Journal of Informatics and Computer Science Vol. 10 No. 1 April 2024
Universitas Ubudiyah Indonesia
e-ISSN : 2615-5346

ENKRIPSI DATA CITRA DIGITAL SIDIK JARI MENGGUNAKAN ALGORITMA KRIPTOGRAFI LUC

Muammar[1], Amsal[2]
Prodi Informatika, Fakultas Sains dan Teknologi, Universitas Ubudiyah Indonesia, Jl. Alue Naga, Tibang, Kec. Syiah Kuala Banda Aceh, Indonesia
Corresponding Author: muammar@uui.ac.id

Abstrak

Dalam era digital yang terus berkembang, keamanan data menjadi isu utama, terutama untuk data pribadi atau rahasia, seperti data sidik jari digital yang sangat sensitif dan digunakan dalam berbagai aplikasi. Keamanan data sidik jari digital semakin krusial seiring dengan perkembangan teknologi yang membawa ancaman siber yang semakin canggih. Oleh karena itu, penelitian ini bertujuan untuk menerapkan Algoritma Kriptografi LUC sebagai solusi untuk melindungi data sidik jari digital dari akses yang tidak sah. Algoritma ini telah terbukti efektif dalam berbagai aplikasi kriptografi karena menggunakan pendekatan permutasi dan substitusi untuk mengenkripsi data. Penelitian ini akan berfokus pada penerapan Algoritma Kriptografi LUC untuk mengamankan data citra digital sidik jari dalam format grayscale dan RGB. Bilangan prima akan ditentukan menggunakan metode Trial Division, dan implementasi akan dilakukan dengan bahasa pemrograman Python. Tujuan dari penelitian ini adalah untuk mengamankan citra digital sidik jari melalui proses enkripsi dan dekripsi menggunakan Algoritma Kriptografi LUC. Hasil penelitian ini diharapkan dapat memberikan wawasan tentang keamanan data sidik jari digital dan menjadi dasar untuk pengembangan sistem keamanan yang lebih baik di masa depan.

Kata kunci : Keamanan data, citra digital sidik jari, Algoritma Kriptografi LUC, enkripsi, dekripsi, metode Trial Division, grayscale, RGB, Python.

Abstract

In the rapidly evolving digital era, data security has become a paramount issue, particularly concerning personal or sensitive information, such as digital fingerprint data, which is widely used in various applications. The security of digital fingerprint data has grown increasingly crucial in light of technological advancements that bring forth sophisticated cyber threats. Therefore, this research aims to implement the LUC Cryptography Algorithm as a solution to safeguard digital fingerprint data from unauthorized access. This algorithm has demonstrated its effectiveness in various cryptography applications by employing permutation and substitution approaches to encrypt data. This research will primarily focus on applying the LUC Cryptography Algorithm to secure digital fingerprint image data in both grayscale and RGB formats. Prime numbers will be determined using the Trial Division method, and implementation will be carried out using the Python programming language. The objective of this research is to secure digital fingerprint images through the process of encryption and decryption using the LUC Cryptography Algorithm. The outcomes of this study are expected to provide insights into the security of digital fingerprint data and serve as a foundation for the development of enhanced security systems in the future.

Keywords*: Data security, digital fingerprint images, LUC Cryptography Algorithm, encryption, decryption, Trial Division method, grayscale, RGB, Python.*

1. PENDAHULUAN

Dalam era digital saat ini, keamanan data sangat penting, terutama dalam penyimpanan dan pengiriman data pribadi atau rahasia. Salah satu bentuk data yang sangat sensitif adalah data sidik jari digital, yang sering digunakan dalam berbagai aplikasi seperti pengamanan perangkat mobile, pengendalian akses fisik, dan pengenalan identitas [1].

Keamanan data sidik jari digital menjadi semakin penting seiring dengan kemajuan teknologi, karena serangan siber yang terus muncul dan semakin canggih. Oleh karena itu, diperlukan metode enkripsi yang kuat untuk melindungi data sidik jari digital dari akses entitas yang tidak berwenang[2].

Salah satu algoritma kriptografi yang menarik untuk menjaga keamanan data sidik jari digital adalah Algoritma Kriptografi LUC. Algoritma ini dikembangkan oleh Smith dan Michael yang berbasis kepada Fungsi Lucas (Lucas Fucntion), dan telah menunjukkan tingkat keamanan yang baik dalam berbagai aplikasi kriptografi. Algoritma LUC adalah algoritma kunci simetris yang menggunakan pendekatan permutasi dan substitusi untuk mengenkripsi data[3].

Penerapan Algoritma Kriptografi LUC pada data sidik jari digital dapat memberikan manfaat besar dalam mengamankan data ini dari ancaman siber. Pihak yang memiliki kunci enkripsi yang benar yang dapat mengakses dan membaca data tersebut. Hal ini akan mengurangi risiko pencurian atau pengaksesan ilegal terhadap data sidik jari digital yang dapat digunakan untuk identifikasi atau autentikasi.

Penelitian ini akan berfokus pada penerapan Algoritma Kriptografi LUC untuk mengamankan data sidik jari digital. Melalui analisis dan pengujian yang cermat, penelitian ini akan mengevaluasi keefektifan algoritma ini. Hasil dari penelitian ini diharapkan akan memberikan wawasan yang berharga tentang keamanan data sidik jari digital dan dapat digunakan sebagai dasar untuk mengembangkan sistem keamanan yang lebih baik di masa depan.

2. TINJAUAN PUSTAKA

2.1 KRIPTOGRAFI

Berbagai literatur memiliki definisi yang beragam tentang kriptografi. Definisi yang ditemukan dalam buku-buku klasik (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah kombinasi ilmu dan seni yang digunakan untuk menjaga kerahasiaan pesan dengan cara mengenkripsinya sehingga tidak lagi dapat dimengerti maknanya. Definisi ini sesuai dengan penggunaan historis kriptografi di masa lalu, yang sering digunakan untuk menjaga kerahasiaan komunikasi yang penting, seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun, saat ini, peran kriptografi telah berkembang lebih jauh daripada sekadar menjaga privasi pesan. Selain itu, kriptografi juga digunakan untuk tujuan seperti menjaga integritas data, otentikasi, dan non-repudiasi[4].

2.2 KOMPONEN KRIPTOGRAFI

Kriptografi terdiri dari beberapa komponen pendukung yaitu [5]:

1. Enkripsi
   Enkripsi sangat penting dalam kriptografi, yaitu metode untuk melindungi data yang dikirim agar tetap rahasia. Pesan aslinya disebut Teks biasa, diubah menjadi kode-kode yang sulit dipahami.
2. Dekripsi
   Dekripsi adalah kebalikan dari enkripsi. Pesan terenkripsi dipulihkan dalam bentuk aslinya. Algoritma yang digunakan untuk dekripsi pasti berbeda dengan algoritma yang digunakan untuk enkripsi.
3. Kunci
   Adalah kunci yang dipakai untuk melakukan enkripsi dan dekripsi. Kunci terbagi menjadi dua bagian, yaitu *private key* dan *public key.*
4. *Ciphertext*

Merupakan suatu pesan yang telah melalui proses enkripsi. Pesan yang ada pada teks kode ini tidak bisa dibaca karena berupa karakter-karakter yang tidak mempunyai makna.

5. *Plaintext*
   Sering disebut dengan teks asli atau teks biasa ini merupakan pesan yang diketik yang memiliki makna. Teks asli inilah yang diproses menggunakan algoritma kriptografi untuk menjadi chipertext (teks-kode).
6. Kriptanalisis
   Kriptografi tumbuh sangat pesat sehingga melahirkan sebuah bidang yang berlawanan dengan kriptografi yang dinamakan kriptanalisis. Kriptanalisis (*cryptanalysis*) adalah ilmu atau teknik untuk membobol *ciphertext* menjadi *plaintext* tanpa memahami kunci yang dipakai. Orang yang melakukannya disebut kriptanalis.

2.3 TUJUAN KRIPTOGRAFI

Terdapat empat tujuan mendasar dari ilmu kriptografi, yaitu[6] :

1. Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data adalah berrhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. Autentifikasi adalah berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, dan waktu pengiriman.
4. Nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang orang mengirimkan atau membuat.

2.4 CITRA DIGITAL

Citra dapat dijelaskan sebagai suatu representasi intensitas cahaya dalam dua dimensi, yang dapat dinyatakan melalui fungsi f(x, y). Nilai atau amplitudo dari fungsi ini pada koordinat spasial (x, y) menggambarkan tingkat intensitas atau kecerahan citra pada titik tersebut. Citra digital, dalam konteks ini, adalah representasi digital dari fungsi intensitas cahaya f(x, y). Di mana nilai x dan y mewakili koordinat spasial, dan nilai fungsi ini pada setiap titik (x, y) mengindikasikan tingkat kecerahan citra pada titik tersebut. Dalam hal ini, citra digital dapat dianggap sebagai matriks di mana indeks baris dan kolomnya menunjukkan lokasi titik pada citra, sementara nilai dalam matriks tersebut mewakili tingkat keabuan pada setiap titik tersebut[2].

2.5 CITRA GRAYSCALE

Citra grayscale merupakan citra digital yang hanya memiliki satu nilai kanal pada setiap pikselnya, dengan kata lain bagian Red, Green, dan Blue memiliki nilai yang sama. Nilai terseut digunakan untuk menunjukkan tingkat intensitas. Warna yang dimiliki adalah warna dari hitam, keabuan, dan putih. Tingkat keabuan di sini merupakan warna abu dengan berbagai tingkatan dari hitam hingga mendekati putih. Nilai intensitas pada citra beraras keabuan merupakan nilai tunggal dengan nilai intensitas berada pada interval 0 sampai 255, sedangkan pada citra berwarna perlu tiga nila intensitas yang berada pada interval 0 sampai 255 untuk setiap pikselnya. Semakin mendekati 255,

maka derajat keabuan akan semakin terang Pada dasarnya proses ini dilakukan dengan meratakan nilai piksel dari tiga nilai RGB menjadi satu nilai[7].

2.6 CITRA WARNA ATAU RGB (RED, GREEN, BLUE)

Pada citra berwarna ini masing-masing piksel memiliki warna tertentu, warna tersebut adalah merah (Red), hijau (Green), dan biru (Blue). Jika masing-masing warna memiliki range 0-255, maka totalnya adalah 2553=16.581.375 (16 K) variasi warna berbeda pada gambar, dimana variasi warna ini cukup untuk gambar apapun. Karena jumlah bit yang diperlukan untuk setiap pixel, gambar tersebut juga disebut gambar-bit warna. Citra berwarna ini terdiri dari tiga matriks yang mewakili nilai-nilai merah, hijau dan biru untuk setiap pikselnya [8].

2.7 ALGORITMA LUC

Algoritma kriptografi LUC merupakan salah satu algoritma kriptografi asimetris. Algoritma ini pertama kali dikemukakan oleh Peter J. Smith dan Michael J.J. Lenon pada tahun 1993 merupakan sebuah algoritma kriptografi yang berbasis pada fungsi lucas (Lucas Function). Fungsi Lucas (lucas function) dapat dijabarkan sebagai berikut[9]:

Masukkan nilai a dan b menjadi persamaan akar polinomial x2 - Px + Q = 0. Kemudian P = a + b dan Q = ab. Pada umumnya kedua linier berulang tersebut adalah:

$$Un = (an - bn) / (a - b) \quad (1)$$

$$Vn = an + bn \quad (2)$$

Ada dua fungsi yang bisa diturunkan dari persamaan (1) dan (2). Adalah :

$$Un + 1 = PUn - QUn-1 \quad (3)$$

$$Vn + 1 = PVn - QVn-1 \quad (4)$$

Kemudian, pada persamaan (4) dapat diturunkan,

$$Vn = PVn-1-Vn-2 \quad (5)$$

Di mana $n \geq 2$, V0 = 2 dan V1 = P

Beberapa persamaan saling berkaitan dan digunakan dengan menambahkan teknik. :

$$V2n = Vn2 - 2 \quad (6)$$

$$V2n + 1 = PVn2 - VnVn-1–P \quad (7)$$

$$V2n-1 = VnVn-1 – P \quad (8)$$

2.8 PROSES PEMBANGKITAN KUNCI ALGORITMA LUC

1. Pilih dua buah bilangan prima, misal p dan q dimana $p \neq q$.
2. Hitunglah nilai n = p x q.
3. Hitung nilai t = (p-1).(q-1).(p+1).(q+1).
4. Ambil sebuah bilangan acak dimana bilangan tersebut lebih besar dari 1 dan lebih kecil dari t kemudian bilangan acak tersebut merupakan bilangan bulat. Bilangan acak disimbolkan dengan e. (1<e<t).
5. Kemudian hitung nilai gcd (e,t) = 1 atau e relative prima terhadap t.
6. Hitung nilai R(n) dengan rumus: R(n) = LCM (p-1, q-1, p+1, q+1).
7. Hitung d untuk mendapatkan hasil e.d mod R(N) = 1.

   Setelah dapat nilai d yang merupakan kunci privat pada algoritma LUC, maka dilakukan proses enkripsi dan dekripsi.

   Keterangan :

   p = Bilangan prima acak

   q = Bilangan prima acak

   n = Hasil perkalian dari nilai p dan q untuk digunakan pada proses enkripsi dan dekripsi

   t = Hasil dari perkalian (p-1).(q-1).(p+1).(q+1) yang akan digunakan pada proses menentukan nilai e (kunci enkripsi)

   e = Nilai kunci enkripsi

   RN = Hasil dari LCM (Least Common Multiple) atau Kelipatan Persekutuan Kecil dari nilai p dan q yang akan digunakan untuk mencari nilai d (kunci dekripsi)

   d = Nilai kunci dekripsi

PROSES ENKRIPSI ALGORITMA LUC

1. Ambil satu nilai pixel yang akan diamankan.
2. V[0] = 2

   V[1] = m

   Jika i ≥ 2 maka V[i] = (m.V[i-1] – V[i-2]) mod n. Proses enkripsi menghasilkan ciphertext.

   Contoh: Pilih sebuah karakter, misal A dengan kode ASCII = 65.

   V [2...e] = (m.V[i-1] – V[i-2]) mod n

   V [0] = 2

   V [1] = 65

   V [2...e] = (65.V[i-1] – V[i-2]) mod 799

   C = V[e] = V[13] = 608

2.9 PROSES DEKRIPSI ALGORITMA LUC

1. Ambil nilai ciphertext dari proses enkripsi, C = Ciphertext.
2. Kemudian dekripsi dengan menggunakan rumus :

   V [0] = 2

   V [1] = C

   Jika i ≥ 2 maka V[i] = (C.V[i-1] – V[i-1]) mod n. Proses dekripsi menghasilkan plaintext (Anggraini, 2017).

   Contoh: Pilih ciphertext sebelumnya yang telah dienkripsi, yaitu 608.

   V [0] = 2

   V [1] = C = 608

   V [2...d] = (C.V[i-1] – V[i-2] mod 799

   m = V[d]

   m = V[2293] = 65 = “A”

3. METODE PENELITIAN

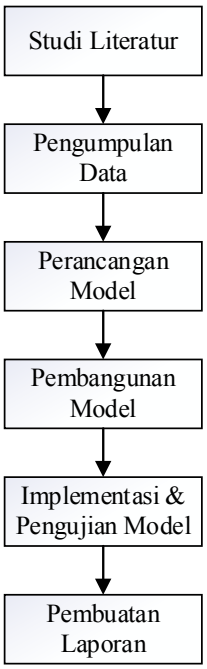
Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian terapan. Penelitian ini berfokus pada kriptografi citra digital sidik jari dengan menerapkan Algoritma Kriptografi LUC. Tahap awal penelitian melibatkan pencarian literatur terkait kriptografi dan konsep matematika yang relevan, seperti Least Common Division, Greatest Common Division, relatif prima, dan aritmatika modulo. Selanjutnya, penulis merancang sebuah model kriptosistem dengan menggambarkan alur proses kriptografi dalam bentuk flowchart.

Pembangunan model kriptosistem dilakukan dengan menggunakan bahasa pemrograman Python dan menggunakan berbagai library yang relevan, seperti NumPy, Tkinter, Python Imaging Library (PIL), dan library math. Proses pengujian model dimulai dari pembangkitan kunci, enkripsi citra digital sidik jari dengan kunci publik, dan dekripsi dengan kunci privat. Hasil penelitian disajikan dalam sebuah laporan yang mencakup pembahasan masalah, tinjauan pustaka, penjelasan mengenai model yang dibangun, hasil dari pengujian model, dan kesimpulan dari penelitian ini.

Alat yang digunakan dalam penelitian ini terdiri dari perangkat keras, yang mencakup sebuah laptop dengan spesifikasi tertentu, dan perangkat lunak, yang mencakup bahasa pemrograman Python versi 3.8, Integrated Development Environment (IDE) Pycharm, serta beberapa library Python yang mendukung pengolahan data, pengolahan gambar, dan operasi matematika. Selain itu, bahan penelitian utama adalah citra digital sidik jari yang diambil dari *The Hong Kong Polytechnic University Contactless 2D to Contact-based 2D Fingerprint Images Database*.

3.1 PERANCANGAN SISTEM

Tujuan dari perancangan sistem secara umum adalah untuk memberikan gambaran umum dan mempermudah dalam melakukan implementasi ataupun evaluasi terhadap sistem yang akan dibangun. Desain sistem secara umum mengidentifikasikan komponen-komponen sistem informasi yang akan didesain secara rinci



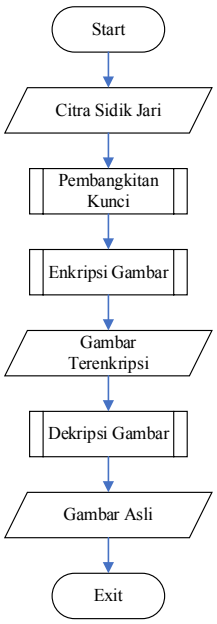
Gambar 2 Bagan Alur Penelitian

3.2 FLOWCHART SISTEM

4. HASIL DAN PEMBAHASAN

4.1 IMPLEMENTASI SISTEM

Implementasi sistem merupakan representatif hasil desaign kedalam bahasa pemrograman. Program enkripsi citra sidik jari menggunakan algoritma LUC telah



dibuat dengan menggunakan bahasa

Gambar 4 Flowchart Sistem

pemrograman Python dan library tkinter, PIL (Python Imaging Library). Program ini memiliki tampilan berbasis GUI (Graphical User Interface) yang memungkinkan pengguna untuk memilih citra sidik jari yang akan dienkripsi, menghasilkan kunci enkripsi, dan melihat hasil citra sidik jari yang telah dienkripsi. Program ini memiliki dua window utama, pertama adalah Home Window, dan Program Window.

4.2 PROGRAM WINDOW

Gambar 1 Home Window

Program window merupakan, window utama dari sistem ini. Window ini berfungsi sebagai media proses memilih citra sidik jari, enkripsi, dekripsi, generate key dan *logout* dilakukan. Pada gambar 4.2 merupakan tampilan Program Window dari Enkripsi Citra Digital Sidik Jari.

Gambar 3 Program Window Enkripsi Citra Digital Sidik Jari

4.3 PEMBAHASAN

Dalam penelitian ini, digunakan dataset eksternal yang telah disediakan oleh The Hong Kong Polytechnic University Contactless 2D to Contact-based 2D Fingerprint Images Database Version 1.0

yang dikembangkan oleh Dr. Ajay Kumar. Dataset ini berisi citra sidik jari dalam format 2D dan bersifat kontak (contact-based), yang nantinya akan digunakan sebagai sampel citra sidik jari untuk pengujian algoritma LUC.

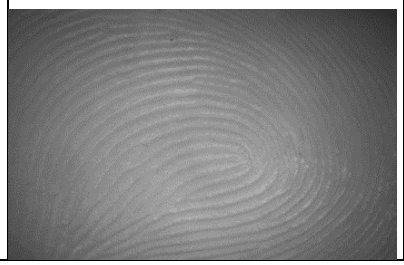
Penggunaan dataset ini bertujuan untuk memungkinkan peneliti dalam melakukan eksperimen enkripsi data citra sidik jari dengan metode yang tepat meskipun dalam kondisi terbatas. Penggunaan dataset eksternal juga dapat menghadirkan variasi data sidik jari yang lebih luas, sehingga hasil pengujian dapat lebih representatif.

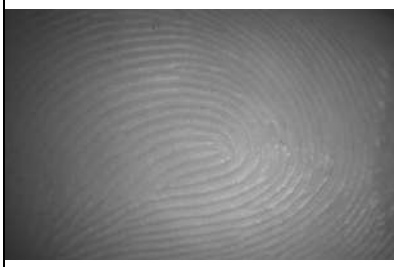
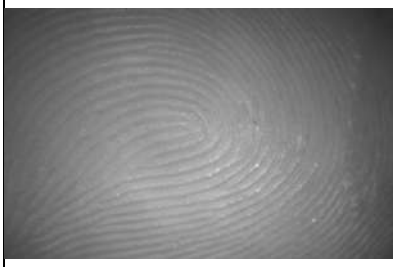
Dalam studi kasus ini, peneliti melakukan langkah-langkah sebagai berikut:

1. Pengumpulan Dataset: Dataset citra sidik jari dari The Hong Kong Polytechnic University Contactless 2D to Contact-based 2D Fingerprint Images Database Version 1.0 diunduh dan digunakan sebagai dataset pengujian dalam penelitian ini.
2. Preprocessing Data: Dataset citra sidik jari dari sumber eksternal diproses dan dipersiapkan sesuai dengan kebutuhan algoritma enkripsi LUC.
3. Implementasi Algoritma LUC: Algoritma LUC diimplementasikan dalam bahasa pemrograman Python menggunakan pustaka (library) seperti PIL (Python Imaging Library) untuk mengenkripsi dan mendekripsi data citra sidik jari.
4. Pengujian dan Evaluasi: Dataset citra sidik jari yang telah dienkripsi menggunakan algoritma LUC akan diuji untuk mengukur kinerja algoritma.
5. Hasil dan Temuan: Hasil pengujian dan temuan dari studi kasus ini akan dianalisis dan dijelaskan dalam poin selanjutnya.

Dengan menggunakan dataset eksternal dari The Hong Kong Polytechnic University, diharapkan penelitian ini dapat memberikan kontribusi dan pemahaman yang lebih mendalam mengenai penerapan algoritma LUC pada data citra sidik jari, meskipun dalam kondisi terbatas di lingkungan Universitas Ubudiyah Indonesia.

Tabel 1 Sampel Citra Digital Sidik Jari

Nama File	Gambar	Ukuran Citra (piksel)	Ukuran Citra (byte)
p9_p1.bmp		350 x 225	78,3 KB

p9_p2.bmp		350 x 225	78,3 KB
p9_p3.bmp		350x225	78,3 KB
p9_p4.bmp		1400x900	3,60 MB
p9_p5.bmp		1400x900	3,60 MB
p9_p6.bmp		1400x900	3,60 MB
1_1.jpg		328x356	55,1 KB

1_2.jpg		328x356	59.6 KB
1_3.jpg		328x356	55,9 KB

4.4 PROSES ENKRIPSI

Pilih citra sidik jari yang ingin dilakukan proses enkripsi

Gambar 5 Pencarian Citra Digital Sidik Jari yang akan di Enkripsi

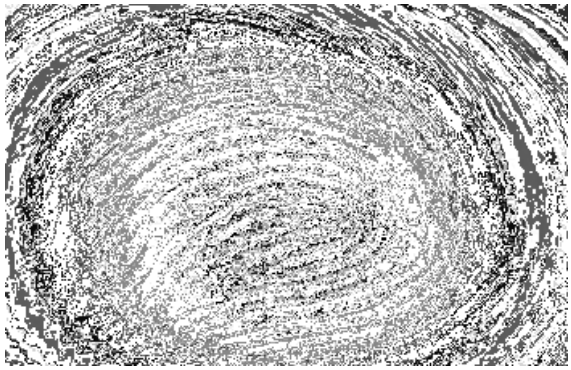
Setiap pixel dalam citra akan dilakukan proses perkalian dengan rumus :

V [2…e] = (m. V [i – 1] – V [i – 2]) mod n

V [0] = 2, nilai V [0] selalu konstan

V [1] = nilai pixel yang sedang dilakukan perkalian

V [e] = menjadi nilai pixel baru setelah dilakukan proses enkripsi



Gambar 6 Citra Sidik Jari p9_p1.bmp yang sudah di Enkripsi

4.5 PROSES DEKRIPSI

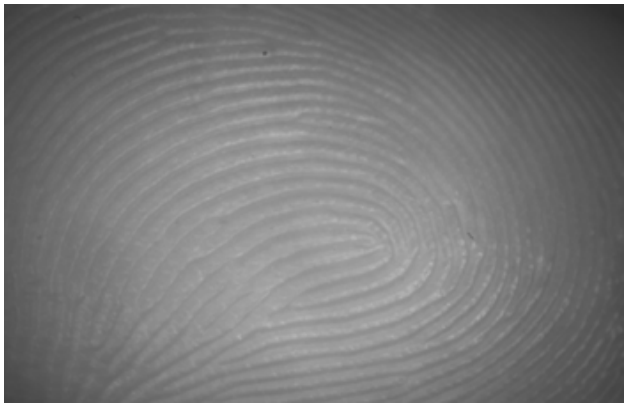
Dari chipertext yang dihasilkan dari proses enkripsi setiap nilai pada pixelnya dikalikan dengan rumus :

V [0] = 2, V[0] Selalu konstant

V [1] = C = nilai pixel yang sedang dilakukan proses dekripsi

V [2…d] = (C. V [i – 1] – V [i – 2]) mod n

V[d] = menjadi nilai pixel baru setelah proses dekripsi

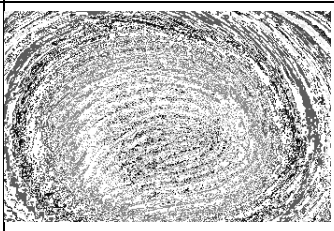
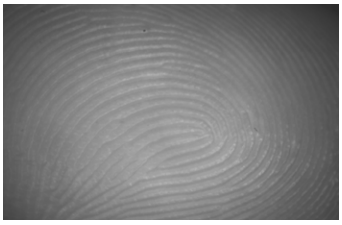
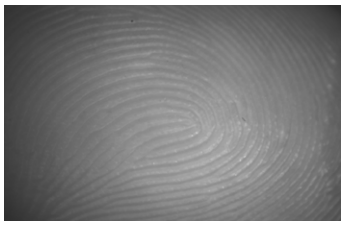
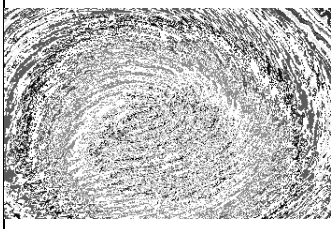
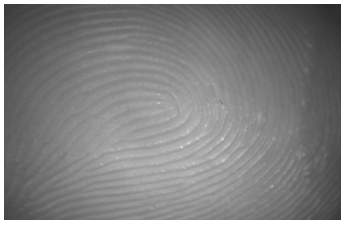


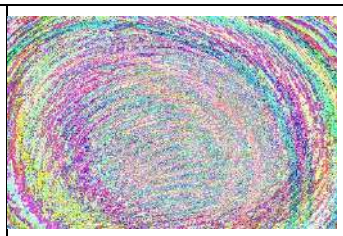
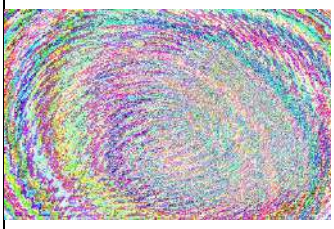
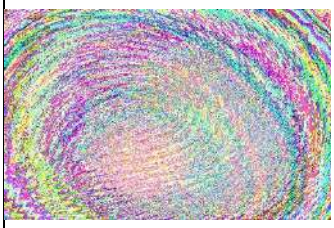
Gambar 7 Citra p9_p1.bmp Hasil Dekripsi

4.6 ANALISIS HASIL

Hasil yang didapatkan pada uji coba data set sampel yang ada pada tabel 1 dengan nilai kunci p = 23, q = 31, e = 59, d = 179, rn = 5280 dan t = 506880 dapat dilihat pada tabel 2 dan 3

Tabel 2 Tabel Uji Coba

Nama File	Citra Terenkripsi	Citra Dekripsi	Image Similarity
p9_p1.bmp			100%
p9_p2.bmp			100%
p9_p3.bmp			100%

p9_p4.bmp			100%
p9_p5.bmp			100%
p9_p6.bmp			100%
1_1.jpg			0%
1_2.jpg			0%

1_3.jpg			0%

Tabel 3 Hasil Uji Coba Citra Digital Sidik Jari

Nama File	Durasi Enkripsi	Durasi Dekripsi	Size Awal	Size Akhir
p9_p1.bmp	3,83 Detik	11,46 Detik	78,3 KB	78,3 KB
p9_p2.bmp	3,85 Detik	11,33 Detik	78,3 KB	78,3 KB
p9_p3.bmp	3,84 Detik	12,07 Detik	78,3 KB	78,3 KB
p9_p4.bmp	196,04 Detik	561,88 Detik	3,60 MB	3,60 MB
p9_p5.bmp	195,21 Detik	556,83 Detik	3,60 MB	3,60 MB
p9_p6.bmp	192,08 Detik	574,19 Detik	3,60 MB	3,60 MB
1_1.jpg	5,78 Detik	17,24 Detik	55,1 KB	37,2 KB
1_2.jpg	5,67 Detik	16,92 Detik	59,6 KB	40,6 KB
1_3.jpg	6,01 Detik	19,44 Detik	55,9 KB	37,6 KB

Dari hasil percobaan di atas menunjukkan bahwa algoritma Kriptografi ini dapat di implementasikan dengan baik. tepada tabel 4.1 dari hasil uji coba untuk semua format citra sidik jari *.bmp mempunyai tingkat kesamaan nilai pixel 100% dan juga ukuran file citra yang sama dengan citra aslinya. Terlihat juga bahwa dengan ukuran file citra yang lebih besar, format file *.bmp mempunya waktu eksekusi yang lebih cepat dibandingkan dengan format citra *.jpg.

Pada kasus file citra yang mempunyai format *.jpg terdapat perubahan ukuran pada file citra sidik jari yang di uji, ini diakibatkan karena pada format citra *.jpg

Gambar 8 Citra sidik jari 1_3 dengan format citra .jpeg

Gambar 9 Citra Sidik Jari 1_3 dengan format .jpeg setelah dilakukan proses enkripsi dan dekripsi

atau *.jpeg (Joint Photograpic Experts Group) ini terjadi karena pada saat

pembentukan kembali file citra sidik jari yang berformat *.jpeg terdapat proses Dicrete Cosine Transform (DCT). Proses DCT ini membuat format citra *.jpeg mengalami penurunan size dengan kualitas citra yang terlihat sama pada saat dilihat menggunakan kasat mata [10]. Bisa dilihat pada gambar 8 dan 9 citra sidik jari yang asli dan sesudah dilakukan proses kriptografi terlihat dengan kasat mata hampir sama, tetapi pada saat dilakukan perhitungan kesamaan nilai pixel didalamnya, menghasilkan 0% tingkat kesamaan pada nilai pixelnya.

5. KESIMPULAN

Berdasarkan analisis, perancangan, dan pengujian dari penelitian, maka dapat diperoleh kesimpulan sebagai berikut :

1. Algoritma LUC dapat diimplementasikan dalam proses enkripsi dan dekripsi pada pengamanan citra digital berbasis desktop dan dapat berjalan dengan baik.
2. Dalam proses enkripsi gambar dengan menggunakan algoritma LUC mampu mengaburkan piksel gambar sehingga informasi di dalam gambar tersebut tidak dapat diketahui.
3. Penelitian ini objek yang digunakan untuk proses enkripsi dan dekripsi dengan menggunakan algoritma LUC adalah gambar dengan format *bmp, *png, *tif , *jpeg
4. Waktu eksekusi algoritma kriptografi LUC sangat bergantung dengan panjang kunci dan ukuran file citra sidik jari tersebut. Semakin besar ukuran citra dan ukuran kunci semakin lama waktu eksekusi yang dibutuhkan.

6. SARAN

Pada penelitian ini, terdapat beberapa saran yang dapat dipertimbangkan untuk pengembangan sistem selanjutnya :

1. Penelitian ini objek yang digunakan adalah citra digital, diharapkan pada pengembangan sistem selanjutnya dapat menggunakan objek lain seperti video, audio, dan lainnya.
2. Penelitian ini hanya menggunakan bilangan prima antara 13-100, diharapkan pada pengembangan sistem selanjutnya menggunakan bilangan prima dengan range yang lebih besar dan dapat mengetahui berapa panjang bilangan p dan q yang paling efektif.
3. Diharapkan untuk penelitian ke depannya dapat melakukan proses enkripsi dan dekripsi pada semua format file citra sidik jari tanpa membuat file citra tersebut mengalami perubahan dalam segi ukuran maupun nilai pixelnya.

7. REFERENSI

[1]. Cahyanto, I. (2023). *Privacy Challenges in Using Wearable Technology in Education Literature Review*. *Formosa Journal of Applied Sciences*, *2*(6), 909-928.

[2]. Sumijan, Widya Purnama, P. A., & Arlis, S. (2021). Buku-Teknologi Biometrik: Impementasi pada Bidang Medis Menggunakan Matlabs.

[3]. Dewi, N. P., Sembiring, D. J., Ginting, R. B., & Ginting, M. B. (2022). Pengamanan Data dengan Kriptografi Hibrida Algoritma Hill Cipher dan Algoritma Luc Serta Steganografi Chaotic Lsb. *Jurnal Syntax Admiration*, *3*(2), 341-361.

[4]. Santoso, H., & Fakhriza, M. F. M. (2018). Perancangan aplikasi keamanan file audio format wav (waveform) menggunakan algoritma

RSA. *Algoritma: Jurnal Ilmu Komputer Dan Informatika*, *2*(1).
[5]. Siregar, S. J., Nugroho, N. B., & Sigalingging, H. (2023). Implementasi Algoritma Kriptografi RSA (Rivest Shamir Adleman) Dalam Pengamanan Data Gaji Karyawan Di Kantor BSPJI. *Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)*, *22*(2), 528-538.
[6]. Nurcahya, S. D. (2022). Implementasi Aplikasi Kriptografi Metode Kode Geser Berbasis Java. *Jurnal Nasional Komputasi dan Teknologi Informasi*, *5*(4).
[7]. Susanto, A. (2019). Penerapan operasi morfologi matematika citra digital untuk ekstraksi area plat nomor kendaraan bermotor. *Pseudocode*, *6*(1), 49-57.
[8]. Prasetio, A. (2021). Citra Digital dan Algoritma Penerapannya.
[9]. Lubis, R. S., Tulus, T., & Nababan, E. B. (2022). Pengamanan File Teks Menggunakan Algoritma RSA–LUC dan Algoritma Zig-Zag dalam Hybrid Crypto Sistem. InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan, 6(2), 186-189.
[10]. Suryadi, N., Indriyani, T., & Nugroho, H. (2020). Sistem Kompresi Citra Berbasis Color Filter Array dan Transformasi 2-D Discrete Cosine pada Manga Reader. *Jurnal Teknologi dan Manajemen*, *1*(1), 18-27.