Pengamanan File Biometrik Pengenalan Wajah Dengan Pendekatan Kriptografi Visual

Gede Sumerta Yoga - 13520021
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13520021@std.stei.itb.ac.id

***Abstrak*—Fitur autentikasi biometrik sudah semakin maju baik dari teknologi maupun algoritma yang digunakan. Setiap device di masa kini pasti memiliki fitur autentikasi biometrik. Salah satu metodenya adalah pengenalan wajah atau face recognition. Namun, fitur ini menimbulkan permasalahan terkait kebocoran data yang dapat melanggar privasi penggunanya. Pada makalah ini, penulis mencoba menggunakan pendekatan kriptografi visual citra biner pada penyimpanan citra atau gambar wajah pengguna. Citra tersebut bisa diubah menjadi beberapa *share* yang tidak memiliki makna jika berdiri sendiri. *Share-share* tersebut dapat disimpan di beberapa tempat berbeda untuk menjaga keamanannya. Kemudian, dicoba untuk dilakukan pengujian dengan teknik pengenalan wajah sederhana untuk membuktikan hasil dekripsi dari *share-share* tersebut masih bisa diperoleh karakteristik wajah yang terbentuk pada citra tersebut.**

Keywords—Kriptografi Visual; Face Recognition; Keamanan Data

I. PENDAHULUAN

Dengan semakin berkembangnya teknologi di era digital ini, keamanan menjadi salah satu aspek yang perlu diperhatikan dalam menjaga integritas data dan privasi. Autentikasi adalah salah satu cara untuk menjaga integritas data tersebut. Kita sudah mengenal beberapa contoh autentikasi "tradisional" seperti kata sandi atau PIN. Saat ini, dengan berkembangnya teknologi, metode autentikasi pun berkembang bersamaan, salah satu yang semakin populer adalah autentikasi biometrik. Autentikasi biometrik ini menggunakan karakteristik dari individu, seperti sidik jari, wajah, atau suara untuk melakukan verifikasi identitas mereka. Autentikasi biometrik ini sulit ditiru karena karakteristik yang ada pada setiap orang itu cukup unik.

Seperti yang sudah disebutkan sebelumnya, autentikasi biometrik bisa dilakukan dengan mengidentifikasi karakteristik wajah atau yang lebih dikenal dengan *Face Recognition* (Pengenalan Wajah). Keunikan setiap wajah manusia, seperti struktur, bentuk, dan hal lainnya memungkinkan kita untuk mengembangkan sistem pengenalan wajah yang cukup dapat diandalkan. Kemudahan dan kenyamanan juga menjadi salah satu alasan fitur ini banyak digunakan. Pengguna hanya perlu menghadapkan wajah mereka ke perangkat atau kamera untuk melakukan autentikasi. Ini juga mengurangi resiko seperti lupa kata sandi atau PIN yang mungkin terjadi pada metode autentikasi lama.

Namun, dibalik keunggulan dari autentikasi dengan *Face Recognition* tersebut, terdapat beberapa tantangan yang perlu diatasi. Salah satunya adalah masalah privasi dalam penggunaan data wajah. Kebanyakan sistem yang menggunakan autentikasi ini lebih memilih untuk menyimpan data keunikan dari wajah seseorang dibanding menyimpan gambar wajah orang tersebut. Hal ini dilakukan untuk mengurangi kemungkinan pelanggaran privasi jika terjadi kebocoran data.

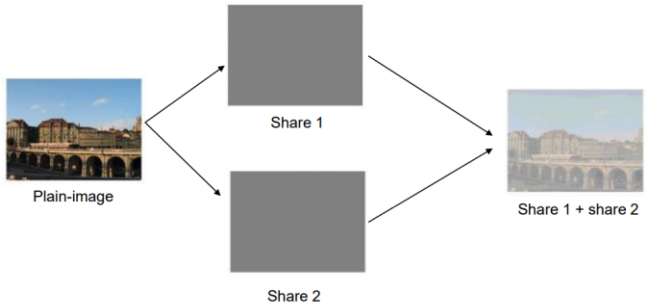
Dalam makalah ini, penulis mencoba membuat alternatif cara penyimpanan data wajah pengguna dengan menggunakan kriptografi visual. Ini bukan berarti mengatasi masalah yang ada sebelumnya, tetapi mencoba meminimalisir kemungkinan pelanggaran privasi dan kemungkinan kebocoran data secara menyeluruh.

II. LANDASAN TEORI

A. *Kriptografi Visual*

Kriptografi visual adalah suatu teknik kriptografi yang melakukan enkripsi terhadap suatu informasi visual dengan suatu cara dan dapat didekripsi sehingga dapat dilihat dengan menggunakan indra penglihatan. Kriptografi visual ini pertama kali dikenalkan pada jurnal *Eurocrypt'94* dan pada makalahnya yang berjudulu "Visual Cryptography" buatan Moni Naor dan Adi Shamir.

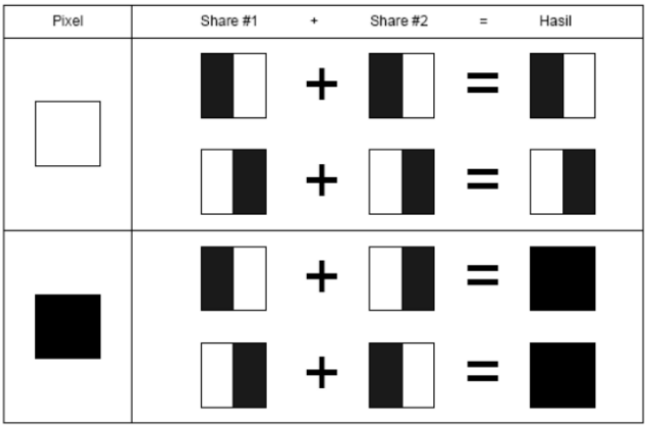
Konsep umum dalam kriptografi visual ini adalah dengan membagi sebuah citra atau gambar menjadi sejumlah bagian yang disebut dengan *share* pada proses enkripsi. *Share* ini adalah sebuah citra yang tidak memiliki informasi atau tak bermakna karena terlihat seperti citra acak. Untuk mendapatkan informasi yang bermakna, perlu dilakukan dekripsi dengan cara menumpuk sejumlah *share* tersebut. *Share* yang ditumpuk, tersebut akan menghasilkan citra atau gambar awal sebelum dienkripsi.



Gambar 1. Proses pada Kriptografi Visual
Sumber:
https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/38-Kriptografi-Visual-Bagian1-2023.pdf

Kriptografi visual yang paling sederhana dapat dilakukan pada sebuah citra biner. Citra biner adalah sebuah citra yang tersusun dari pixel-pixel hitam atau putih. Adapun pada kriptografi visual ini, pixel tersebut akan dipecah lagi menjadi sub-pixel yang berguna dalam pembentukan *share*. Adapun langkah yang lebih detail terkait penerapan kriptografi visual pada citra biner adalah sebagai berikut:

1. Setiap pixel dibagi menjadi sejumlah sub-pixel.
2. Setiap pixel muncul pada setiap *share*.
3. Setiap sub-pixel dari setiap share yang ditumpuk akan dipersepsikan sebagai "hitam" atau "putih".
4. Skema lainnya, satu pixel dibagi menjadi empat buah sub-pixel.
5. Setiap *share* dicetak pada plastik transparansi.
6. Ketika dua buah *share* ditumpuk, maka mata manusia mempersepsi pixel yang terbentuk sebagai hitam atau putih. Pixel hitam akan terlihat sebagaimana mestinya dan pixel putih akan terlihat sedikit perbedaan dan masih dapat menunjukkan informasi yang sesuai.



Gambar 2. Skema Kriptografi Visual dengan pembentukan 2 sub-pixel.
Sumber:
https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/38-Kriptografi-Visual-Bagian1-2023.pdf

Dapat diperhatikan pada gambar 2, pixel yang awalnya berwarna hitam pada citra asli akan tetap menjadi warna hitam setelah proses penumpukan *share*. Namun, terdapat sedikit perbedaan pada pixel berwarna putih karena mengandung sedikit *noise*. Meskipun begitu, informasi awal yaitu citra asli masih dapat dipersepsikan dengan cukup baik.

Kriptografi visual dapat dilakukan dengan skema (k, n). Nilai n disini berarti sebuah citra atau gambar akan dibagi menjadi n buah *share*, sedangkan nilai k berarti butuh k buah *share* untuk bisa melakukan dekripsi gambar. Jika jumlah *share* yang digunakan untuk dekripsi kurang dari k, maka tidak dapat menghasilkan gambar semula.

Selain bisa dilakukan pada citra biner, kriptografi visual juga bisa dilakukan pada citra *grayscale* maupun citra berwarna. Namun, penjelasan kedua citra tersebut tidak akan dijelaskan lebih lanjut pada makalah ini.

Walaupun kriptografi visual ini terlihat sedikit berbeda dengan teknik kriptografi lainnya yang lebih umum, tetapi kriptografi visual ini juga memiliki kekurangan. Adapun salah satu kekurangannya adalah hasil dekripsi yang tidak tepat sama dengan citra asli. Ini diakibatkan karena adanya *noise* pada pixel putih. Selain itu kriptografi visual ini juga dapat digabungkan dengan teknik steganografi untuk menciptakan teknik yang dinamakan *camouflage*.

B. Pengenalan Wajah (Face Recognition)

Pengenalan wajah atau *face recognition* adalah bagian dari *computer vision* dan juga merupakan kategori dari autentikasi biometrik. *Face recognition* ini digunakan untuk mengidentifikasi seseorang dalam metode biometrik menggunakan gambar dari wajah seseorang tersebut. Seseorang dapat dikenali melalui keunikannya secara biologis, termasuk dalam karakteristik wajahnya. Mata manusia dapat dengan mudah mengenali seseorang dengan sekali lihat. Hal inilah yang menginspirasi penemuan dari *face recognition*.

Terdapat beberapa langkah yang umumnya dilakukan dalam sistem *face recognition* yang dapat dilihat pada gambar 3. Untuk melakukan *face recognition*, diperlukan sebuah input untuk dideteksi dan diverifikasi. Input bisa berupa gambar ataupun video baik video rekaman maupun *real-time video*. Setelah diperoleh input tersebut, wajah yang ada pada input akan dideteksi untuk dilakukan *training* atau pelatihan dengan suatu *classifier* ini. Pelatihan biasanya dilakukan dengan mengidentifikasi beberapa karakteristik dari wajah seseorang. Setelah pelatihan selesai, *classifier* tersebut dapat digunakan untuk melakukan identifikasi terhadap masukan lainnya dengan data yang sudah dimiliki sebelumnya.

Gambar 3. *Flowchart* dari *Face Recognition*
Sumber: KH Teoh et al 2021 J. Phys.: Conf. Ser. 1755 012006

Pada proses pengidentifikasian wajah seseorang, akan dihitung akurasi kemiripan dari input dengan data yang dimiliki atau dengan *classifier*. Biasanya terdapat batas minimum kemiripan sehingga seseorang bisa dikenali wajahnya. Semakin tinggi nilai akurasi berarti semakin sesuai input dengan data yang dimiliki atau dengan *classifier*.

Namun, terdapat hal yang juga menjadi tantangan dari penggunaan *face recognition* ini. Salah satunya adalah terkait keamanan, yaitu privasi dan integritas data. Sistem pasti perlu menyimpan informasi baik itu gambar dari wajah pengguna atau informasi karakteristik dari wajah pengguna. Biasanya pembuat sistem akan cenderung memilih untuk menyimpan karakteristik dari wajah pengguna tersebut dibanding menyimpan gambar wajah dari pengguna. Hal ini karena rentan terhadap penyalahgunaan data privasi seseorang dan kebocoran data tersebut.

III. RANCANGAN SOLUSI DAN IMPLEMENTASI

A. *Deskripsi Solusi*

Pada makalah ini, penulis mencoba untuk membuat solusi alternatif yang menjawab masalah privasi dan kerentanan terhadap data wajah pengguna yang digunakan pada autentikasi biometrik dengan face recognition. Idenya adalah dibanding menyimpan secara utuh gambar wajah pengguna, teknik kriptografi visual dapat digunakan untuk meminimalisir dampak jika terjadi kebocoran data. Dengan menggunakan kriptografi visual, sebuah gambar wajah pengguna dapat dibagi menjadi dua buah *share*. Kedua buah *share* ini bisa disimpan di dua database yang berbeda sehingga untuk melakukan dekripsi, diperlukan data dari kedua database tersebut. Hal ini mengurangi resiko kebocoran data secara menyeluruh jika sebuah database berhasil ditembus oleh orang lain yang tidak berwenang.

B. *Rancangan Implementasi*

Pada implementasinya, proses dilakukan sesuai dengan cara kerja kriptografi visual sehingga gambar atau citra input yang akan data acuan akan ditranslasikan terlebih dahulu menjadi sebuah citra biner. Adapun konversi yang dilakukan untuk menghasilkan citra biner adalah dengan mengubah gambar atau citra tersebut menjadi citra *grayscale* terlebih dahulu. Kemudian, dengan citra *grayscale* tersebut, pembuatan citra biner menjadi lebih mudah dilakukan.

Selanjutnya, citra biner tersebut akan dilakukan enkripsi dengan menggunakan skema (2,2) dan sebuah pixel akan dibagi menjadi 4 sub-pixel pada *share*. Skema (2,2) berarti gambar akan dibagi menjadi dua buah *share* dan perlu kedua *share* tersebut untuk melakukan dekripsi agar menghasilkan informasi sesuai gambar semula. Adapun, untuk pembentukan dua *share* tersebut dilakukan sesuai dengan skema yang ada pada tabel 1 dan tabel 2. Atau dijelaskan lebih detail sebagai berikut:

1. Dibatasi terdapat 4 kemungkinan sebuah pixel dipecah menjadi 4 sub-pixel pada sebuah share. Hal ini dapat dilihat pada kedua tabel.
2. Ketika share 1 sudah ditentukan susunan sub-pixel untuk sebuah pixel, susunan sub-pixel pada share 2 akan menyesuaikan dengan susunan sub-pixel pada share 1 dan juga warna pixel pada citra aslinya.
3. Jika warna pixel pada citra asli adalah putih, maka pemilihan sub-pixel bisa mengacu pada tabel 1. Dan begitu sebaliknya jika warna pixel pada citra asli adalah hitaam, pemilihan sub-pixel dapat mengacu tabel 2.
4. Untuk pemilihan sub-pixel dilakukan secara acak dengan tiap kemungkinan memiliki peluang dipilih yang sama, yaitu 25%.

Tabel 1. Skema pmebentukan share pada pixel putih

Peluang	Share 1	Share 2	Hasil Penumpukan
25%			
25%			
25%			
25%			

Tabel 2. Skema pembentukan share pada pixel hitam

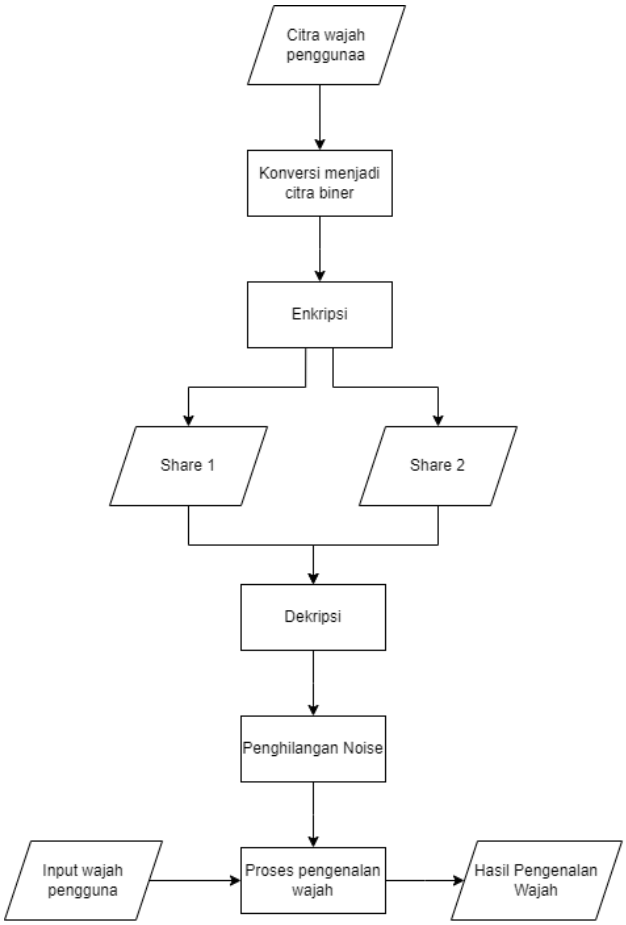
Peluang	Share 1	Share 2	Hasil Penumpukan
25%			
25%			
25%			
25%			

Setelah dihasilkan dua buah share, kedua share tersebut dapat disimpan di dua database yang berbeda untuk mengurangi kemungkinan data berhasil dibobol. Namun, pada implementasi ini, kedua *share* cukup disimpan di lokal saja karena tujuannya hanya untuk simulasi.

Ketika ingin mulai melakukan pengenalan wajah, kedua *share* dari tiap data citra akan digunakan dalam proses dekripsi untuk menghasilkan citra yang merepresentasikan citra awal. Hasil dari proses dekripsi adalah sebuah citra yang merepresentasikan citra awal, tetapi memiliki kekurangan karena adanya noise. *Noise* ini dapat menjadi hambatan pada proses pengenalan wajah karena dapat mengaburkan pengidentifikasian karakteristik wajah sehingga perlu proses yang membuat *noise* menjadi berkurang.

Setelah noise sudah dikurangi, input dari wajah pengguna yang diperoleh melalui video secara *real-time* akan dianalisis dan dibandingkan dengan semua citra hasil dekripsi yang dimiliki. Semakin tinggi tingkat kemiripan maka semakin sesuai wajah pengguna tersebut dengan identitas pengguna yang sesuai dengan data wajah yang dimiliki. Jika tidak ada data wajah yang memiliki kemiripan melebihi minimum persentasi kemiripan, maka pengguna tidak dapat dikenali dan akan ditolak pada proses autentikasi.

Untuk algoritma pengenalan wajah yang digunakan cukup sederhana dan tidak perlu menggunakan Deep Learning karena tujuan dari pengetesannnya adalah melihat karakteristik dari wajah hasil citra dekripsi tersebut. Terdapat beberapa karakteristik yang akan diidentifikasi, seperti ukuran mata, panjang wajah, lebar wajah, ukuran hidung, dll. Kemudian data tersebut akan dibandingkan dengan data yang diperoleh secara real-time video saat pengguna mencoba mendeteksi wajahnya. Pada algoritma tersebut dihitung kemiripan dari karakteristik wajah kedua data tersebut.



Gambar 4. Flowchart Implementasi
Sumber: Dokumen Pribadi

IV. Analisis dan Pengujian

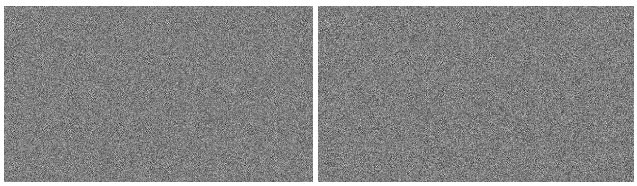
Rancangan implementasi sebelumnya diprogram dengan menggunakan bahasa Python. Khusus untuk fitur *Face Recognition* menggunakan library face_recognition milik akun "ageitgey". Metode pengenalan wajah pada library tersebut juga sangat sederhana, yaitu dengan membandingkan data karakteristik wajah dari dua gambar dan menghitung persentase kemiripannya.

Untuk pengujian digunakan dua buah gambar wajah, yaitu gambar wajah Lionel Messi dan Cristiano Ronaldo.

Gambar 5. Gambar Wajah Lionel Messi yang digunakan
Sumber: https://dailypost.ng/wp-content/uploads/2023/05/Messi.jpg

Gambar 6. Gambar Wajah Cristiano Ronaldo
Sumber:
https://library.sportingnews.com/styles/crop_style_16_9_desktop/s3/2023-01/cristiano-ronaldo-al-nassr-presentation.jpg?itok=KQ7-LwnU

Adapun agar makalah ini tidak terlalu panjang, beberapa gambar berikutnya adalah gambar yang berkaitan dengan wajah Lionel Messi. Selanjutnya, kedua data gambar tersebut dienkripsi dan menghasilkan dua buah *share* untuk masing-masing gambar. Kedua buah share ini tidak memiliki makna jika dilihat secara satu per satu. Inilah ide dari makalah ini, yaitu jika kedua *share* ini disimpan di dua tempat berbeda dan salah satu *share* berhasil diperoleh, maka pembobol tersebut tidak akan memperoleh hasil apapun dari sebuah *share* tersebut.



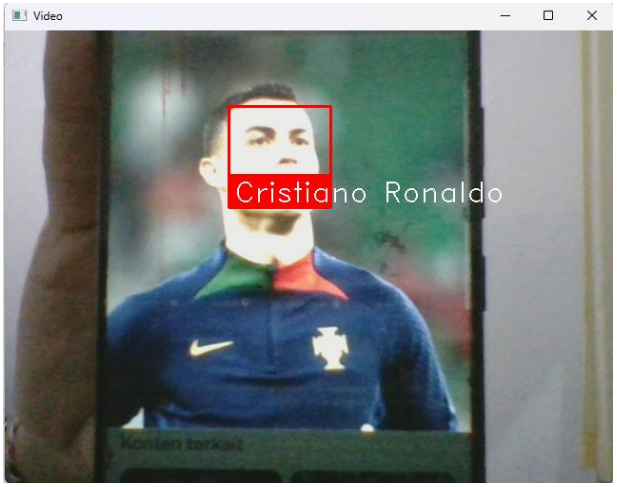
Gambar 7. *Share* 1 dan *Share* 2 dari Gambar wajah Lionel Messi
Sumber: Dokumen Pribadi

Untuk melakukan dekripsi, kedua share tersebut akan digabung atau ditumpuk dan menghasilkan sebuah citra baru hasil dekripsi. Citra baru ini masih memiliki *noise* dan akan diproses lebih lanjut untuk diminimalkan.

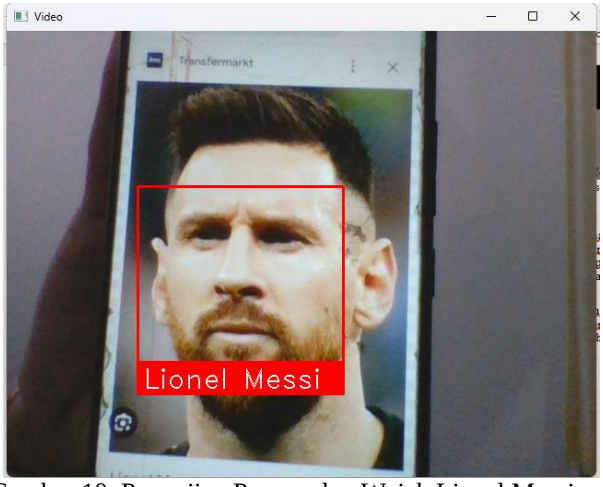
Gambar 8. Gambar wajah Lionel Messi setelah proses Dekripsi dan penghilangan noise.
Sumber: Dokumen Pribadi

Dapat dilihat gambar setelah proses meminimalkan *noise* pada citra wajah Lionel Messi. Memang gambar yang dihasilkan tidak sebaik dengan gambar awal, tetapi ini sudah cukup untuk mengidentifikasi karakteristik wajah yang terdapat pada gambar tersebut.

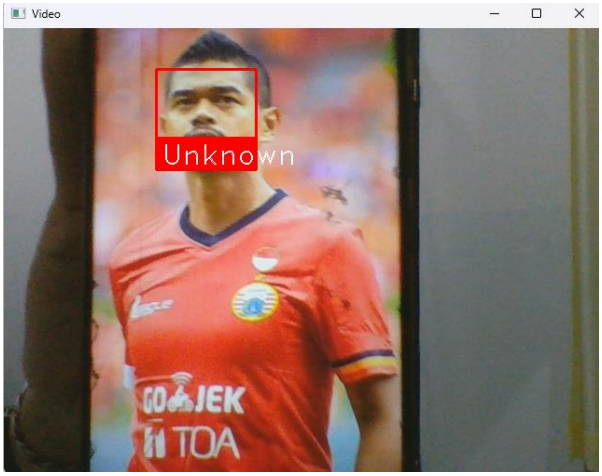
Kemudian, pengujuan dilanjutkan dengan mencoba digunakan pada aplikasi pengenalan wajah sederhana yang dibuat dengan library face_recognition pada python. Kedua citra hasil dekripsi (Lionel Messi dan Cristiano Ronaldo) dimasukkan ke dalam algoritma pengenalan wajah untuk diidentifikasi karakteristik dari wajahnya. Kemudian dicoba untuk mengidentifikasi beberapa gambar wajah. Yang pertama adalah dengan mengidentifikasi gambar wajah Lionel Messi dan Cristiano Ronaldo, tetapi dengan menggunakan gambar yang berbeda dan yang kedua adalah dengan gambar wajah orang lain.



Gambar 9. Pengujian Pengenalan Wajah Cristiano Ronaldo
Sumber: Dokumen Pribadi



Gambar 10. Pengujian Pengenalan Wajah Lionel Messi
Sumber: Dokumen Pribadi



Gambar 11. Pengujian Pengenalan Wajah Bambang Pamungkas
Sumber: Dokumen Pribadi

Dari hasil pengujian tersebut, aplikasi sukses untuk mengenali wajah dari Lionel Messi dan Cristiano Ronaldo dengan data yang diperoleh melalui proses kriptografi visual sebelumnya. Selain itu, diuji juga untuk data wajah yang tidak ada dan aplikasi tidak dapat mengenali wajah tersebut. Hal ini menunjukkan bahwa gambar hasil proses kriptografi visual masih bisa digunakan sebagai data untuk mengidentifikasi wajah seseorang. Meskipun begitu, tentu bukan berarti ini menunjukkan metode terbaik karena yang digunakan adalah citra biner dan tentunya masih banyak ruang untuk pengembangan kedepannya.

V. Simpulan dan Saran

Autentikasi Biometrik dengan menggunakan metode pengenalan wajah atau Face Recognition adalah cara autentikasi yang sangat efektif dan juga memberikan kemudahan kepada pengguna. Namun, metode ini rentan terhadap masalah privasi dan kebocoran data pribadi sehingga biasanya pengembang akan memilih untuk menyimpan data karakteristik wajah pengguna dibanding menyimpan file gambar wajah pengguna. Dengan menggunakan kriptografi visual, dapat dibuat alternatif baru, yaitu dengan menyimpan *share* dari suatu gambar dan menyimpannya di berbagai tempat atau database sehingga lebih aman dan pembobol perlu untuk membobol semua database untuk mendapatkan file wajah pengguna.

Berdasarkan pengujian yang dilakukan, gambar hasil dekripsi dengan kriptografi visual citra biner masih dapat mengidentifikasi karakteristik wajah pada gambar. Meskipun begitu, masih dapat dikembangkan lagi seperti, membagi gambar menjadi *share* yang lebih banyak untuk meningkatkan keamanan dan bisa dilakukan dengan metode kriptografi citra lain seperti citra berwarna sehingga mendapatkan perhitungan yang lebih akurat.

VI. Ucapan Terima Kasih

Pertama-tama, penulis mengucapkan puji syukur kepada Tuhan Yang Maha Esa karena atas berkat dan rahmatNya penulis dapat menyelesaikan makalah ini tepat waktu. Adapun tujuan penulisan makalah ini adalah sebagai bentuk pemenuhan tugas mata kuliah IF4020 Kriptografi.

Dalam penyusunan ini penulis ingin berterima kasih kepada berbagai pihak yang telah mendukung dan mendorong pembuatan makalah ini. Oleh karena itu, saya menyampaikan terima kasih kepada:

1. Dr. Ir. Rinaldi Munir, MT., selaku dosen mata kuliah Kriptografi yang telah memberikan bimbingan dan dorongan untuk membuat makalah ini dan telah menyiapkan bahan ajar yang juga digunakan dalam makalah ini.
2. Orang tua yang senantiasa memberikan dukungan secara moril ataupun material kepada anak-anaknya sehingga bisa seperti saat ini.

Demikian ucapan terima kasih penulis kepada orang-orang yang mendukung dalam proses pembuatan makalah ini. Semoga dengan adanya makalah ini dapat memberikan gambaran dan sedikit pemikiran tentang masalah yang disampaikan.

Referensi

[1] Munir, Rinaldi. “Kriptografi Visual, Teori dan Aplikasinya (Bag. 1)”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/38-Kriptografi-Visual-Bagian1-2023.pdf. Diakses pada 20 Mei 2023.

[2] Munir, Rinaldi. “Kriptografi Visual, Teori dan Aplikasinya (Bag. 2)”. https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2022-2023/39-Kriptografi-Visual-Bagian2-2023.pdf. Diakses pada 20 Mei.

[3] KH Teoh et al 2021 J. Phys.: Conf. Ser. 1755 012006

[4] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5] Geitgey, Adam. 2016. “Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning”. https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78

[6] Rajanwar, S., Kumbar, S., & Jadhav, A. (2014). Visual Cryptography for Biometric Privacy. International Journal of Science and Research (IJSR), 3(12), December 2014.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Mei 2023

Gede Sumerta Yoga - 13520021