}{M \times N} \sum_{x}^{M} \sum_{y}^{N} \left[f_1(x,y) - f_2(x,y) \right]^2$$

Keterangan :

1. MSE : Nilai *Mean Square Error*
2. M : Banyaknya Kolom
3. N : Banyaknya Baris
4. $f_1(x,y)$: Nilai Entri Matriks Pertama pada Baris x dan Kolom y
5. $f_2(x,y)$: Nilai Entri Matriks Kedua pada Baris x dan Kolom y

Semakin kecil (mendekati 0) nilai MSE menunjukan bahwa hasil dari pemrosesan citra semakin bagus, atau dengan kata lain citra setelah diproses semakin mendekati citra aslinya (Andono, Sutojo, & Muljono, 2017).

Jadi, semakin besar nilai MSE menunjukan citra setelah proses semakin berbeda dari citra aslinya.

Contoh :

Diberikan dua matriks A dan B dengan masing -masing ukuran 2 x 2 sebagai berikut.

$A = \begin{bmatrix} 10 & 3 \\ 7 & 12 \end{bmatrix}$, $B = \begin{bmatrix} 5 & 21 \\ 13 & 9 \end{bmatrix}$

Kemudian nilai-nilai pada matriks disubstitusikan kedalam persamaan MSE

$MSE = \frac{1}{2\times2}((10-5)^2+(3-21)^2+(7-13)^2+(12-9)^2)$

$= \frac{1}{4}((5)^2+(-18)^2+(-6)^2+(3)^2)$

$= \frac{1}{4}(25+324+36+9)$

$= \frac{1}{4}(394)$

$= 98.5$

Jadi, diperoleh nilai eror dari kedua matriks adalah 98.5

2.14 *Peak Signal-to-Noise Ratio*

Peak Signal-to-Noise Ratio merupakan salah satu jenis pengukuran pengukuran kualitas citra yang mana hasil perhitungan yang menentukan nilai *noise* dari sebuah citra digital. *Peak Signal-to-Noise Ratio* atau yang disingkat PSNR dapat dihitung dengan syarat memiliki nilai *Mean Square Error.* Adapun berikut persamaan yang digunakan untuk menghitung nilai PSNR.

$$PSNR = 10\log_{10}(MaxCit^2 \times \frac{1}{MSE})$$

Keterangan :

MSE : Nilai *Mean Square Error*

MaxCit : Nilai Maksimum dari sebuah piksel citra yang digunakan

2.15 Kajian Keagamaan

Setiap manusia memiliki ruang pribadi (*privacy*) sendiri seperti aib atau pun sesuatu yang bersifat privasi atau rahasia dan tidak boleh diketahui dan disebarkan oleh orang lain tanpa seizin pemiliknya. Allah S.W.T. dalam firmannya talah menjelaskan agar sesama manusia untuk saling menghormati batas-batas privasi. Hal tersebut juga banyak dijelaskan dalam berbagai hadits. Salah satu hadits yang diriwayatkan dalam kitab *shahih bukhari* yang berbunyi.

حَدَّثَنَا بِشْرُ بْنُ مُحَمَّدٍ أَخْبَرَنَا عَبْدُ اللَّهِ أَخْبَرَنَا مَعْمَرٌ عَنْ هَمَّامِ بْنِ مُنَبِّهٍ عَنْ أَبِي هُرَيْرَةَ عَنْ النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ إِيَّاكُمْ وَالظَّنَّ فَإِنَّ الظَّنَّ أَكْذَبُ الْحَدِيثِ وَلَا تَحَسَّسُوا وَلَا تَجَسَّسُوا وَلَا تَحَاسَدُوا وَلَا تَدَابَرُوا وَلَا تَبَاغَضُوا وَكُونُوا عِبَادَ اللَّهِ إِخْوَانًا (رواه بخاري)

Artinya:*"Telah menceritakan kepada kami Bisyr bin Muhammad telah memberi kabar kepada kami Abdullah telah memberi kabar kepada kami Ma'mar dari Hammam bin Munabbih dari Abu Hurairah dari Nabi Shallallahu 'alaihi wassalam beliau bersabda: "Jauhilah prasangka buruk, karena prasangka buruk adalah ucapan yang paling dusta, janganlah kalian saling mendiamkan, janganlah suka*

mencari-cari aib, saling mendengki, saling membenci, tetapi, jadilah kalian hamba-hamba Allah yang bersaudara".” (HR Bukhari no 5604)

Hadits tersebut menunjukan larangan kepada kita untuk tidak saling membenci, mencari aib orang lain dan berprasangka buruk antar sesame muslim utamanya. Sama halnya seperti aib atau sesuatu yang bersifat rahasia, pesan atau informasi juga ada yang bersifat privasi atau rahasia serta hanya diketahui pemilik informasi dan penerima informasi. Oknum-oknum tertentu yang tidak bertanggung jawab selalu ingin membocorkan informasi/pesan yang seharusnya bersifat rahasia untuk memperoleh keuntungan pribadi. Oknum yang melakukan hal tersebut termasuk golongan orang buruk dan akan mendapat balasan di akhirat kelak.

حَدَّثَنَا يَحْيَى بْنُ أَكْثَمَ وَالْجَارُودُ بْنُ مُعَاذٍ قَالَا حَدَّثَنَا الْفَضْلُ بْنُ مُوسَى حَدَّثَنَا الْحُسَيْنُ بْنُ وَاقِدٍ عَنْ أَوْفَى بْنِ دَلْهَمٍ عَنْ نَافِعٍ عَنْ ابْنِ عُمَرَ قَالَ صَعِدَ رَسُولُ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ الْمِنْبَرَ فَنَادَى بِصَوْتٍ رَفِيعٍ فَقَالَ يَا مَعْشَرَ مَنْ أَسْلَمَ بِلِسَانِهِ وَلَمْ يُفْضِ الْإِيمَانُ إِلَى قَلْبِهِ لَا تُؤْذُوا الْمُسْلِمِينَ وَلَا تُعَيِّرُوهُمْ وَلَا تَتَّبِعُوا عَوْرَاتِهِمْ فَإِنَّهُ مَنْ تَتَبَّعَ عَوْرَةَ أَخِيهِ الْمُسْلِمِ تَتَبَّعَ اللَّهُ عَوْرَتَهُ وَمَنْ تَتَبَّعَ اللَّهُ عَوْرَتَهُ يَفْضَحْهُ وَلَوْ فِي جَوْفِ رَحْلِهِ قَالَ وَنَظَرَ ابْنُ عُمَرَ يَوْمًا إِلَى الْبَيْتِ أَوْ إِلَى الْكَعْبَةِ فَقَالَ مَا أَعْظَمَكِ وَأَعْظَمَ حُرْمَتَكِ وَالْمُؤْمِنُ أَعْظَمُ حُرْمَةً عِنْدَ اللَّهِ مِنْكِ قَالَ أَبُو عِيسَى هَذَا حَدِيثٌ غَرِيبٌ لَا نَعْرِفُهُ إِلَّا مِنْ حَدِيثِ الْحُسَيْنِ بْنِ وَاقِدٍ وَرَوَى إِسْحَقُ بْنُ إِبْرَاهِيمَ السَّمَرْقَنْدِيُّ عَنْ حُسَيْنِ بْنِ وَاقِدٍ نَحْوَهُ وَرُوِي عَنْ أَبِي بَرْزَةَ الْأَسْلَمِيِّ عَنْ النَّبِيِّ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ نَحْوُ هَذَا(رواه الترمذي)

Artinya:*“Telah menceritakan kepada kami Yahya bin Aktsam dan Jarud bin Mu’adz keduanya berkata, telah menceritakan kepada kami Fadlu bin Musa, telah menceritakan kepada kami Husain bin Waqid dari Aufa bin Dalham dari nafi’ dari Ibnu Umar ia berkata: Rasulullah Shallallaahu ‘alaihi wa sallam menaiki mimbar lalu menyeru dengan suara yang lantang: “Wahai sekalian orang yang telah berIslam dengan lisannya namun keimanan belum tertancap di hatinya, janganlah kalian menyakiti kaum muslimin dan jangan pula kalian menelusuri dan membongkar aib mereka, maka barang siapa yang menyelidiki aib saudaranya se-Islam niscaya Allah akan menyelidiki aibnya dan barang siapa yang aibnya diselidiki oleh Allah niscaya Allah akan membongkar aibnya meskipun di dalam rumahnya sendiri.” Nafi' berkata: Suatu hari Ibnu Umar melihat Ka'bah, lantas beliau berkata, Betapa agungnya kamu, dan betapa luhurnya kehormatanmu namun seorang mukmin lebih agung kehormatannya di sisi Allah dari padamu.*

Berkata Abu Isa; Ini merupakan hadits gharib yang tidak kami ketahui kecuali dari haditsnya Husain bin Wakid. Dan [Ishaq bin Ibrahim Samarqandi] meriwayatkan dari [Husain bin Wakid] seperti hadits di atas. Diriwayatkan juga dari Abi Barzah Aslamy dari Nabi Shallallaahu 'alaihi wa sallam seperti hadits di atas." (HR Tirmidzi no 1955)

Agar menghindari kebocoran informasi/pesan yang bersifat rahasia maka peran ilmu kriptografi sangat penting. Dimana kriptografi akan mengamankan pesan atau informasi dari gangguan orang yang ingin mengetahui tanpa sepengetahuan pemiliknya. Berikut hadits mengapa sebaiknya kita menjaga aib kita dan aib saudara kita.

حَدَّثَنَا قُتَيْبَةُ حَدَّثَنَا اللَّيْثُ عَنْ عُقَيْلٍ عَنْ الزُّهْرِيِّ عَنْ سَالِمٍ عَنْ أَبِيهِ أَنَّ رَسُولَ اللَّهِ صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ قَالَ الْمُسْلِمُ أَخُو الْمُسْلِمِ لَا يَظْلِمُهُ وَلَا يُسْلِمُهُ وَمَنْ كَانَ فِي حَاجَةِ أَخِيهِ كَانَ اللَّهُ فِي حَاجَتِهِ وَمَنْ فَرَّجَ عَنْ مُسْلِمٍ كُرْبَةً فَرَّجَ اللَّهُ عَنْهُ كُرْبَةً مِنْ كُرَبِ يَوْمِ الْقِيَامَةِ وَمَنْ سَتَرَ مُسْلِمًا سَتَرَهُ اللَّهُ يَوْمَ الْقِيَامَةِ قَالَ أَبُو عِيسَى هَذَا حَدِيثٌ حَسَنٌ صَحِيحٌ غَرِيبٌ مِنْ حَدِيثِ ابْنِ عُمَرَ(رواه الترمذي)

Artinya:*"Telah menceritakan kepada kami Qutaibah telah menceritakan kepada kami Al Laits dari 'Uqail dari Az Zuhri dari Salim dari ayahnta bahwa Rasulullah shallallaahu 'alaihi wa sallam bersabda: "Seorang muslim adalah saudara bagi muslim lainnya, tidak menzhalimi dan tidak menganiayanya, barangsiapa yang menolong kebutuhan saudaranya, maka Allah akan senantiasa menolongnya. Barangsiapa menghilangkan kesusahan seorang muslim maka Allah akan menghilangkan kesusahan-kesusahannya pada hari kiamat. Dan barangsiapa menutup aib seorang muslim, maka Allah akan menutup aibnya pada hari kiamat." Abu Isa berkata; hadits ini hasan shahih Gharib dari hadits Ibnu Umar."* (HR Tirmidzi no. 1346)

Berdasarkan hadits riwayat at-tirmidzi no 1346 di atas, seorang muslim diajarkan untuk tidak boleh menzalimi orang lain terutama saudara sesama muslim. Perilaku menyebarkan aib atau pesan amanah yang bersifat rahasia atau pribadi juga merupakan termasuk kedalam sifat zalim. Saat ini perilaku menyebarkan aib tersebut sangat mudah dilakukan melalui media teknologi saat ini. Pelaku melakukan *hacking* dan mencari aib atau rahasia seseorang tersebut lalu

menyebarkannya untuk mendapatkan keuntungan sendiri. Dengan adanya ilmu kriptografi atau ilmu menyadikan pesan dan data hal tersebut dapat dihindari.

Apabila kita yang tidak sengaja mengetahui rahasia atau aib saudara kita maka hendaknya kita menjaganya dengan baik seperti halnya ilmu kriptografi tersebut menjaga pesan dari diketahui oleh orang lain. Dari hadits tirmidzi di atas juga menjelaskan bahwa *"Barangsiapa menutup aib seorang muslim, maka Allah akan menutup aibnya pada hari kiamat."*. karena sesuatu aib apabila diketahui orang banyak atau tersebar akan memiliki dampak besar kepada orang yang memiliki aib tersebut seperti pembunuhan karakter. Dimana dia akan merasa terkucil dan malu menghadapi kehidupan sosial.

BAB III
METODE PENELITIAN

3.1 Jenis Penelitian

Dalam Penelitian ini, jenis penelitian yang digunakan peneliti adalah metode penelitian eksperimen. Penelitian eksperimen adalah metode penelitian yang menggunakan pangaturan eksperimental untuk mempelajari hubungan antara sebab dan akibat suatu kejadian. Selain itu, penelitian ini juga termasuk penelitian yang objektif dan terkontrol dalam mempelajari suatu peristiwa. Sehingga peneliti dapat mengetahui hasil penelitian dengan hasil yang akurat. Alasan peneliti menggunakan penelitian ini dikarenakan sesuai dengan tujuan dari penelitian ini untuk mempelajari secara objektif dari proses enkripsi dan dekripsi citra digital menggunakan algoritma *Arnold's Cat Map* dan *Affine Cipher* dengan variabel-variabelnya, serta agar peneliti dapat menghasilkan perhitungan yang akurat dalam proses tersebut.

3.2 Data dan Sumber Data

Penelitian ini menggunakan jenis data berupa data gambar atau citra digital berwarna dengan ukuran citra $M \times M$ dengan ekstensi atau format .bmp (bitmap) dan PNG (*Portabel Network Graphic*).

3.3 Tahapan Penelitian

Penelitian memeliki tiga proses tahapan di awali dengan proses enkripsi, kemudian dekripsi dan di akhiri oleh tahap evaluasi.

3.3.1 Proses Enkripsi

Proses enkripsi terdiri dari dua tahap enkripsi, tahap pertama enkripsi menggunakan persamaan enkripsi *Arnold's cat map.*

1. Pada algoritma enkripsi *Arnold's Cat Map*, tentukan tiga kunci rahasia yaitu c, d dan banyaknya iterasi, dimana nilai c, d adalah bilangan bulat positif agar menghasilkan determinan matriks transformasi sebesar 1.
2. Mempersiapkan citra digital kemudian ubah menjadi matriks *plain-image* dengan ukuran $M \times M$.
3. Matriks *plain-image* yang masih terdiri dari tiga komponen warna dipisah menjadi tiga matriks *plain-image grayscale* berbeda.
4. Substitusikan nilai kunci (*c,d*) yang telah ditentukan ke dalam matriks transformasi *Arnold Cat Map* atau matriks $[A]$.

$$[A]=\begin{bmatrix}1 & c\\ d & cd+1\end{bmatrix}$$

5. Melakukan operasi perkalian matriks pada setiap entri ketiga matriks *plain-image* dengan matriks kunci [*A*]. kemudian hasil perkalian akan dimodulokon dengan nilai 256, agar intesitas sebuah citra yang diperoleh akan tetap berada pada rentang nilai 0 sampai 255.
6. Selanjutnya diperoleh matriks hasil operasi algoritma *Arnold's cat map.*

Setelah diperoleh matriks hasil operasi *Arnold's Cat Map,* melanjutkan proses enkripsi tahap kedua dengan persamaan enkripsi *Affine Cipher.*

1. Sebelum melakukan proses enkripsi, lakukan pembangkitan kunci dengan menggunakan persamaan *Logistic Map.* Tentukan inisialisasi nilai kunci r, x dan n, untuk nilai $3{,}569969 \le r \le 4$, $0 < x < 1$, dan $n = M \times M$ dimana nilai *n* adalah iterasi.

2. Dari proses pembangkitan kunci akan diperoleh matriks kunci *B* dan tentukan nilai kunci *m* yang harus relatif prima terhadap 256.
3. Selanjutnya akan dilakukan proses enkripsi tahap kedua dengan menggunakan persamaan algoritma *Affine Cipher* pada ketiga matriks hasil enkripsi sebelumnya.
4. Proses enkripsi akan menghasil tiga matriks *cipher-image* yang berbeda, kemudian disatukan kembali menjadi matriks citra berwarna.

3.3.2 Proses Dekripsi

Proses pendekripsi sama halnya seperti enkripsi terdiri dari dua tahap dekripsi. Tahap pertama dekripsi dilakukan dengan persamaan dekripsi *Affine Cipher*.

1. Matriks citra warna *cipher-image* hasil proses enkripsi dibagi menjadi tiga matriks *grayscale* sesuai dengan jenis komponennya.
2. Dengan menggunakan inisialisasi nilai yang sama pada proses enkripsi lakukan pembangkitan kunci menggunakan persamaan *Logistic Map* sehingga diperoleh kunci *B.*
3. Mencari nilai *invers* dari kunci *m* dengan menggunakan kekongruenan sehingga diperoleh kunci *invers m* yang relatif prima dengan 256.
4. Lakukan proses dekripsi menggunakan persamaan dekripsi *Affine Cipher* beserta kuncinya pada ketiga matrik. Sehingga diperoleh matriks baru yang berbeda.

Selanjutnya ketiga matriks baru hasil dekripsi akan dilakukan proses dekripsi tahap kedua dengan algoritma *Arnold's Cat Map.*

1. Dengan nilai kunci yang sama pada proses enkripsi yaitu c dan d serta banyak iterasi yang telah ditentukan sebelumnya.
2. Substitusikan nilai kunci (*c*,*d*) yang kedalam persamaan matriks [*A*] dan inverskan matriks [*A*].

$$[A] = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}$$

$$[A]^{-1} = \frac{1}{\big(1.(cd+1)\big) - cd} \begin{bmatrix} cd+1 & -p \\ -d & 1 \end{bmatrix}$$

3. Melakukan operasi perkalian matriks pada setiap entri matriks *cipher-image* dengan matriks transformasi *invers*[*A*]. kemudian hasil perkalian akan dimodulokon dengan nilai 256. Lakukan operasi pada ketiga matriks *cipher-image.*
4. Selanjutnya diperoleh matriks hasil operasi persamaan dekripsi *Arnold's Cat Map.*
5. Proses dekripsi akan menghasil tiga matriks *plain-image* yang berbeda, kemudian disatukan kembali menjadi matriks citra *plain-image* berwarna.

3.3.3 Evaluasi

Tahap evaluasi yaitu tahap pengukuran kualitas citra dengan pengukuran secara objektif (tanpa keterlibatan manusia). Tahap ini dilakukan dengan menggunakan dua persamaan pengukuran yaitu persamaan *Mean Square Error* kemudian dengan menggunakan nilai hasil dari *Mean Square Error* akan dihitung nilai *Peak Signal-to-Noise Ratio.* Pada tahap tersebut akan dilakukan perhitungan dengan menggunakan matriks *plain-image* dan *cipher-image*. Nilai yang diperoleh akan menunjukan apakah citra setelah proses enkripsi mendekati citra sebelum proses enkripsi.

BAB IV
HASIL DAN PEMBAHASAN

4.1 Proses Enkripsi Citra Digital

4.1.1 Proses Enkripsi Menggunakan Algoritma *Arnold's Cat Map*

Berikut diberikan contoh hasil pemrosesan enkripsi citra digital dengan menggunakan algoritma *Arnold's Cat Map* pada citra digital berordo 4×4 piksel dengan jenis citra *grayscale.*

Gambar 4.1 *Plain-Image* dengan Jenis Citra *Grayscale*

Dari gambar citra digital di atas kita peroleh matriks *plain-image* dengan ordo 4×4 sebagai berikut.

$$P = \begin{bmatrix} 84 & 169 & 47 & 157 \\ 191 & 56 & 197 & 32 \\ 51 & 244 & 190 & 132 \\ 95 & 146 & 132 & 127 \end{bmatrix}$$

Selanjutnya matriks *plain-image* akan dioperasikan menggunakan algoritma *Arnold's Cat Map*.

1. Tentukan nilai kunci $c = 2,\ d = 3$ dan $M = 4$ (sesuai dengan ordo matriks transformasinya) serta iterasi = 1 (rahasia).

$$P = \begin{bmatrix} 84 & 169 & 47 & 157 \\ 191 & 56 & 197 & 32 \\ 51 & 244 & 190 & 132 \\ 95 & 146 & 132 & 127 \end{bmatrix}$$

Masukan nilai kunci tersebut kedalam persamaan enkripsi *Arnold's Cat Map* berikut.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}(M)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \mathrm{mod}(M)$$

Keterangan :

x' : Posisi baru pixel di baris x.

y' : Posisi baru pixel di kolom y.

x : Posisi mula-mula pixel di baris x.

y : Posisi mula-mula pixel di kolom y.

2. Kemudian transformasikan matriks P menggunakan persamaan enkripsi *Arnold's Cat Map* kepada matriks baru yang disimbolkan dengan I.

Jika $p_{(x,y)} \in P$ dan $i_{(x',y')} \in I$ dengan

nilai $x = 0,1,2,\dots,(M-1)$ dan $y = 0,1,2,\dots,(M-1)$

- Untuk matriks dengan baris $x = 0$ dan kolom $y = 0$

$$p_{(0,0)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \rightarrow i_{(0,0)}$$

- Untuk matriks dengan baris $x = 0$ dan kolom $y = 1$

$$p_{(0,1)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 \\ 7 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 2 \\ 3 \end{bmatrix} \rightarrow i_{(2,3)}$$

- Untuk matriks dengan baris $x = 0$ dan kolom $y = 2$

$$p_{(0,2)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 4 \\ 14 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 0 \\ 2 \end{bmatrix} \rightarrow i_{(0,2)}$$

- Untuk matriks dengan baris $x = 0$ dan kolom $y = 3$

$$p_{(0,3)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 3 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 6 \\ 21 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 2 \\ 1 \end{bmatrix} \rightarrow i_{(2,1)}$$

- Untuk matriks dengan baris $x = 1$ dan kolom $y = 0$

$$p_{(1,0)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \mathrm{mod}(4)$$

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

$$= \begin{bmatrix} 1 \\ 3 \end{bmatrix} \rightarrow i_{(1,3)}$$

- Untuk matriks dengan baris $x = 1$ dan kolom $y = 1$

$$p_{(1,1)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 3 \\ 10 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 3 \\ 2 \end{bmatrix} \rightarrow i_{(3,2)}$$

- Untuk matriks dengan baris $x = 1$ dan kolom $y = 2$

$$p_{(1,2)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 5 \\ 17 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 1 \\ 1 \end{bmatrix} \rightarrow i_{(1,1)}$$

- Untuk matriks dengan baris $x = 1$ dan kolom $y = 3$

$$p_{(1,3)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 7 \\ 24 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 3 \\ 0 \end{bmatrix} \rightarrow i_{(3,0)}$$

- Untuk matriks dengan baris $x = 2$ dan kolom $y = 0$

$$p_{(2,0)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 \\ 6 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 2 \\ 2 \end{bmatrix} \rightarrow i_{(2,2)}$$

- Untuk matriks dengan baris $x = 2$ dan kolom $y = 1$

$$p_{(2,1)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} \mathrm{mod}(4)$$

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

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow i_{(0,1)}$$

- Untuk matriks dengan baris $x = 2$ dan kolom $y = 2$

$$p_{(2,2)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} \mathrm{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 6 \\ 20 \end{bmatrix} \text{mod}(4)$$

$$= \begin{bmatrix} 2 \\ 0 \end{bmatrix} \rightarrow i_{(2,0)}$$

- Untuk matriks dengan baris $x = 2$ dan kolom $y = 3$

$$p_{(2,3)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} \text{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 8 \\ 27 \end{bmatrix} \text{mod}(4)$$

$$= \begin{bmatrix} 0 \\ 3 \end{bmatrix} \rightarrow i_{(0,3)}$$

- Untuk matriks dengan baris $x = 3$ dan kolom $y = 0$

$$p_{(3,0)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} \text{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 3 \\ 9 \end{bmatrix} \text{mod}(4)$$

$$= \begin{bmatrix} 3 \\ 1 \end{bmatrix} \rightarrow i_{(3,1)}$$

- Untuk matriks dengan baris $x = 3$ dan kolom $y = 1$

$$p_{(3,1)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} \text{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 5 \\ 16 \end{bmatrix} \text{mod}(4)$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow i_{(1,0)}$$

- Untuk matriks dengan baris $x = 3$ dan kolom $y = 2$

$$p_{(3,2)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \text{mod}(4)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 7 \\ 23 \end{bmatrix} mod(4)$$

$$= \begin{bmatrix} 3 \\ 3 \end{bmatrix} \rightarrow i_{(3,3)}$$

- Untuk matriks dengan baris $x = 3$ dan kolom $y = 3$

$$p_{(3,3)} \rightarrow \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 3 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix} \bmod(4)$$

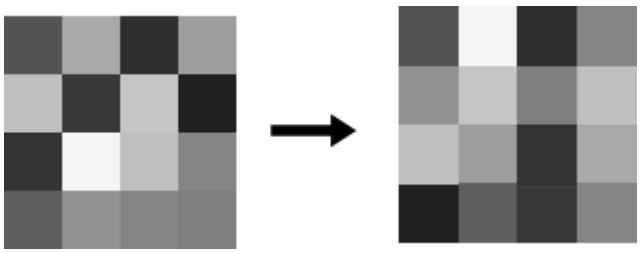
$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 9 \\ 30 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 1 \\ 2 \end{bmatrix} \rightarrow i_{(1,2)}$$

Dari hasil transforamsi menggunakan persamaan enkripsi *Arnold's Cat Map* diperoleh matriks I sebagai berikut.

$$I = \begin{bmatrix} 84 & 244 & 47 & 132 \\ 146 & 197 & 127 & 191 \\ 190 & 157 & 51 & 169 \\ 32 & 95 & 56 & 132 \end{bmatrix}$$

3. Berikut hasil enkripsi pada citra digital.



Gambar 4.2 Hasil Enkripsi Citra dengan Algoritma *ACM*

4.1.2 Proses Enkripsi dengan Menggunakan Algoritma *Affine Cipher*

Matriks (*I*) hasil enkrpsi menggunakan algoritma *Arnold's Cat Map* akan dienkripsi kembali dengan menggunakan persamaan enkripsi *Affine Cipher*.

1. Sebelum melakukan operasi enkripsi dengan persamaan enkripsi *Affine Cipher* akan dilakukan pembangkitan kunci dengan menggunakan persamaan *Logistic Map.*
2. Tentukan nilai kunci $r = 3.95,\ x = 0.5$ dan $n =$ jumlah ordo matriks yaitu 16 karena matriks 4×4.
3. Dengan persamaan *Logistic Map* berikut.

$$x_{n+1} = rx_n(1 - x_n)$$

4. Substitusikan kunci dan nilai inisialisasi ke dalam persamaan, sehingga diperoleh.

- $x_{(0,0)} = 3.95 \times 0.5\ (1 - 0.5)$

  $x_{(0,0)} = 0.9875$

- $x_{(0,1)} = 3.95 \times 0.9875\ (1 - 0.9875)$

  $x_{(0,1)} = 0.04875781249999983$

- $x_{(0,2)} = 3.95 \times 0.04875781249999983\ (1 - 0.04875781249999983)$

  $x_{(0,2)} = 0.183202928469848$

- $x_{(0,3)} = 3.95 \times 0.183202928469848\ (1 - 0.183202928469848)$

  $x_{(0,3)} = 0.591076481106183$

- $x_{(1,0)} = 3.95 \times 0.591076481106183\ (1 - 0.591076481106183)$

  $x_{(1,0)} = 0.9547350446277946$

- $x_{(1,1)} = 3.95 \times 0.9547350446277946\ (1 - 0.9547350446277946)$

  $x_{(1,1)} = 0.17070335479006285$

- $x_{(1,2)} = 3.95 \times 0.17070335479006285\ (1 - 0.17070335479006285)$

  $x_{(1,2)} = 0.5591766918412491$

- $x_{(1,3)} = 3.95 \times 0.5591766918412491\ (1 - 0.5591766918412491)$

  $x_{(1,3)} = 0.9736675706137671$

- $x_{(2,0)} = 3.95 \times 0.9736675706137671\ (1 - 0.9736675706137671)$

  $x_{(2,0)} = 0.10127417856796533$

- $x_{(2,1)} = 3.95 \times 0.10127417856796533\ (1 - 0.10127417856796533)$

  $x_{(2,1)} = 0.35951999132722934$

- $x_{(2,2)} = 3.95 \times 0.35951999132722934\ (1 - 0.35951999132722934)$

  $x_{(2,2)} = 0.9095482002950283$

- $x_{(2,3)} = 3.95 \times 0.9095482002950283\ (1 - 0.9095482002950283)$

  $x_{(2,3)} = 0.3249675729586585$

- $x_{(3,0)} = 3.95 \times 0.3249675729586585\ (1 - 0.3249675729586585)$

  $x_{(3,0)} = 0.8664864154618691$

- $x_{(3,1)} = 3.95 \times 0.8664864154618691\ (1 - 0.8664864154618691)$

  $x_{(3,1)} = 0.4569664437635456$

- $x_{(3,2)} = 3.95 \times 0.4569664437635456\ (1 - 0.4569664437635456)$

  $x_{(3,2)} = 0.9801850464986934$

- $x_{(3,3)} = 3.95 \times 0.9801850464986934\ (1 - 0.9801850464986934)$

  $x_{(3,3)} = 0.07671816842023815$

Karena didalam matriks citra rentang nilai dari 1 sampai 255 maka nilai yang telah diperoleh dikali 255 dan dilakukan pembulatan bilangan decimal menjadi bilangan bulat terdekat.

- $x_{(0,0)} = 0.9875 \times 255 = 251{,}8125 = 252$
- $x_{(0,1)} = 0.04875781249999983 \times 255 = 12.43324219 = 12$
- $x_{(0,2)} = 0.183202928469848 \times 255 = 46.71674676 = 47$
- $x_{(0,3)} = 0.591076481106183 \times 255 = 150.72450268 = 151$

- $x_{(1,0)} = 0.9547350446277946 \times 255 = 243.45743638 = 243$
- $x_{(1,1)} = 0.17070335479006285 \times 255 = 43.52935547 = 44$
- $x_{(1,2)} = 0.5591766918412491 \times 255 = 142.59005642 = 143$
- $x_{(1,3)} = 0.9736675706137671 \times 255 = 248.28523051 = 248$
- $x_{(2,0)} = 0.10127417856796533 \times 255 = 25.82491553 = 26$
- $x_{(2,1)} = 0.35951999132722934 \times 255 = 91.67759779 = 92$
- $x_{(2,2)} = 0.9095482002950283 \times 255 = 231.93479108 = 232$
- $x_{(2,3)} = 0.3249675729586585 \times 255 = 82.8667311 = 83$
- $x_{(3,0)} = 0.8664864154618691 \times 255 = 220.95403594 = 221$
- $x_{(3,1)} = 0.4569664437635456 \times 255 = 116.52644316 = 117$
- $x_{(3,2)} = 0.9801850464986934 \times 255 = 249.94718686 = 250$
- $x_{(3,3)} = 0.07671816842023815 \times 255 = 19.56313295 = 20$

Dari pembangkitan kunci diperoleh matriks kunci *B* sebagai berikut.

$$B = \begin{bmatrix} 252 & 12 & 47 & 151 \\ 243 & 44 & 143 & 248 \\ 26 & 92 & 232 & 83 \\ 221 & 117 & 250 & 20 \end{bmatrix}$$

5. Tentukan nilai m yang relatif prima terhadap 256, $m = 137$. Untuk mengetahui apakah m relatif prima terhadap 256 dapat dibuktikan dengan $PBB(137{,}256) = 1$.
6. Lakukan proses enkripsi dengan persamaan enkripsi *Affine Cipher*.

$$C = (mP + B) \bmod(256)$$

- $C_{(0,0)} = (137 \times 84 + 252) \bmod(256) = 240$
- $C_{(0,1)} = (137 \times 244 + 12) \bmod(256) = 160$

- $C_{(0,2)} = (137 \times 47 + 47) \mathrm{mod}(256) = 86$
- $C_{(0,3)} = (137 \times 132 + 151) \mathrm{mod}(256) = 59$
- $C_{(1,0)} = (137 \times 146 + 243) \mathrm{mod}(256) = 21$
- $C_{(1,1)} = (137 \times 197 + 44) \mathrm{mod}(256) = 153$
- $C_{(1,2)} = (137 \times 127 + 143) \mathrm{mod}(256) = 134$
- $C_{(1,3)} = (137 \times 191 + 248) \mathrm{mod}(256) = 47$
- $C_{(2,0)} = (137 \times 190 + 26) \mathrm{mod}(256) = 200$
- $C_{(2,1)} = (137 \times 157 + 92) \mathrm{mod}(256) = 97$
- $C_{(2,2)} = (137 \times 51 + 232) \mathrm{mod}(256) = 51$
- $C_{(2,3)} = (137 \times 169 + 83) \mathrm{mod}(256) = 196$
- $C_{(3,0)} = (137 \times 32 + 221) \mathrm{mod}(256) = 253$
- $C_{(3,1)} = (137 \times 95 + 117) \mathrm{mod}(256) = 76$
- $C_{(3,2)} = (137 \times 56 + 250) \mathrm{mod}(256) = 242$
- $C_{(3,3)} = (137 \times 132 + 20) \mathrm{mod}(256) = 184$

Dari enkripsi dengan persamaan *Affine Cipher* diperoleh matriks *cipher-image.*

$$C = \begin{bmatrix} 240 & 160 & 86 & 59 \\ 21 & 153 & 134 & 47 \\ 200 & 97 & 51 & 196 \\ 253 & 76 & 242 & 184 \end{bmatrix}$$

7. Berikut gambar hasil enkripsi melalui dua tahapan.

Gambar 4.3 Citra Hasil Enkripsi Algoritma ACM dan *Affine Cipher*

4.2 Proses Dekripsi Citra Digital

4.2.1 Proses Dekripsi dengan Algoritma *Affine Cipher*

Citra digital yang telah di enkripsi dan dikirim kepada penerima selanjutnya penerima akan melakukan proses dekripsi. Proses dekripsi akan dilakukan pada matriks *cipher-image*.

$$C = \begin{bmatrix} 240 & 160 & 86 & 59 \\ 21 & 153 & 134 & 47 \\ 200 & 97 & 51 & 196 \\ 253 & 76 & 242 & 184 \end{bmatrix}$$

Tahap dekripsi diawali dengan mendekripsikan matriks *cipher-image* dengan persamaan invers dari *Affine Cipher*.

1. Sama halnya dengan proses enkripsi sebelum melakukan dekripsi akan dilakukan proses pembangkitan kunci dengan persamaan *Logistic Map* sehingga diperoleh matriks kunci *B*.

$$B = \begin{bmatrix} 252 & 12 & 47 & 151 \\ 243 & 44 & 143 & 248 \\ 26 & 92 & 232 & 83 \\ 221 & 117 & 250 & 20 \end{bmatrix}$$

2. Menentukan nilai $m^{-1}, m = 137$ dengan kekongruenan linear

$$137^{-1}\text{mod}(256)$$

Dapat dihitung dengan memecahkan kekongruenan linear

$$137x \equiv 1(\text{mod}256)$$

Diperoleh $x \equiv 185(\text{mod}256)$ karena

$$137 \times 185 = 25345 \equiv 1(\text{mod}256)$$

jadi, nilai $m^{-1} = 185$.

3. Substitusikan kunci kedalam persamaan dekripsi *Affine Cipher*.

$$I = m^{-1}(C - B)\ \text{mod}(256)$$

- $I_{(0,0)} = 185 \times (240 - 252) \mathrm{mod}(256) = 84$
- $I_{(0,1)} = 185 \times (160 - 12) \mathrm{mod}(256) = 244$
- $I_{(0,2)} = 185 \times (86 - 47) \mathrm{mod}(256) = 47$
- $I_{(0,3)} = 185 \times (59 - 151) \mathrm{mod}(256) = 132$
- $I_{(1,0)} = 185 \times (21 - 243) \mathrm{mod}(256) = 146$
- $I_{(1,1)} = 185 \times (153 - 44) \mathrm{mod}(256) = 197$
- $I_{(1,2)} = 185 \times (134 - 143) \mathrm{mod}(256) = 127$
- $I_{(1,3)} = 185 \times (47 - 248) \mathrm{mod}(256) = 191$
- $I_{(2,0)} = 185 \times (200 - 26) \mathrm{mod}(256) = 190$
- $I_{(2,1)} = 185 \times (97 - 92) \mathrm{mod}(256) = 157$
- $I_{(2,2)} = 185 \times (51 - 232) \mathrm{mod}(256) = 51$
- $I_{(2,3)} = 185 \times (196 - 83) \mathrm{mod}(256) = 169$
- $I_{(3,0)} = 185 \times (253 - 221) \mathrm{mod}(256) = 32$
- $I_{(3,1)} = 185 \times (76 - 117) \mathrm{mod}(256) = 95$
- $I_{(3,2)} = 185 \times (242 - 250) \mathrm{mod}(256) = 56$
- $I_{(3,3)} = 185 \times (184 - 20) \mathrm{mod}(256) = 132$

4. Dari persamaan dekripsi *Affine Cipher* diperoleh matriks *I*.

$$I = \begin{bmatrix} 84 & 244 & 47 & 132 \\ 146 & 197 & 127 & 191 \\ 190 & 157 & 51 & 169 \\ 32 & 95 & 56 & 132 \end{bmatrix}$$

4.2.2 Proses Dekripsi dengan Algoritma *Arnold's Cat Map*

Setelah diperoleh matriks *I*, selanjutnya matriks akan didekripsi dengan menggunakan persamaan dekripsi *Arnold's Cat Map.*

1. Dengan nilai kunci yang sama seperti proses enkripsi yaitu kunci $c = 2$, $d = 3$ dan $M = 4$ serta iterasi = 1. Masukan kunci tersebut kedalam persamaan dekripsi *Arnold's Cat Map* berikut.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & c \\ d & cd+1 \end{bmatrix}^{-1} \begin{bmatrix} x \\ y \end{bmatrix} \bmod(M)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \frac{1}{\big(1.(cd+1)\big) - cd} \begin{bmatrix} cd+1 & -c \\ -d & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod(M)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \frac{1}{\big(1.(7)\big) - 6} \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod(M)$$

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod(M)$$

Keterangan :

x' : Posisi baru pixel di baris x.

y' : Posisi baru pixel di kolom y.

x : Posisi mula-mula pixel di baris x.

y : Posisi mula-mula pixel di kolom y.

2. Kemudian transformasikan matriks *I* menggunakan persamaan enkripsi *Arnold's Cat Map* kepada matriks plaintext yang disimbolkan dengan *P*. Jika $i_{(x\prime,y\prime)} \in I$ dan $p_{(x,y)} \in P$ dengan nilai $x = 0,1,2,\dots,(M-1)$ dan $y = 0,1,2,\dots,(M-1)$

- Untuk matriks dengan baris $x' = 0$ dan kolom $y' = 0$

$$i_{(0,0)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 0 \\ 0 \end{bmatrix} \rightarrow p_{(0,0)}$$

- Untuk matriks dengan baris $x' = 0$ dan kolom $y' = 1$

$$i_{(0,1)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} -2 \\ 1 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 2 \\ 1 \end{bmatrix} \rightarrow p_{(2,1)}$$

- Untuk matriks dengan baris $x' = 0$ dan kolom $y' = 2$

$$i_{(0,2)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} -4 \\ 2 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 0 \\ 2 \end{bmatrix} \rightarrow p_{(0,2)}$$

- Untuk matriks dengan baris $x' = 0$ dan kolom $y' = 3$

$$i_{(0,3)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 3 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} -6 \\ 3 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 2 \\ 3 \end{bmatrix} \rightarrow p_{(2,3)}$$

- Untuk matriks dengan baris $x' = 1$ dan kolom $y' = 0$

$$i_{(1,0)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 7 \\ -3 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 3 \\ 1 \end{bmatrix} \rightarrow p_{(3,1)}$$

- Untuk matriks dengan baris $x' = 1$ dan kolom $y' = 1$

$$i_{(1,1)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 5 \\ -2 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 1 \\ 2 \end{bmatrix} \rightarrow p_{(1,2)}$$

- Untuk matriks dengan baris $x' = 1$ dan kolom $y' = 2$

$$i_{(1,2)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 3 \\ -1 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 3 \\ 3 \end{bmatrix} \rightarrow p_{(3,3)}$$

- Untuk matriks dengan baris $x' = 1$ dan kolom $y' = 3$

$$i_{(1,3)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow p_{(1,0)}$$

- Untuk matriks dengan baris $x' = 2$ dan kolom $y' = 0$

$$i_{(2,0)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 14 \\ -6 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 2 \\ 2 \end{bmatrix} \rightarrow p_{(2,2)}$$

- Untuk matriks dengan baris $x' = 2$ dan kolom $y' = 1$

$$i_{(2,1)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 1 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 12 \\ -5 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 0 \\ 3 \end{bmatrix} \rightarrow p_{(0,3)}$$

- Untuk matriks dengan baris $x' = 2$ dan kolom $y' = 2$

$$I_{(2,2)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 2 \end{bmatrix} \mathrm{mod}(4)$$

$$= \begin{bmatrix} 10 \\ -4 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 2 \\ 0 \end{bmatrix} \rightarrow p_{(2,0)}$$

- Untuk matriks dengan baris $x' = 2$ dan kolom $y' = 3$

$$i_{(2,3)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 2 \\ 3 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 8 \\ -3 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow p_{(0,1)}$$

- Untuk matriks dengan baris $x' = 3$ dan kolom $y' = 0$

$$i_{(3,0)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 21 \\ -9 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 1 \\ 3 \end{bmatrix} \rightarrow p_{(1,3)}$$

- Untuk matriks dengan baris $x' = 3$ dan kolom $y' = 1$

$$i_{(3,1)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 19 \\ -8 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 3 \\ 0 \end{bmatrix} \rightarrow p_{(3,0)}$$

- Untuk matriks dengan baris $x' = 3$ dan kolom $y' = 2$

$$i_{(3,2)} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 17 \\ -7 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 1 \\ 1 \end{bmatrix} \rightarrow p_{(1,1)}$$

- Untuk matriks dengan baris $x' = 3$ dan kolom $y' = 3$

$$i_{(3,3)} = 132 \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & -2 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 3 \end{bmatrix} \bmod(4)$$

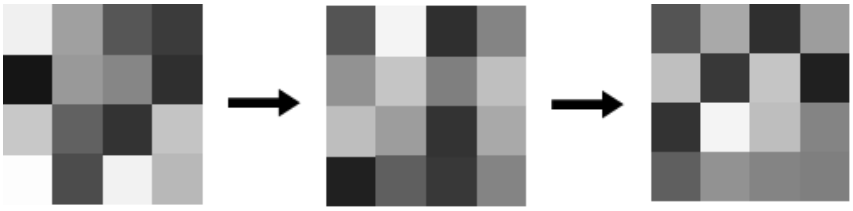
$$= \begin{bmatrix} 15 \\ -6 \end{bmatrix} \bmod(4)$$

$$= \begin{bmatrix} 3 \\ 2 \end{bmatrix} \rightarrow p_{(3,2)}$$

3. Dari hasil transforamsi menggunakan persamaan dekripsi *Arnold's Cat Map* diperoleh matriks *Plain-image* sebagai berikut.

$$P = \begin{bmatrix} 84 & 169 & 47 & 157 \\ 191 & 56 & 197 & 32 \\ 51 & 244 & 190 & 132 \\ 95 & 146 & 132 & 127 \end{bmatrix}$$

4. Berikut gambar hasil dekripsi kedua algoritma



Gambar 4.4 Citra Hasil Dekripsi dengan *Affine Cipher* dan ACM

4.3 Pembahasan Hasil Enkripsi dan Dekripsi

Pada subbab ini, akan dibahas tentang hasil pengujian terhadap proses enkripsi dan dekripsi yang sebelumnya telah dilakukan dengan meggunakan program aplikasi *text editor* yaitu *visual studio code* dengan bahasa pemrograman *python.* Proses pengujian dengan memasukan citra digital dan kunci pada algoritma yang telah dipersiapkan pada aplikasi *text-editor* kemudian setelah beberapa saat citra hasil enkripsi dan dekripsi akan diperoleh. Selama proses berjalan akan dihitung dalam satuan detik berapa lama waktu yang dibutuhkan untuk menyelesaikan proses tersebut.

Pengujian dilakukan terhadap enam citra digital berbeda yang dibagi tiga citra dengan ekstensi bitmap (.bmp) dan tiga citra dengan ekstensi *Portabel Network Graphic* (.png). Pengujian tersebut menggunakan algoritma *Arnold's Cat Map* dan *Affine Cipher* serta pembangkitan kunci dengan *Logistic Map* pada *Affine Cipher*.

Tabel 4.1 Tabel Hasil Pengujian Waktu pada Proses Enkripsi dan Dekripsi

No	Nama Percobaan	Iterasi		Waktu (detik) Enkripsi		Waktu (detik) Dekripsi	
		ACM	*Affine Cipher*	Dengan Pembangkit Kunci	Kunci tunggal (7)	Dengan Pembangkit Kunci	Kunci tunggal (7)
1	Pe1PNG_1	1	1	59.76	49.39	67.30	67.03
2	Pe2PNG_1	1	1	56.12	50.59	68.72	65.00
3	Pe3PNG_1	1	1	56.59	50.26	68.48	64.47
4	Pe1BMP_1	1	1	55.12	49.59	68.34	64.14
5	Pe2BMP_1	1	1	57.65	56.05	69.94	68.67
6	Pe3BMP_1	1	1	69.58	50.13	70.58	64.91
7	Pe1PNG_2	2	2	133.19	114.29	136.25	133.09
8	Pe2PNG_2	2	2	115.98	111.20	139.37	130.74
9	Pe3PNG_2	2	2	122.98	103.51	139.20	132.31
10	Pe1BMP_2	2	2	120.34	108.61	146.43	128.80
11	Pe2BMP_2	2	2	137.18	111.34	137.41	130.61
12	Pe3BMP_2	2	2	145.12	142.51	137.06	129.91

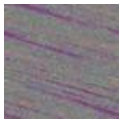
Berdasarkan tabel di atas didapatkan waktu lamanya proses enkripsi dan dekrispi citra digital, Waktu yang terlihat saat citra digital di enkripsi menggunakan algoritma *Arnold's Cat Map* dan *Affine Cipher* dengan kunci yang dibangkitkan dengan menggunakan *Logistic Map* pada *Affine Cipher* dan tanpa pembangkitkan melainkan kunci nilai tunggal yaitu 7, memiliki perbedaan waktu. Waktu proses dengan menggunakan pembangkitan kunci lebih lama dibandingkan tanpa pembangkitan kunci. Contohnya dapat dilihat pada percobaan pada baris pertama waktu yang dibutuhkan yaitu diangka 59.76 detik, sedangkan tanpa menggunakan

pembangkitan kunci waktu yang dibutuhkan 49.39 detik. Begitu juga pada proses dekripsi yang dapat dilihat pada baris pertama 67.30 berbanding 67.03.

Selain itu pada pengujian waktu nilai iterasi mempengaruhi berapa lama proses enkripsi berlangsung. Pada baris ketujuh telihat waktu yang dibutuhnya dengan nilai iterasi 2 adalah 133.19 dan114.29. Waktu proses dua kali lebih lama daripada dengan iterasi 1.

Selanjutnya merupakan pengujian yang dilakukan adalah menghitung nilai *Mean Square Error* (MSE) dan *Peak Signal-to-Noise Ratio* (PSNR) untuk mengukur tingkat kesamaan dan *noise* citra antara citra sebelum dilakukan proses enkripsi dengan citra yang telah melalui proses enkripsi.

Tabel 4.2 Tabel Hasil Perhitungan Nilai MSE dan PSNR dari Proses Enkripsi dengan Iterasi 1

No.	*Plain-Image*	*Cipher-Image*		Dengan Pembangkit kunci		Kunci tunggal (7)	
		Dengan Pembangkit kunci	Kunci tunggal (7)	MSE	PSNR	MSE	PSNR
1				105,5301	27,8970	105,2889	27,9069
2				105,4090	27,9020	105,3743	27,9034
3				104,9651	27,9203	105,2833	27,9072
4				106,026	27,8766	105,8430	27,8841
5				105,2740	27,9075	104,9708	27,9201

6				105,1194	27,9139	105,1522	27,9126

Nilai *Mean Square Error* (MSE) yang diperoleh dapat menjadi tolak ukur dari tingkat similaritas citra digital mula-mula sebelum dengan citra digital setelah proses enkripsi dilakukan. Pada penentuan similaritas dengan menggunakan MSE nilai yang diperoleh mendekati nilai 1 akan menunjukan kedua citra sama persis. Sehingga apabila nilai MSE yang diperoleh semakin tinggi maka kedua citra semakin tidak serupa. Selanjutnya dari nilai MSE yang diperoleh dapat dilanjutkan menemukan nilai *Peak Signal-to-Noise Rati* (PSNR). Nilai PSNR menunjukan seberapa besar kualitas sebuah citra terhadap citra sebelumnya dengan menghitung tingkat *noise*-nya. Apabila nilai yang diperoleh di bawah 30 db maka citra tersebut semakin buruk dalam kata lain citra memiliki *noise* yang tinggi.

Pada tabel di atas, dapat dilihat hasil pengujian dengan total 6 citra dengan masing-masing 2 kali percobaan, dengan iterasi maksimum 1. Rata-rata nilai MSE dan PSNR yang diperoleh terletak disekitar 105,2 dan 27,9. Hal ini menunjukan citra hasil enkripsi tidak serupa dengan citra digital awal (*Plain-Image*).

Tabel 4.3 Tabel Hasil Perhitungan Nilai MSE dan PSNR dari Proses Dekripsi dengan Iterasi 1

No.	*Plain-Image*	Cipher-image		Hasil Dekripsi		Nilai MSE	
		Dengan Pembangkit kunci	Kunci tunggal (7)	Dengan Pembangkit kunci	Kunci tunggal (7)	Dengan Pembangkit kunci	Kunci tunggal (7)
1						0	0
2						0	0

3						0	0
4						0	0
5						0	0
6						0	0

Pada tabel 4.3, citra hasil dekripsi nilai rata -rata *Mean Square Error* yang dimiliki citra hasil dekripsi adalah nol. Hal tersebut menunjukan bahwa citra hasil dekripsi memiliki tingkat kemiripan yang tinggi terhadap citra mula-mula (*Plain-Image*).

4.4 Integrasi Keagamaan

Dunia modern saat ini dimana teknologi terus berkembang sehingga berbagai kemudahan dapat dirasakan dari berbagai aspek salah satu berkomunikasi. Selain aspek positif, perkembangan teknologi tentu juga memiliki aspek negatif yaitu munculnya kejahatan *cyber* seperti *hacking, scamming,* dan sebagainya. Oleh karena itu, pengamanan data dan pesan dibutuhkan. Enkripsi atau penyandian data dan pesan merupakan bagaian dari pengamanan data yang bertujuan untuk melindungi data dan pesan dari serangan kejahatan *cyber* seperti *hacking* (Pencurian data virtual) saat berkomunikasi. Dalam ajaran islam kita diajarkan untuk selalu menjaga Amanah dan aib kita. Selaras dengan itu kriptografi dalam hal ini proses enkripsi dan dekripsi berperan untuk menjaga keamanan data pribadi kita

ketika berkomunikasi serta membatasi privasi kita dari orang yang tidak bertanggung jawab.

BAB V
PENUTUP

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil berdasarkan pembahasan hasil penelitian implementasi metode *super encryption* (*Arnold's Cat Map* dan *Affine Cipher*) serta pembangkitan kunci pada *Affine Cipher* dengan menggunakan persamaan *Logistic Map*, sebagai berikut.

1. Pada proses enkripsi menggunakan algoritma *Arnold's Cat Map* dan algoritma *Affine Cipher* serta menggunakan kunci yang dibangkitkan melalui persamaan *Logistic Map* yang digunakan pada persamaan *Affine Cipher*. Proses enkripsi dapat disimpulkan bahwa citra digital awal (*Plain-image*) di awali dengan membagi citra tersebut kedalam 3 matriks berskala abu-abu (*Grayscale*) kemudian setiap matriks dilakukan operasi dengan menggunakan persamaan *Arnold's Cat Map* sehingga ketiga matriks akan teracak atau nilai elemen matriks berpindah posisi (tranposisi), selanjutnya ketiga matriks akan dilakukan operasi dengan menggunakan persamaan *Affine Cipher*. Namun sebelumnya, akan dilakukan pembangkitan kunci dengan menggunakan persamaan *Logistic Map*. Setelah operasi menggunakan persamaan *Affine Cipher*, ketiga matriks berskala abu-abu tersebut akan disatukan dan akan menghasilkan *Cipher-Image* yang mana citra tersebut memiliki tingkat kesamaan yang kecil.
2. Pada proses Dekripsi, tidak jauh berbeda dengan proses enkripsi. Perbedaanya terletak pada proses dimulai dari pembangkitan kunci dengan nilai yang sama pada pembangkitan kunci proses enkripsi. Kemudian

dilanjutkan dengan melakukan operasi persamaan *Affine Cipher* kepada tiga matriks citra yang sudah dipisah sebelumnya kedalam matriks berskala abu-abu. Tiga matriks hasil operasi *Affine Cipher* tersebut akan dilanjukan kedalam proses dekripsi dengan persamaan *Arnold's Cat Map* sehingga menghasilkan tiga matriks baru. Ketiga matriks baru tersebut kemudian disatukan dan akan menghasilkan pesan citra awal (*Plain-Image*).

5.2 Saran

Melihat hasil yang telah diperoleh pada penelitian ini, terdapat saran yaitu melakukan pengembangan pada penelitian selanjutnya terkait bagaimana mendapatkan hasil enkripsi dengan menggunakan nilai iterasi dan kunci yang lebih besar, serta dapat dilakukan denga uji coba menggunakan data citra digital yang lebih beragam. Selain itu, dapat dikembangkan terkait penelitian yang dapat menerapkan sistem yang telah dibuat pada system pengamanan berbagai media komunikasi.

DAFTAR PUSTAKA

Andono, P. N., Sutojo, T., & Muljono. (2017). *Pengolahan Citra Digital.* Yogyakarta: Penerbit ANDI.

Arianty, R., & Susetianingtias, D. T. (2020). Kombinasi Logistic Map dan Pseudo-random Number Generator pada Pembangkitan Kunci untuk Enkripsi Citra Digital. *Jurnal Ilmiah Teknologi dan Rekayasa*, 187-198.

Hadits riwayat Bukhari No. 5604.

Hadits riwayat Timidzi No. 1346.

Hadits riwayat Tirmidzi No. 1955.

Hariyanto, E., & Rahhim, R. (2016). Arnold's Cat Map Algorithm in Digital Image Encryption. *International Journal of Science and Research*.

Irawan, W. H., Hijriyah, N., & Habibi, A. R. (2014). *Pengantar Teori Bilangan.* Malang: UIN-MALIKI Press.

Kementrian Agama Republik Indonesia. (2014). *Al-Qur'an dan Terjemahan.* Penerbit Sahifa.

Kraft, J. S., & Washington, L. C. (2013). *An Introduction to Number Theory with Cryptography*. Boca Raton: CRC Press.

Kromodimoeljo, S. (2010). *Teori dan Aplikasi Kriptografi.* Yogyakarta: SPK IT Consulting.

Mezaal, Y. S., & Abdulkareem, S. F. (2017). Affine Cipher Cryptanalysis Using Genetic Algorithms. *JP Journal of Algebra, Number Theory and Applications*, 785-802.

Munir, R. (2012). Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map. *Jurnal Nasional Pendidikan Teknik Informatika*.

Munir, R. (2019). *Kriptografi.* Bandung: Informatika.

Purba, R., Halim, A., & Syahputra, I. (2014). Enkripsi Citra Digital Menggunakan Arnold's Cat Map dan Nonlinear Chaotic Algorithm. *Jurnal SIFO Mikroskil*.

Rosen, K. H. (2011). *Elementary number theory and it's aplications.* Addison-wesley publishing company.

Rubinstein-Salzedo, S. (2018). *Cryptography.* California: Springer International Publishing.

Setyaningsih, E., Iswahyudi, C., & Widyastuti, N. (2011). Konsep Super Enkripsi untuk Meningkatkan Keamanan Data Citra. *Prosiding Seminar Nasional Sistem & Teknologi Informasi*.

Winarti, E. R., Kartono, Wardono, & Masrukan. (2023). *Pengantar Teori Bilangan Pembelajaran dengan Model IRA-CA (Issue Rule Application Collaborative Assessment).* Klaten: Lakeisha.

LAMPIRAN

Lampiran 1. Script Enkripsi *Arnold's Cat Map*

```
# Library modul yang dibutuhkan
import numpy as np
from PIL import Image

# ENKRIPSI TAHAP PERTAMA DENGAN ALGORITMA ARNOLD CAT MAP

# Load the image
image = Image.open("Memasukan Citra yang akan dienkripsi")

# Menentukan nilai kunci a dan b dalam persamaan Arnold Cat Map
a = 2
b = 3
# Convert the image to a numpy array
image_array = np.array(image)

# Mengambil ukuran panjang dan lebar dari matriks
row, colom = image_array.shape[:2]
M = (row, colom)

# Menentukan matriks A dari persamaan Arnold Cat Map
matrik_A = np.array([[1, a], [b, ((a*b)+1)]])

# Membuat matriks baru untuk hasil enkripsi
acm_encrypt = np.zeros(image_array.shape)

# Perform the Arnold cat map transformation
for l in range (1):
    for i in range(row):
        for j in range(colom):
            new_x, new_y = np.dot(matrik_A, [i, j]) % (M)
            acm_encrypt[new_x, new_y] = image_array[i, j]
```

Lampiran 2. Script Pembangkit Kunci dengan *Logistic Map*

```
# Generate kunci menggunakan persamaan logistic map

# parameter yang akan digunakan
r = 3.95                 # parameter di ambil antara rentan 0-4

# n menjadi jumlah iterasi berdasarkan ordo matrik
n = row * colom
x = 0.5                 # nilai inisial dengan rentang 0-1

# generate kunci dengan persamaan logistic map
key1 = np.zeros(n)
key = key1.reshape(row,colom)

for i in range(row):
  for j in range(colom):
    x = r * x * (1 - x)
    key[i][j] = round(x*256)
key = key.astype('int64')          # melakukan pembulatan bilangan
```

Lampiran 3. Script Persamaan Enkripsi *Affine Cipher*

```
# menentukan nilai pergeseran multiplikatif
a = 137     # nilai a haruslah relatif prima terhadap 256
it = 10     # banyaknya iterasi

C = np.zeros(image_array.shape)
for l in range(2):
    for i in range(row):
        for j in range(colom):
            for n in range (it):
                C[i][j] = (a * acm_encrypt[i][j] + key[i][j]) % 256


output_image = Image.fromarray(C.astype("uint8"))
output_image.save("Tempat menyimpan hasil enkripsi")
output_image.show()
```

Lampiran 4. Script Persamaan Dekripsi *Affine Cipher*

```
# DEKRIPSI TAHAP PERTAMA DENGAN ALGORITMA DEKRIPSI AFFINE CIPHER
DENGAN KUNCI LOGISTIC MAP

# Load the image
image = Image.open(r"memasukan gambar yang akan didekripsi")

# Convert the image to a numpy array
image_array = np.array(image)

# Mengambil ukuran panjang dan lebar dari matrik
row, colom = image_array.shape[:2]

# Membuat matriks baru untuk hasil enkripsi
afn_decrypt = np.zeros(image_array.shape)

# parameter yang akan digunakan
r = 3.95                  # parameter di ambil antara rentan 0-4
n = row * colom          # n menjadi jumlah iterasi berdasarkan
ukuran matrik
x = 0.5                  # nilai inisial dengan rentang 0-1

# menentukan nilai invers pergeseran multiplikatif
a_inv = 185     # nilai invers dari a diperoleh dari kekongruenan x
= 185 (mod256)
it = 10
for i in range(row):
  for j in range(colom):
    for n in range(it):
      afn_decrypt[i][j] =(a_inv*(image_array[i][j]-key[i][j])) % 256
```

Lampiran 5. Script Persamaan Dekripsi *Arnold's Cat Map*

```
# DEKRIPSI TAHAP KEDUA DENGAN ALGORITMA DEKRIPSI ARNOLD CAT MAP
# Nilai kunci a dan b dalam persamaan Enkripsi Arnold Cat Map
a = 2
b = 3
M = (row, colom)

# Menentukan matriks A dari persamaan Arnold Cat Map
matrik_A = np.array([[1, a], [b, ((a*b)+1)]])

# menginvers kan matriks A
inv_matrik_A = np.linalg.inv(matrik_A)
inv_matrik_A = inv_matrik_A.astype('int64')
```

```
decrypted_array = np.zeros(image_array.shape)
# Melalkukan Operasi transformasi inverse Arnold cat map
for i in range(row):
    for j in range(colom):
        x, y = np.dot(inv_matrik_A, [i, j]) % (row, colom)
        decrypted_array[x, y] = afn_decrypt[i, j]

output_image = Image.fromarray(decrypted_array.astype("uint8"))
output_image.save("Tempat menyimpan gambar setelah dekripsi")
output_image.show()
```

RIWAYAT HIDUP

Egi Novaldi, putra kedua dari dua bersaudara dari Bapak Effendi dan Ibu Erniwati. Lahir di Kota Bangko, Kabupaten Merangin pada 8 November 1999. Memiliki nama panggilan egik. Tempat tinggal Kampung Baru 1 No. 46 Gg. Kamis, RT 011 RW 005, Pasar Bangko, Kecamatan Bangko, Kabupaten Merangin, Jambi. Pendidikan yang pernah ditempuh yaitu TK Negeri Pertiwi Dharma Wanita Bangko. Kemudian melanjutkan sekolah di SD Negeri 88/VI Bangko V dan lulus pada tahun 2012. Menempuh pendidikan sekolah menengah pertama di SMP Negeri 01 Merangin dan lulus pada tahun 2015. Melanjutkan pendidikan di sekolah menengah atas di SMA Negeri 1 Merangin dan lulus pada tahun 2018. Tahun 2018 melanjutkan studi ke jenjang strata 1 di Universitas Islam Negeri Maulana Malik Ibrahim Malang dan mengambil program studi Matematika di Fakulatas Sains dan Teknologi. Aktif mengikuti kegiatan intra kampus HMJ Integral Matematika UIN Malang (2019). Anggota dan pengurus SeMatA (2020-2021). Kegiatan yang pernah diikuti yaitu *Steering Committee* Kompetisi Matematika Nasional (KOMET 2019-2020). Peneliti dapat dihubungi melalui *e-mail*: eggia0811@gmail.com.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

BUKTI KONSULTASI SKRIPSI

Nama : Egi Novaldi
NIM : 18610039
Fakultas / Program Studi : Sains dan Teknologi/Matematika
Judul Skripsi : Implementasi Algoritma Super Enkripsi *Arnold's Cat Map* dan *Affine Cipher* dengan Pembangkitan Kunci Menggunakan Persamaan *Logistic Map*
Pembimbing I : Muhammad Khudzaifah, M.Si.
Pembimbing II : Erna Herawati, M.Pd.

No	Tanggal	Hal	Tanda Tangan
1.	28 Februari 2023	ACC Pengajuan Topik	1.
2.	1 Maret 2023	Konsultasi Bab I, II, dan III	2.
3.	8 Maret 2023	Konsultasi Bab I, II, dan III	3.
4.	21 Maret 2023	Konsultasi Bab I, II, dan III	4.
5.	31 Maret 2023	Konsultasi Kajian Agama Bab I dan II	5.
6.	3 April 2023	Konsultasi Kajian Agama Bab I dan II	6.
7.	4 April 2023	ACC Kajian Agama Bab I dan II	7.
8.	5 April 2023	ACC Bab I, II, dan III	8.
9.	22 Juni 2023	Konsultasi Kajian Agama Bab IV	9.
10.	13 Juli 2023	Konsultasi Kajian Agama Bab IV	10.
11.	9 November 2023	Konsultasi Revisi Seminar Proposal	11.
12.	10 November 2023	Konsultasi Bab IV dan V	12.
13.	14 November 2023	Konsultasi Bab IV dan V	13.
14.	17 November 2023	Konsultasi Kajian Agama Bab IV	14.

KEMENTERIAN AGAMA RI
UNIVERSITAS ISLAM NEGERI
MAULANA MALIK IBRAHIM MALANG
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Gajayana No.50 Dinoyo Malang Telp. / Fax. (0341)558933

15.	21 November 2023	ACC Bab IV dan V	15.
16.	21 November 2023	ACC Kajian Agama Bab IV	16.
17.	19 Desember 2023	Konsultasi Revisi Seminar Hasil	17.
18.	20 Desember 2023	ACC Revisi Seminar Hasil	18.
19.	22 Desember 2023	Revisi Skripsi	19.
20.	27 Desember 2023	ACC Keseluruhan (Pembimbing I)	20.
21.	27 Desember 2023	ACC Keseluruhan (Pembimbing II)	21.

Malang, 27 Desember 2023
Mengetahui,
Ketua Program Studi Matematika

Dr. Elly Susanti, M.Sc
NIP. 19741129 200012 2 005