Pembangkitan Kunci Berdasarkan Pengenalan Wajah Menggunakan Algoritma Kanade-Lucas-Tomasi

Bahrianto Prakoso[1)], Fitri Ramadhanti[2)]
1) Badan Siber dan Sandi Negara, bahrianto.prakoso@bssn.go.id
2) Badan Siber dan Sandi Negara, fitri.ramadhanti@bssn.go.id

Abstrak

Sistem biometrik menawarkan keunggulan yaitu memiliki keunikan yang berbeda pada setiap manusia. Biometrik juga memiliki keunggulan yaitu bersifat permanen, sulit dipalsukan, sulit diretas atau dicuri, dan anti penyangkalan. Dari berbagai banyak keunggulan biometrik maka penelitian ini membahas pembangkitan kunci berbasis biometrik wajah. Syarat suatu angka acak dianggap sebagai kunci kriptografi yang baik adalah angka acak tersebut lulus uji keacakan. Pada penelitian ini menggunakan algoritma Kanade-Lucas-Tomasi (KLT) untuk pelacakan titik unik wajah dan algoritma Viola Jones untuk pendeteksian wajah pada gambar. Pengujian keluaran nilai hash SHA256 sebagai kunci dari proses ekstraksi titik unik wajah menggunakan NIST Stastical Test Suite (NIST STS) untuk menentukan kunci yang dihasilkan dapat digunakan sebagai kunci kriptografi. Sistem yang diusulkan disimulasikan menggunakan MATLAB versi 2017a. Hasil terhadap uji keacakan angka menunjukkan bahwa kunci keluaran hanya dapat memenuhi 7 dari 15 NIST STS sehingga metode ini tidak lolos uji keacakan. Selain itu, terdapat pengujian histogram dan pengujian False Acceptance Rate (FAR) dan False Rejection Rate (FRR). Pengujian histogram menunjukkan terdapat nilai dominan yang menjelaskan bahwa piksel gambar tersebut tidak terdistribusi rata. Pengujian FAR dan FRR menunjukkkan persentase FAR akan semakin kecil jika nilai threshold semakin tinggi dan nilai FRR akan semakin meningkat dengan Equal Error Rate (EER) pada nilai T=4.

Kata kunci: biometrik, deteksi wajah, keacakan, KLT, pelacakan wajah, SHA256, titik fitur, viola jones

Abstract

Biometric systems offer the advantage of being unique to each human being. Biometrics also have the advantage of being permanent, difficult to fake, difficult to hack or steal, and anti-denial. From the many advantages of biometrics, this research discusses the generation of facial biometric-based keys. The requirement for a random number to be considered a good cryptographic key is that the random number passes the randomness test. This research uses the Kanade-Lucas-Tomasi (KLT) algorithm for tracking unique facial points and Viola Jones for face detection in images. Testing the SHA256 hash value output as a key from the face unique point extraction process using the NIST Stastical Test Suite (NIST STS) to determine the resulting key can be used as a cryptographic key. The proposed system was simulated using MATLAB version 2017a. The results of the numerical randomness test show that the output key can only fulfill 7 out of 15 NIST STS so this method does not pass the randomness test. In addition, there is histogram testing and False Acceptance Rate (FAR) and False Rejection Rate (FRR) testing. Histogram testing shows that there is a dominant value which explains that the image pixels are not evenly distributed. FAR and FRR testing shows that the percentage of FAR will be smaller if the threshold value is higher and the FRR value will increase with Equal Error Rate (EER) at a value of T = 4.

Keywords: biometric, feature points, face detection, face tracking, KLT, randomness, SHA256, viola jones

1. PENDAHULUAN

Kriptografi menyediakan teknik untuk menjaga informasi rahasia, untuk menentukan informasi belum diubah, serta untuk menentukan siapa yang menulis informasi tersebut [1]. Teknik kriptografi menyediakan jaminan untuk keamanan informasi dan kunci kriptografi memegang peran penting [2]. Pada setiap algoritma enkripsi pasti memerlukan kunci yang dapat bersifat rahasia seperti *private key* dan kunci yang bersifat publik seperti *public key* [3]. Kunci enkripsi yang disimpan tak jarang dilindungi oleh kata sandi yang dapat ditebak ataupun dapat diperoleh melalui serangan *brute force* yang membahayakan kerahasiaan kunci [3].

Salah satu tahap dalam sistem manajemen kunci adalah proses pembangkitan kunci. Kunci yang dihasilkan apabila terlalu pendek, maka keamanannya akan rendah, sedangkan apabila terlalu panjang dapat menyulitkan pengguna untuk mengingatnya. Proses pembangkitan kunci dapat menggunakan berbagai metode diantaranya menggunakan sistem biometrik [2].

Sistem biometrik menggunakan keunikan pada diri manusia yang berbeda-beda pada setiap individu. Keunikan yang didapatkan dari sistem biometrik akan

menghasilkan suatu nilai yang bersifat unik dan dapat dipastikan berbeda untuk setiap orangnya. Selain itu, sistem biometrik juga memiliki keunggulan yaitu sifatnya universal, unik, permanen, mudah didapatkan, dan juga anti penyangkalan sehingga dapat memenuhi kebutuhan kunci yang aman dan mudah digunakan. Penggabungan biometrik dengan kriptografi sebagai sarana untuk meningkatkan keamanan secara keseluruhan dengan menghilangkan kebutuhan untuk penyimpanan kunci menggunakan kata sandi [3].

Keberhasilan implementasi pada pengguna otentikasi telah menunjukkan bahwa banyak keuntungan dapat diperoleh dengan menggabungkan biometrik dengan kriptografi [4]. Kunci kriptografi dapat dihasilkan dari fitur atau ciri-ciri biometrik pengguna seperti iris, wajah, retina, sidik jari, dan lain-lain. Sebagai sifat biometrik yang digunakan dalam pembangkitan kunci harus bersifat pribadi yaitu seharusnya tidak mengungkapkan apa pun di sekitar data biometrik pengguna [5].

Pelacakan fitur wajah menggunakan algoritma KLT merupakan metode sederhana dan efektif untuk mengenali ekspresi wajah. KLT menggunakan pelacakan dua bingkai sederhana yang cepat tetapi rentan terhadap perubahan isi dalam gradien gambar di sekitar titik pelacakan [6].

Sebagian besar teknik deteksi wajah bergantung pada penampilan, pencocokan *template*, atau fusi multifitur daripada teknik berdasarkan metode segmentasi. Teknik deteksi wajah manusia dalam bentuk apa pun harus mempertimbangkan beberapa masalah untuk memberikan hasil yang akurat. Barnouti *et al*. [6] mengusulkan dua metode pelacakan wajah dan pengenalan pada *video seqeunce* yaitu KLT *feature extraction* dan 2DPCA *Two-Dimensional Principle Component Analysis.* KLT merupakan teknik pelacakan poin fitur dan metode umum digunakan untuk objek deteksi dan pelacakan. KLT menggunakan konsep *two frame tracking* yang memberikan informasi yang tepat tentang lokasi objek.

Pada penelitian [5] menggunakan algoritma *Convolutional Neural Network* (CNN) untuk mengekstraksi gambar yang didapatkan dan dilanjutkan dengan mekanisme pengolahan nilai yang hasilnya dapat memenuhi standar uji keacakan *NIST Statistical Test Suite* (STS). Selain CNN juga terdapat algoritma lain untuk melakukan ekstraksi gambar yaitu algoritma KLT. Namun algoritma ini belum diketahui apakah nilai keluaran dapat memenuhi standar uji keacakan NIST *Statistical Test Suite* dan dapat digunakan sebagai kunci kriptografi. Pengujian persentase nilai *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR) dari sistem biometrik yang diusulkan juga harus dilakukan.

Penelitian ini bertujuan mencari solusi baru sistem pembangkitan kunci kriptografi yang aman dan mudah digunakan dengan menggunakan metode pengambilan gambar manusia, mendeteksi posisi wajah dengan algoritma *Viola Jones* dan mengekstraknya menggunakan algoritma KLT untuk menghasilkan nilai yang dapat digunakan sebagai kunci kriptografi. Aplikasi yang digunakan adalah matlab versi R2017a.

2. LANDASAN TEORI

2.1 Biometrik

Biometrik didefinisikan sebagai ilmu pembentukan identitas individu sesuai dengan karakteristik kimia, perilaku, atau fisik orang. Biometrik adalah karakteristik perilaku individu seperti wajah, sidik jari, dinamika suara, atau dinamika *keystroke*. Data biometrik mengacu pada metrik yang terkait dengan unik karakteristik manusia seperti sidik jari, iris, pengenalan wajah, suara, telapak tangan, dan lain-lain.

2.2 Performa Akurasi Biometrik

Pengukuran akurasi biometrik dilakukan dengan membagi jumlah sampel biometrik yang berhasil diidentifikasi oleh total percobaan atau sampel yang diuji dan hasilnya kemudian dikalikan dengan 100%. Formula untuk menghitung nilai akurasi autentikasi adalah sebagai berikut:

$$\text{Akurasi} = \frac{Jumlah\ sampel\ yang\ berhasil}{Jumlah\ sampel\ percobaan} \text{ x } 100\% \quad (1)$$

- Jumlah sampel yang berhasil merujuk pada total percobaan yang berhasil mengidentifikasi pengguna yang sah.
- Jumlah sampel percobaan adalah jumlah keseluruhan sampel percobaan yang dilakukan.

False Acceptance Rate (FAR) mencerminkan kesalahan sistem dalam mengenali identitas wajah, pengguna yang seharusnya diidentifikasi secara sah dapat keliru terdeteksi sebagai pengguna lain atau bahkan sebagai pengguna yang tidak sah. Rumus yang digunakan untuk menghitung FAR adalah:

$$\text{FAR} = \frac{Jumlah\ penerimaan\ yang\ salah}{Jumlah\ sampel\ percobaan} \text{ x } 100\% \ (2)$$

Keterangan:

- Jumlah penerimaan yang salah mencakup banyaknya percobaan yang keliru dalam mengidentifikasi pengguna yang seharusnya diakui.
- Jumlah percobaan merujuk pada total percobaan yang dilakukan.

FAR dapat memberikan akses kepada pengguna yang tidak sah,untuk mengatasi hal tersebut, dapat dilakukan penyesuaian nilai *threshold*. Namun, perlu diingat bahwa penyesuaian nilai *threshold* dapat meningkatkan nilai *False Rejection Rate* (FRR), yang merupakan kesalahan sistem dalam menolak akses kepada pengguna yang seharusnya diakui. FRR terjadi

ketika wajah pengguna yang seharusnya dikenali dan terdapat dalam *database* tidak diakui oleh sistem. Perhitungan FRR dilakukan dengan menggunakan rumus:

$$FRR = \frac{Jumlah\ penolakan\ yang\ salah}{Jumlah\ sampel\ percobaan} \text{ x } 100\% \quad (3)$$

- Jumlah penolakan yang salah mencakup banyaknya percobaan penolakan terhadap pengguna yang seharusnya diakui.
- Jumlah sampel percobaan merujuk pada total percobaan yang dilakukan.

Nilai *False Acceptance Rate* (FAR) dan *False Rejection Rate* (FRR) dapat direpresentasikan secara grafis dengan menunjukkan titik perpotongan, yang menghasilkan nilai *Equal Error Rate* (ERR) atau *Crossover Error Rate* (CER). Nilai ERR menunjukkan tingkat akurasi yang optimal.

2.3 *Key Generation*

Merupakan proses menghasilkan kunci untuk kriptografi [7]. Pembuatan kunci kriptografi baik sebagai proses tunggal menggunakan generator bit acak dan seperangkat aturan yang disetujui atau seperti yang dibuat selama kesepakatan kunci atau derivasi kunci [8].

2.4 NIST SP 800-22

NIST SP 800-22 merupakan dokumen yang membahas mengenai aspek dalam memilih dan menguji generator bilangan acak dan *pseudorandom.* Dokumen ini berisi pengujian terhadap bilangan acak untuk kebutuhan kriptografi seperti pembuatan materi kunci. Generator yang digunakan dalam aplikasi kriptogafi perlu memenuhi persyaratan yang terdapat dalam dokumen ini. Secara khusus, keluarannya harus tidak dapat diprediksi. Beberapa syarat untuk memilih generator yang sesuai dibahas dalam dokumen ini. Pengujian generator pada dokumen ini terdapat 15 jenis uji yaitu [9]:

1. *The Frequency (Monobit) Tets;*
2. *Frequency Test Within a Block;*
3. *The Runs Test;*
4. *Tests for the Longest-Run-of-Ones in a Block;*
5. *The Binary Matrix Rank Test;*
6. *The Discrete Fourier Transform (Spectral) Test;*
7. *The Non-overlapping Template Matching Test;*
8. *The Overlapping Template Matching Test;*
9. *Maurer's "Universal Statistical" Test;*
10. *The Linear Complexity Test;*
11. *The Serial Test; The Approximate Entropy Test;*
12. *The Approximate Entropy Test;*
13. *The Cumulative Sums (Cusums) Test;*
14. *The Random Excursions Test;*
15. *The Random Excursions Variant Test.*

2.5 Pengenalan Wajah

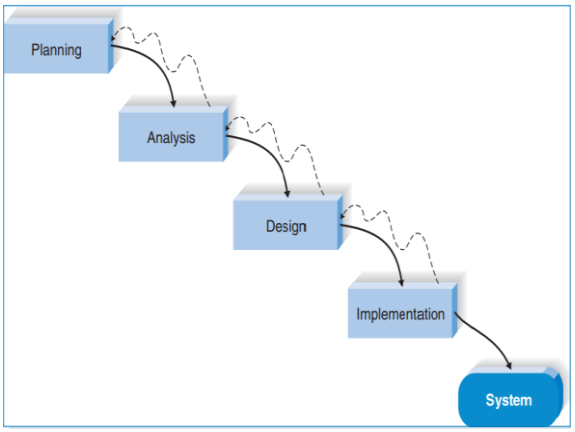
Teknologi pengenalan wajah adalah teknik biometrik yang menggunakan wajah untuk mengidentifikasi karakteristik individu. Teknologi pengenalan wajah mencakup pendeteksian wajah, posisi, pengenalan identitas, dan prapemrosesan gambar. Algoritma pendeteksi wajah mengidentifikasi sistem koordinat semua wajah dalam satu gambar dan menggunakan pemindaian seluruh gambar untuk mengidentifikasi area wajah. Posisi wajah adalah posisi fitur wajah di sistem koordinat deteksi wajah. [10]

2.6 Algoritma Kanade-Lucas-Tomasi (KLT)

KLT adalah algoritma yang populer untuk pelacakan fitur dan estimasi aliran optik dalam visi komputer. Algoritma KLT bekerja pada urutan gambar dan menggunakan perkiraan gerakan untuk melacak sejumlah titik fitur dari waktu ke waktu. Algoritma ini percaya bahwa dalam lingkungan kecil, intensitas titik fitur tetap konstan. Tujuan utama algoritma ini adalah untuk menemukan perpindahan setiap titik fitur di antara *frame* yang berurutan [11].

3. METODE PENELITIAN

Desain pada penelitian ini menggunakan metode *System Development Life Cycle* (SDLC) dengan pendekatan *Waterfall Development*. Pendekatan ini dilakukan dengan beberapa proses yaitu *planning*, *analysis*, *design*, dan *implementation* [12]. Pada Gambar 1 menjelaskan proses SDLC dengan pendekatan *Waterfall Development*.



Gambar 1. Pendekatan *Waterfall* [12]

3.1 *Planning* (Perencanaan)

Pada tahap perencanaan bertujuan untuk memahami pembangunan sistem dan menetukan bagaimana cara membangun sistem. Pada penelitian ini, tahap perencanaan dilakukan dengan melakukan studi literatur mengenai topik penelitian terkait dari berbagai jurnal dan *paper*. Studi literatur yang dilakukan mengenai proses pembangkitan kunci, pengenalan wajah, dan uji keacakan menggunakan NIST SP 800-22. Hasil dari studi literatur menunjukkan bahwa diperlukan metode baru untuk menghasilkan pembangkitan kunci yang memenuhi NIST SP 800-22.

3.2 *Analysis*

Penelitian ini akan membuat skema penelitian mengenai pembangkitan kunci dengan menggunakan nilai eigen dan vektor eigen dari hasil ekstraksi wajah seseorang.

3.3 *Design*

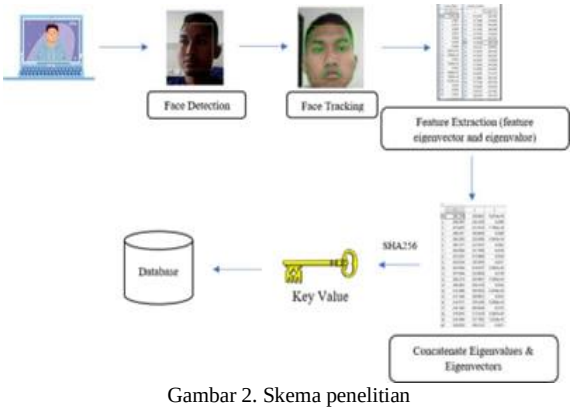
Tahapan desain menentukan bagaimana sistem akan beroperasi. Perancangan sistem menggunakan *flowchart* untuk menjelaskan, menggambarkan, dan menyederhanakan proses yang terdapat pada sistem yang dibangun. Hasil dari tahapan ini adalah cara kerja sistem yang dibangun. Sistem yang akan dibangun mengenai pembangkitan kunci menggunakan pemrosesan wajah dengan uji keacakan menggunakan NIST SP 800-22.

3.4 *Implementation*

Pada tahap implementasi bertujuan untuk menerapkan skema penelitian yang diusulkan pada tahap desain dan menguji skema tersebut. Tahap ini menggunakan MATLAB untuk membuat program dan memproses wajah seseorang yang diambil dari kamera.

4. HASIL DAN PEMBAHASAN

Tahapan yang dilakukan adalah melakukan pengambilan gambar dengan kamera laptop, proses deteksi wajah, setelah didapatkan posisi wajah pada gambar dilakukan proses pelacakan wajah untuk memetakan titik unik wajah yang selanjutnya diekstraksi untuk mendapatkan nilai wajah. Keluaran nilai wajah terdiri dari tiga variabel yang semuanya akan digabungkan dan menjadi keluaran nilai kunci. Pada Gambar 2 menjelaskan proses dari masing-masing tahap yang dilakukan dari skema penelitian ini.



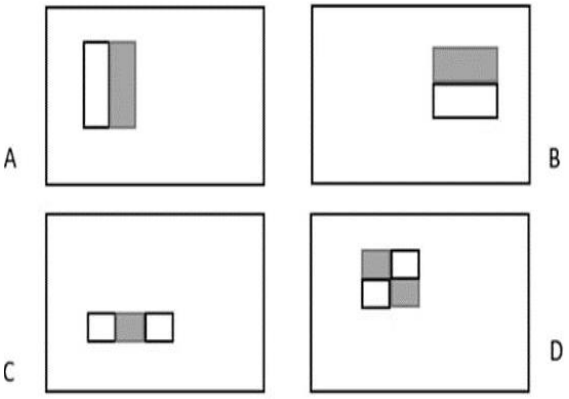
Gambar 2. Skema penelitian

1. Input gambar dari kamera

Pada tahap ini kamera yang telah tersambung dengan sistem akan melakukan proses pengambilan gambar. Sistem ini dijalankan di atas aplikasi Matlab sehingga ketika kamera sudah aktif, kamera didefinisikan pada kode program untuk mengatur ukuran piksel pengambilan gambar. Pada penelitian ini ukuran piksel yang diambil adalah 800 x 600 karena sistem membutuhkan gambar yang tidak terlalu besar dan hanya akan mengambil gambar satu orang. Namun, juga tidak dapat menggunakan piksel yang terlalu kecil karena tidak dapat mendapatkan proporsi wajah yang sesuai dan dapat diproses.

2. Deteksi wajah

Pada tahapan ini dilakukan proses deteksi wajah yang sudah direkam oleh kamera menggunakan algoritma Viola-Jones. Klasifikasi gambar dilakukan berdasarkan nilai dari sebuah fitur. Terdapat tiga jenis fitur berdasarkan jumlah persegi panjang yang terdapat di dalamnya, seperti gambar berikut [13]

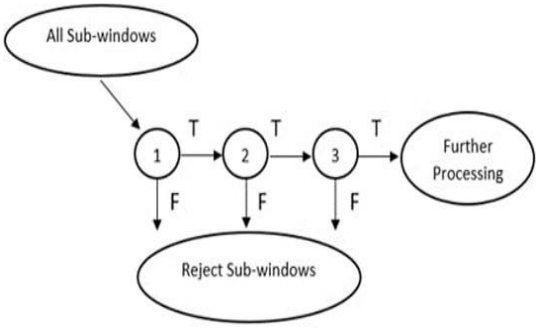


Gambar 3. Jenis filter gambar pada Viola Jones [13]

Pada Gambar 3 menggambarkan bahwa fitur A dan B terdiri dari dua persegi panjang, sedangkan fitur C terdiri dari tiga persegi panjang dan D empat persegi panjang. Untuk menghitung nilai dari fitur tersebut adalah mengurangkan nilai piksel area putih dengan area hitam. Proses perhitungan menggunakan *integral image*. *Integral Image* adalah sebuah citra yang nilai dari setiap pikselnya merupakan penjumlahan dari nilai piksel kiri atas hingga kanan bawah.

Untuk memilih fitur spesifik yang akan digunakan dan untuk menentukan *threshold*, maka digunakan sebuah metode AdaBoost. AdaBoost menggabungkan banyak *classifier* lemah untuk membuat *classifier* kuat.

Karakteristik dari algoritma Viola-Jones adalah klasifikasi bertingkat yang merupakan eleminasi sub-citra yang terdeteksi bukan wajah. Hasil klasifikasi final berupa *True* untuk gambar yang memenuhi proses AdaBoost dan *False* apabila tidak seperti yang ditunjukan pada Gambar 4.



Gambar 4. Alur klasifikasi algoritma *Viola Jones* [13]

Algoritma Viola-Jones dipilih karena merupakan algoritma deteksi wajah yang ringan, dan mudah untuk digunakan.

3. Pelacakan Wajah

Proses ini menandakan wajah yang dideteksi dengan pengenalan titik-titik tertentu. Prinsip kerja dari pelacakan wajah ini adalah melacak titik fitur wajah, memilih fitur wajah kemudian mengekstraksi titik fitur wajah. Titik yang didapat pada setiap pengambilan gambar jumlahnya belum tentu sama tergantung dari kualitas gambar yang dihasilkan dari setiap pengambilan.

4. Ekstraksi Fitur

Pada tahap ini titik wajah yang sudah dipetakan akan diekstraksi untuk diambil nilainya. Pada penelitian ini terdapat dua variabel keluaran yaitu nilai eigen dan vektor eigen dari gambar. Nilai eigen berbentuk urutan data bilangan riil. Sedangkan vektor eigen berisi matriks 2 x n dimana nilai n merupakan jumlah titik yang didapatkan pada tahap *face tracking* yang juga berupa bilangan riil.

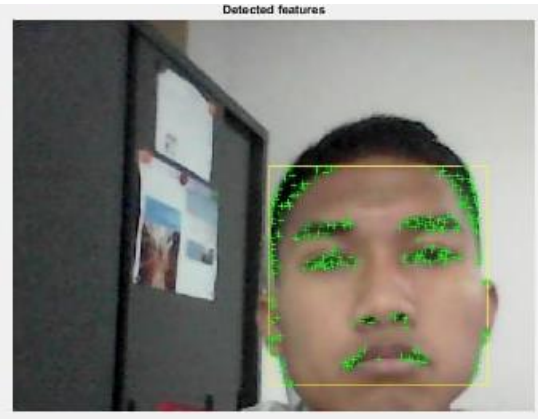
5. Penggabungan Nilai Eigen dan Vektor Eigen

Nilai eigen dan vektor eigen yang didapatkan dari tahap *feature extraction* akan digabungkan menjadi satu urutan data berbentuk matriks 1 x (3 x n) dimana n merupakan jumlah titik yang didapatkan dari tahap *feature extraction*. Kedua nilai tersebut merupakan keluaran dari algoritma KLT yang tidak dapat dikesampingkan salah satu tetapi merupakan satu kesatuan keluaran maka harus digunakan keduanya.

4.1 Hasil

1. Input gambar dari kamera
   Mengambil gambar wajah satu orang dari kamera dengan ukuran 800 x 600.
2. Deteksi wajah
   Pada tahap ini sistem mendeteksi wajah menggunakan algoritma Viola-Jones. Jika sistem mendeteksi wajah maka akan muncul gambar wajah yang diberi tanda kotak *bounding box* (bbox) sebagai tanda wajah yang telah terdeteksi. Bbox merupakan kotak persegi panjang imajiner yang berisi objek titik. bbox mengacu pada koordinat pembatasan. Bbox bertujuan untuk mengidentifikasi target dan berfungsi sebagai titik referensi untuk pendeteksian objek. Berikut hasil deteksi wajah ditunjukkan pada Gambar 5.
3. Pelacakan Wajah
   Proses pelacakan wajah melakukan pemetaan titik unik wajah (*unique property*). Algoritma yang digunakan pada pelacakan wajah adalah algoritma KLT. Terdapat tiga prinsip kerja KLT dalam melacak titik fitur wajah yaitu ekstraksi titik fitur wajah, memilih fitur wajah, dan melacak titik fitur wajah. Dari ketiga proses tersebut menghasilkan gambar wajah yang diberikan tanda pada titik unik wajah yang terdeteksi. Hasil pelacakan wajah tercantum pada Gambar 6.

Gambar 5. Hasil Deteksi Wajah



Gambar 6. Hasil Pelacakan Wajah

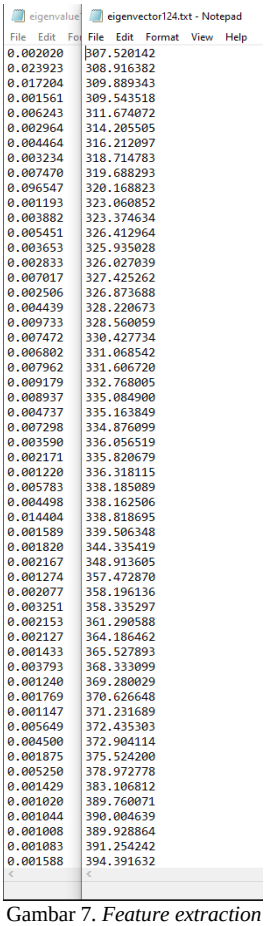
4. Ekstraksi Fitur
   Proses ini menghasilkan dua data dari proses *face tracking* yaitu *Location* menunjukkan posisi titik eigenvector dalam matriks dalam bentuk data *count*x2 *single*, *Metric* merupakan nilai dari eigenvalue dalam bentuk data *count* x 1 *single*, dan *Count* menunjukkan jumlah data *metric* dari fitur eigen. Jumlah data *metric* dari setiap pembangkitan kunci akan berbeda-beda bergantung pada berapa banyak titik yang dihasilkan dari proses pelacakan wajah. Pada penelitian ini rata-rata jumlah titik yang terdeteksi adalah 200 titik. Selain itu didapatkan hasil bahwa nilai vektor eigen yang dihasilkan berada pada rentang nilai yang berdekatan atau hampir sama. Meskipun tidak sepenuhnya sama karena terdapat perbedaan pada nilai di belakang koma. Hasil ekstraksi fitur dapat dilihat pada Gambar 7.
5. Menggabungkan Nilai Eigen dan Vektor Eigen
   Keluaran dari proses *feature extraction* yang terdiri dari 2 variabel nilai akan digabungkan menjadi 1 variabel. Variabel hasil *concate* berjumlah n x 3 dengan n merupakan jumlah titik yang didapatkan dari tahap ektraksi fitur. Proses ini menggabungkan nilai eigen dan vektor eigen dari setiap pengambilan gambar atau pembangkitan kunci. Hasil penggabungan nilai eigen dan vektor eigen dapat dilihat pada Gambar 8.

6. *Hash* Hasil Penggabungan Nilai Eigen dan Vektor Eigen
   Proses ini melakukan proses *hash* dengan SHA 256 nilai hasil penggabungan nilai eigen dan vektor eigen dari gambar wajah sebelum disimpan pada *database*. Nilai *hash* inilah yang digunakan sebagai kunci kriptografi atau keluaran dari proses pembangkitan kunci. Berikut ini nilai hash yang dihasilkan:

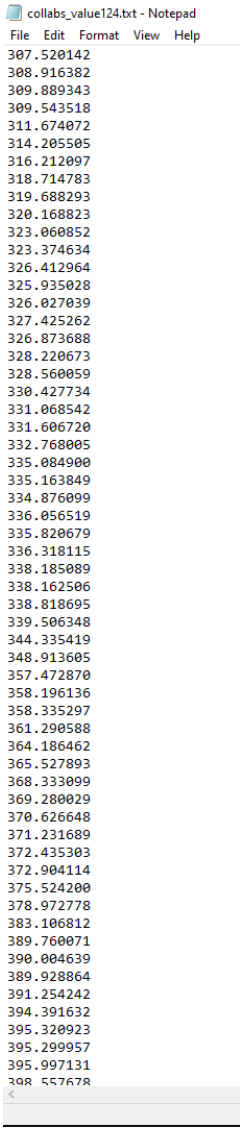
   ```
   5437DAC79A01A4C8FA17F5BA27A572B35328
   9BAA6B20748FD6E306DAA141095C
   ```

   Berdasarkan data yang didapat terdapat kecenderungan pola nilai biner yang dihasilkan adalah nilai yang sama pada bagian belakang dari setiap pembangkitan kunci. Nilai *hash* yang didapat dari penelitian ini totalnya sejumlah 25.600 bit yang digabungkan untuk dilakukan proses pengujian NIST STS. Berikut nilai biner dari nilai *hash* yang dihasilkan.

   ```
   01010100001101111101101011000111
   10011010000000011010010011001000
   11111010000101111111010110111010
   00100111101001010111001010110011
   01010011001010001001101110101010
   01101011001000000111010010001111
   11010110111000110000011011011010
   10100001010000010000100101011100
   ```



Gambar 7. *Feature extraction*



Gambar 8. *Concate* Nilai eigenvalue dan eigenvector

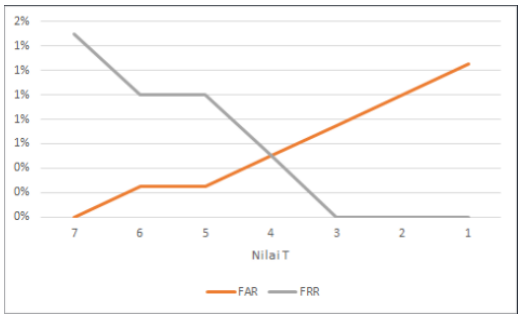
4.2 Pengujian

Dalam penelitian ini dilakukan pengujian keacakan dengan NIST *Statistical Test Suite* untuk mengetahui nilai akhir yang dihasilkan apakah benar-benar acak atau tidak. Selain itu untuk mengukur ketepatan sistem biometrik dilakukan perhitungan *False Acceptance Rate* (FAR), *False Rejection Rate* (FRR), dan uji histogram juga dilakukan untuk melihat nilai keacakan gambar yang diambil.

1. FAR dan FRR
   Pengujian presentase penerimaan gambar biometrik dalam hal ini adalah apakah sistem dapat mengenali wajah dengan tepat atau tidak. FAR atau *False Acceptance Rate* mendefinisikan presentasi kesalahan dimana gambar yang seharusnya tidak terdapat wajah untuk justru dikenali sebagai wajah atau pada satu gambar dikenali dua wajah padahal hanya ada satu wajah. Sedangkan FRR atau *False Rejection Rate* akan mendefinisikan persentase sistem yang tidak mendeteksi wajah pada gambar yang sebenernya

terdapat wajah pada gambar tersebut. Titik pertemuan dari nilai FAR dan FRR disebut sebagai EER atau *Error Equal Rate*.

Pengujian FAR dan FRR dilakukan dengan pengambilan 300 kali gambar dengan nilai diubah dari 1 sampai 7. Apabila nilai T semakin tinggi maka proses *haar filter* atau proses penyaringan gambar akan semakin tinggi dan nilai FAR akan semakin kecil namun justru meningkatkan nilai FRR seperti yang digambarkan pada Gambar 9.



Gambar 9. Grafik FAR dan FRR

Pada Tabel 1 menjelaskan hasil FAR dan FRR dalam persen dari 400x pengambilan gambar FAR terbesar berada pada ambang batas nilai T = 1 dengan 5 kesalahan penerimaan. Sedangkan pada FRR nilai terbesarnya berada pada ambang batas nilai T = 7 dengan 6 kesalahan penerimaan. Nilai EER atau *Error Equal Rate* berada pada nilai T = 4 yang digambarkan pada Gambar 10 sehingga menjadi nilai T yang digunakan sistem pada tahap pendeteksian wajah.

Tabel 1. Nilai FAR dan FRR

Nilai T	FAR (dalam persen)	FRR (dalam persen)
7	0	2
6	0	1
5	0	1
4	1	1
3	1	0
2	1	0
1	1	0

2. *Randomness Test*

Pengujian keacakan dilakukan untuk mengetahui apakah kunci yang dihasilkan dapat memenuhi standar keacakan yang ada atau tidak. Metode yang dilakukan adalah dengan melakukan pengambilan data sebanyak 100 kali dari satu orang dan nilai kunci yang dihasilkan dalam bentuk biner disatukan dengan urutan nilai sesuai dengan urutan pengambilan. Setelah melakukan penyatuan kunci, selanjutnya terdapat pengujian kunci tersebut menggunakan NIST *Statistical Suite Test.* Hasil pengujian menunjukan bahwa kunci keluaran memenuhi tujuh pengujian dan tidak lolos pada delapan pengujian yang ada pada NIST *Statistical Test Suite* dengan rincian ditunjukan pada Tabel 2. Pengolahan nilai hasil ekstraksi dengan algoritma SHA-256 memberikan peningkatan pada nilai keacakan dengan indikator pada hasil pengujian NIST STS yang dibandingkan dengan hasil pengujian nilai penggabungan antara nilai eigen dan vektor eigen memberikan hasil uji lolos pada tujuh pengujian meskipun masih terdapat delapan pengujian yang belum lolos dari total 15 pengujian. Pengujian yang tidak lolos adalah *rank, non-overlapping template, overlapping template, universal, approximately entropy, random excursions, random excursions variant, dan linear complexity* dengan rincian nilai ditunjukkan Tabel 2.

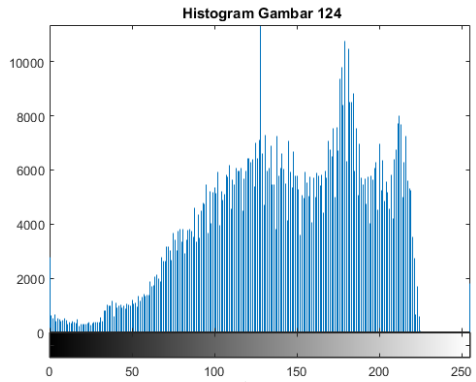
Tabel 2. Hasil Uji NIST STS

No	Pengujian	*p-value*	*proportion*	Hasil
1	Frequency	0,213309	10/10	Lolos
2	Block Frequency	0,739918	10/10	Lolos
3	Cumulative Sums	0,739918	10/10	Lolos
4	Runs	0,350485	10/10	Lolos
5	FFT	0,213309	10/10	Lolos
6	Non-OverlappingTemplate	145/147	147/147	Tidak Lolos
7	Overlapping	0,350485	0/10	Tidak lolos
8	Universal	0,350485	0/10	Tidak lolos
9	Approximate Entropy	0,000000	10/10	Tidak lolos
10	Random Excursions	-	-	Tidak lolos
11	Random Excursions Variant	-	-	Tidak lolos
12	Serial	0,350485	9/10	Lolos
13	Liner Complexity	0,000000	10/10	Tidak lolos
14	Rank	0,000000	0/10	Tidak lolos
15	Longest Run	0,122325	10/10	Lolos

Hasil menunjukan bahwa nilai kunci yang dihasilkan belum sepenuhnya acak dan diperlukan pengembangan lebih lanjut baik dari sisi metode pengolahan nilai yang dihasilkan dari proses ekstraksi maupun dari perangkat yang digunakan seperti kualitas kamera.

3. Uji Histogram

Untuk pengujian histogram mengambil tiga sampel gambar dari 100 total kali pengambilan gambar yang menghasilkan grafik histogram seperti pada Gambar 10. Pada grafik tersebut menunjukkan bahwa persebaran pada gambar tidak tersebar merata dan terdapat nilai-nilai dominan. Hal ini membuktikan bahwa gambar tersebut dikatakan tidak acak. Hasil ini juga dapat dilihat dari keluaran tahap ekstraksi fitur sistem ini.



Gambar 10. Grafik uji histogram

5. KESIMPULAN

Berdasarkan hasil dan pengujian pada penelitian ini maka dapat disimpulkan bahwa metode biometrik dengan pemrosesan gambar wajah tidak sepenuhnya dapat menghasilkan kunci kriptografi yang memenuhi standar keacakan karena kunci keluaran hanya dapat memenuhi 7 dari 15 NIST STS sehingga metode ini tidak lolos uji keacakan. Salah satu penyebabnya adalah nilai biometrik wajah pada satu orang cenderung sama. Kesamaan nilai ini dapat dilihat dari data nilai hasil algoritma KLT yang meskipun terdiri dari dua variabel nilai yang berbeda namun dalam satu variabel nilai di dalamnya cenderung sama. Penambahan proses *hashing* pada sistem yang diusulkan mampu menambah nilai keacakan kunci yang dihasilkan namun proses tersebut belum cukup untuk menghasilkan kunci yang dapat digunakan sebagai kunci kriptografi. Solusi lebih lanjut untuk dapat meningkatkan keacakan hasil sistem adalah dengan menambahkan metode pengolahan nilai yang lebih rumit dan kompleks. Persentase FAR sistem biometrik pada penelitian ini berada pada rentang 0-1 persen. Sedangkan persentase FRR berada pada rentang 0-2 persen. Nilai FAR dan FRR dipengaruhi oleh nilai ambang batas T dari algoritma pendeteksi wajah Viola Jones. Nilai ERR berada pada ambang batas T = 4 yang kemudian sebagai nilai T sistem pendeteksian wajah.

REFERENSI

[1] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, “Applied Cryptography,” 2018.

[2] A. Sarkar, B. K. Singh, and U. Bhaumik, “RSA Key Generation From Cancelable Fingerprint Biometrics,” 2017.

[3] S. Aanjanadevi, V. Palanisamy, and S. Aanjankumar, “An Improved Method For Generating Biometric Cryptographic System From Face Feature,” 2019.

[4] D. Salman, R. Azeez, and A. M. Hossen, “Key Generation from Multibiometric System Using Meerkat Algorithm,” *Engineering and Technology Journal*, vol. 38, no. 3B, pp. 115–127, Dec. 2020, doi: 10.30684/etj.v38i3b.652.

[5] Y. Wang, B. Li, Y. Zhang, J. Wu, P. Yuan, and G. Liu, “A Biometric Key Generation Mechanism for Authentication Based on Face Image,” in *2020 IEEE 5th International Conference on Signal and Image Processing, ICSIP 2020*, Institute of Electrical and Electronics Engineers Inc., Oct. 2020, pp. 231–235. doi: 10.1109/ICSIP49896.2020.9339252.

[6] N. H. Barnouti, M. H. N. Al-Mayyahi, and S. S. M. Al-Dabbagh, “Real-Time Face Tracking and Recognition System Using Kanade-Lucas-Tomasi and Two-Dimensional Principal Component Analysis,” 2018.

[7] E. Barker, “Recommendation for Key Management:,” Gaithersburg, MD, May 2020. doi: 10.6028/NIST.SP.800-57pt1r5.

[8] E. Barker, A. Roginsky, and R. Davis, “Recommendation for Cryptographic Key Generation,” Gaithersburg, MD, Jun. 2020. doi: 10.6028/NIST.SP.800-133r2.

[9] L. E. Bassham *et al.*, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications,” Gaithersburg, MD, 2010. doi: 10.6028/NIST.SP.800-22r1a.

[10] L. Li, X. Mu, S. Li, and H. Peng, “A Review of Face Recognition Technology,” *IEEE Access*, vol. 8, pp. 139110–139120, 2020, doi: 10.1109/ACCESS.2020.3011028.

[11] H. Dorbi and P. Joshi, “Face Recognition Algorithms: A Comparative Study,” *International Research Journal of Modernization in Engineering Technology and Science*, Jun. 2023, doi: 10.56726/irjmets41255.

[12] Dennis A, Wixom B, and Tegarden D, *Systems Analysis and Design*. 2008.

[13] T. M. Effendi, H. B. Seta, and T. Wati, “The Combination of Viola-Jones and Eigen Faces Algorithm for Account Identification for Diploma,” in Journal of Physics: Conference Series, Institute of Physics Publishing, Apr. 2019. doi: 10.1088/1742-6596/1196/1/012070