I. PENDAHULUAN

1.1 Latar Belakang

Informasi telah menjadi bagian terpenting dalam kehidupan manusia. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat penting bagi seluruh kalangan baik organisasi, perguruan tinggi, lembaga pemerintahan, perusahaan, sampai dengan individual (perorangan). Perkembangan teknologi informasi telah membuat penyimpanan dan transmisi citra menjadi lebih mudah dan efisien. Persoalan yang timbul dari kemudahan ini adalah terdapatnya celah keamanan bagi pihak–pihak yang tidak bertanggung jawab untuk melakukan pencurian terhadap data, baik dalam proses transmisi atau yang tersimpan pada *harddrive*.

Menurut Kerley dan Muzaki (2019), kasus pembobolan data dapat menghancurkan perusahaan. Dampak yang dirasakan seperti pengaruh pada kinerja bisnis, menurunnya reputasi perusahaan, menurunnya tingkat kepercayaan pelanggan. Dalam beberapa kasus akan berakhir dengan jatuhnya perusahaan tersebut. Meningkatnya jumlah pencurian data oleh *hacker* di seluruh penjuru dunia menjadikan kebutuhan sistem keamanan sangat penting diterapkan, sehingga keamanan data yang disimpan atau dikirimkan akan terjamin.

Beberapa tahun terakhir seringnya proses pengiriman citra digital melalui internet (Filler and Fridrich, 2010). Sehingga penting untuk mengamankan citra dari manipulasi data. Kriptografi merupakan cara pengamanan data yang telah dikenal sejak perang dunia kedua. Perlu adanya skema pengamanan data salah satunya menggunakan kombinasi Algoritma *Logistic Map* dan *Arnold Cat Map (ACM)*, dimana enkripsi dan dekripsi citra menjadi aman. Citra digital merupakan salah satu multimedia yang penting. Citra tidak hanya disimpan di dalam *storage*, tetapi juga ditransmisikan melalui publik seperti internet. Maka dari itu, sangat penting untuk diamankan.

Pada instansi-instansi sangat diperlukan pengamanan data. Salah satunya seperti di PT.Taspen yang bergerak pada bidang asuransi jiwa. Sebagian besar informasi disimpan dan dikumpulkan dikomputer dan dikirim melalui jaringan. Untuk citra yang bersifat *privat* atau yang bersifat rahasia, penyimpanan dan pengiriman citra perlu memperhatikan aspek keamanan. Jika informasi citra digital jatuh ke tangan yang salah maka akan terjadi pelanggaran digital dan bisa saja disalahgunakan. Untuk mencegah terjadinya pembobolan

data atau kebocoran data rahasia yang berupa citra maka dapat dilakukan dengan enkripsi citra digital.

Enkripsi citra digital bertujuan untuk menyandikan citra (*plainimage)* sehingga tidak dapat dikenal lagi *(cipherimage)*. Cara enkripsi sudah digunakan secara luas sebagai salah satu teknik menjaga keamanan informasi. Enkripsi merupakan salah satu teknik keamanan pesan dalam kriptografi termasuk pesan dalam bentuk citra. Salah satu layanan yang diberikan oleh kriptografi adalah kerahasiaan pesan (*confidentiality)* dan *confidentiality* diimplementasikan dengan enkripsi dan dekripsi pesan (Schneier, 1996). Terdapat dua operasi dasar di dalam algoritma enkripsi citra digital adalah permutasi dan substitusi. Permutasi mengubah posisi *pixel-pixel* di dalam citra digital, sedangkan substitusi adalah mengubah nilai *pixel*. (Younes, 2008).

Logistic Map adalah sistem *chaos* yang paling sederhana yang berbentuk persamaan iteratif. Dimana nilai awal persamaan iterasi adalah $\boldsymbol{x_0}$ yang dimana persamaan satu bersifat deterministik sebab jika dimasukkan nilai $\boldsymbol{x_0}$ yang sama maka dihasilkan barisan nilai chaotik ($\boldsymbol{x_i}$) yang sama pula. Oleh karena itu, pembangkit bilangan acak dengan sistem *chaos* disebut pseudo-random generator. Sifat algoritma *chaos* yang paling penting adalah sensitivitasnya pada perubahan kecil nilai awal (Stallings dan William, 2004).

Arnold Cat Map adalah transformasi yang mengubah posisi relatif *pixel-pixel* dalam sebuah gambar persegi menjadi posisi yang baru. Transformasi ini memilih gambar persegi dengan dua dimensi dan menghasilkan gambar persegi dengan dimensi yang sama. *Arnold Cat Map* digunakan untuk mengacak susunan *pixel* dan *Logistic Map* digunakan untuk difusi gambar. *Arnold Cat Map* memiliki beberapa sifat menarik, seperti konservasi energi dan kekacauan *(Chaotic).*

Pada penelitian sebelumnya yang dilakukan oleh Candra Irawan dan Eko Hari Rachmawanto (2022), yang berjudul "*Implementasi Kriptografi dengan Menggunakan Algoritma Arnold's Cat Map dan Henon Map".* Pada penelitian tersebut didapatkan hasil penelitian yaitu enkripsi *Arnold Cat Map* memiliki nilai korelasi yang tinggi sehingga dibandingkan dengan algoritma lain memiliki tingkat reduksi citra yang rendah. Sedangkan pengujian *ACM + Henon Map* memiliki nilai korelasi yang mendekati 0 yang artinya algoritma yag diusulkan berhasil mereduksi citra yang berdekatan.

Dengan demikian, berdasarkan objek penelitian yaitu PT.Taspen yang bergerak pada bidang ansuransi jiwa, dimana sebagian besar informasi disimpan dan dikumpulkan dikomputer dan dikirim melalui jaringan. Citra yang bersifat *privat* atau yang bersifat rahasia, penyimpanan dan pengiriman citra perlu memperhatikan aspek keamanan. Untuk mencegah terjadinya pembobolan data

atau kebocoran data rahasia yang berupa citra maka dapat dilakukan dengan enkripsi citra digital. Salah satu citra yang akan di enkripsi pada penelitian ini yaitu Kartu Taspen.

Berdasarkan uraian di atas, maka pada penelitian ini akan digunakan fungsi *chaos* yaitu *Arnold Cat Map (ACM)* dan *Logistic Map.* Dengan mengajukan judul **"Enkripsi dan Dekripsi Citra Digital Menggunakan Kombinasi Algoritma *Logistic Map* dan *Arnold Cat Map (ACM)*"**

1.2 Rumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana analisis sensitivitas kunci terhadap perubahan nilai parameter pada *chiperimage?*
2. Bagaimana tingkat keamanan *chiperimage* berdasarkan histogramnya?

1.3 Tujuan

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Melihat hasil *chiperimage* berdasarkan perubahan nilai parameter.
2. Melihat tingkat keamanan c*hiperimage* berdasarkan histogram.

1.4 Manfaat

Manfaat penelitian ini adalah sebagai berikut:

1. Bagi penulis adalah sebagai sarana dalam mengaplikasikan ilmu yang telah diperoleh khususnya dalam *enkripsi* citra digital dalam kriptografi.
2. Bagi penulis lain adalah sebagai bahan perbandingan mengenai metode kriptografi yang telah ada saat ini.
3. Bagi pembaca adalah untuk menambah pengetahuan dan wawasan tentang kriptografi terutama algoritma *Logistic Map* dan *Arnold Cat Map (ACM)* sebagai referensi untuk penelitian selanjutnya.
4. Bagi pemerintah adalah dapat dijadikan bahan pertimbangan dalam penyandian citra digital berikutnya dengan menggunakan algoritma *Logistic Map* dilanjutkan dengan algoritma *Arnold Cat Map (ACM)*

1.5 Batasan Masalah

Dalam penelitian ini adapun batasan masalah adalah sebagai berikut:

1. Data yang digunakan adalah kartu taspen berbentuk citra digital
2. Citra digital yang digunakan adalah format *PNG* (*Portabel Network Graphics*).
3. Ukuran *pixel* yang digunakan adalah 3×3 *pixel.*
4. Algoritma kriptografi yang digunakan adalah algoritma *Logistic Map* dan *Arnold Cat Map (ACM).*