ALMA MATER STUDIORUM – UNIVERSITÀ DI BOLOGNA
CAMPUS DI CESENA

Corso di Laurea in Scienze e Tecnologie Informatiche

Morphing di immagini digitali

Fondamenti di Elaborazione delle Immagini

Relatore:
Chiar.mo Prof. RAFFAELE CAPPELLI

Co-Relatore:
Dott. MATTEO FERRARA

Presentata da:
Fabbri Mirco

II Sessione
Anno Accademico 2014/2015

Indice

Glossario

Sorgente	Immagine, contenente il volto di un soggetto, fornita in input ad un processo
Morphing	Processo in cui, fornite due sorgenti in input, viene generata un'immagine finale contenente le caratteristiche di entrambe le immagini.
Morphed	Immagini risultante dal processo di morphing
Database	Raccolta di immagini morphed
…coordinate assegnate alle immagini…	Punti assegnati a due immagini per realizzare il warping. (
…punti assegnati alle immagini…	Coordinate assegnate a due immagini per realizzare il warping.
Mappare punti | coordinate	Assegnare punti | coordinate
Soglia minima | Score minimo | Limite minimo	Valore minimo ottenuto da un tool di verifica per considerare una morphed appartenente ad un immagine di test

Introduzione

Al giorno d'oggi la verifica dell'identità ricopre un ruolo predominante nell'ambito della sicurezza informatica e sociale. L'identificazione di un soggetto ha da sempre avuto un'importanza strategica nella lotta alla criminalità, ma negli ultimi anni lo sviluppo di tecnologie sempre più raffinate ed affidabili ha cambiato il modo in cui viene affrontato il problema. La diversificazione degli ambiti in cui è richiesto il riconoscimento dell'identità di una persona, ha portato ad un utilizzo sempre maggiore di strumenti automatici in grado di rilevare e verificare le generalità di un soggetto.

In questo lavoro di tesi si vuole valutare la fattibilità dell'alterazione di immagini contenenti il volto di un individuo con il fine di ingannare sistemi automatici per la verifica dell'identità del possessore di un documento elettronico.

Lo sviluppo di sistemi biometrici sempre più affidabili, ha favorito il proliferare di tali tecnologie per aiutare il personale umano nel monitoraggio della sicurezza nelle zone di frontiera.

Nel 2002 l'organizzazione internazionale per l'aviazione civile (ICAO) ha selezionato il volto come la caratteristica biometrica primaria da utilizzare in sistemi per la verifica automatica dell'identità. In particolar modo l'avvento dei documenti elettronici di nuova generazione (eMRTD) ha consentito di memorizzare al loro interno informazioni digitali, quali immagini e dati personali, con il fine di creare un documento in grado di identificare univocamente un passeggero.

L'alterazione della fisionomia di un soggetto, contenuta nella fotografia integrata all'interno di un documento elettronico, potrebbe essere sfruttata da malintenzionati per trarre in inganno i sistemi automatici di riconoscimento delle generalità utilizzati alle frontiere (es. ABC gates).

La verifica dell'identità, consiste nell'acquisizione digitale del volto di un individuo che verrà confrontato con quello memorizzato all'interno del documento elettronico presentato. Un potenziale attacco a questi tipi di sistemi potrebbe essere la memorizzazione di un'immagine alterata, contenente caratteristiche di uno o più soggetti in un unico volto, all'interno dell'eMRTD. L'inserimento di tale immagine consentirebbe a più persone di varcare la frontiera tramite uno stesso documento.

Nel corso di questo lavoro di tesi sarà analizzata la fattibilità della creazione di immagini alterate in grado di ingannare sistemi automatici di riconoscimento dell'identità, permettendo così a più soggetti di passare i controlli utilizzando un singolo documento.

Capitolo 1.
Morphing

Il morphing è una tecnica nata con l'avvento della computer grafica per soddisfare esigenze cinematografiche. Prima di allora infatti, non si era in grado di eseguire una trasformazione fluida e senza soluzione di continuità tra due immagini di diversa natura. L'unica metodologia conosciuta consisteva nell'utilizzo di dissolvenza incrociata, in cui si effettuava una sovrapposizione graduale dell'immagine di arrivo su quella di partenza fino alla sua totale sostituzione. Tale tecnica aveva un limite insormontabile che si manifestava in maniera tanto più evidente quanto più le due sorgenti avevano contorni differenti, poiché non era possibile ottenere una vera deformazione tra l'immagine di partenza e quella di arrivo.

L'avvento della computer grafica nella seconda metà degli anni sessanta e lo sviluppo delle tecnologie informatiche, hanno portato, nei primi anni novanta, ad un massiccio impiego di tecniche digitali nelle produzioni cinematografiche. Grazie al contributo economico e tecnologico che l'industria ha esercitato sulla computer grafica, il morphing venne portato alla ribalta mediatica mediante alcune produzioni quali Terminator 2 ed il video musicale Black Or White.

L'utilizzo in contemporanea della tecnica di dissolvenza incrociata e di un effetto di deformazione chiamato warping, dà origine al morphing. Mentre la prima tecnica era possibile fin dagli albori dell'industria cinematografica, il warping richiedeva risorse ai tempi non disponibili. Tale metodologia consiste nell'assegnazione di punti "chiave" tra le sorgenti da processare che verranno utilizzati per generare una maglia triangolare, la cui modifica, tramite spostamento dei punti chiave, si ripercuoterà sull'immagine stessa ottenendo così l'effetto desiderato.

Grazie alle potenze di calcolo oggi disponibili, il morphing si è evoluto e raffinato tanto da garantire risultati eccellenti ed alla portata di tutti. In particolar modo in questo lavoro, si vuole analizzare la fattibilità della creazione di immagini morphed con il fine di ingannare sistemi automatici di verifica dell'identità.

1.1 Dissolvenza incrociata

La dissolvenza incrociata, impiegata fin dai primi anni 60 nelle produzioni cinematografiche, consiste nel calcolo di una media pesata tra due punti delle immagini da processare. Il nuovo valore può essere ottenuto tramite interpolazione lineare delle due sorgenti.

Dati due punti, all'interno delle immagini, la media dei pixel è definita come:

$$\begin{cases} aS1 + bS2 = S1 + (1-a)S2 \\ a + b = 1 \\ S1 \in \text{Immagine1} \\ S2 \in \text{Immagine 2} \end{cases}$$

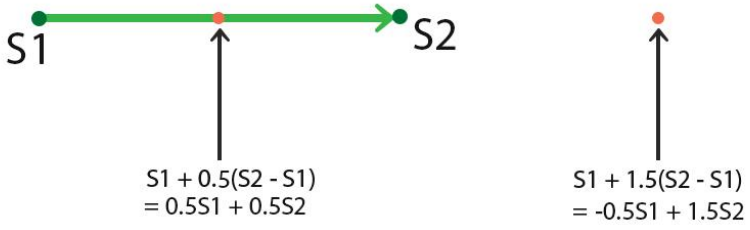


Figura 1 (Punto medio)

Il nuovo pixel interpolato è definito come:

$$\begin{cases} (1-t)S1 + tS2 \\ t \in [0,1] \\ S1 \in \text{Immagine1} \\ S2 \in \text{Immagine 2} \end{cases}$$

Dove t è l'istante in cui calcolare il valore del nuovo pixel mentre S1 e S2 sono i pixel rispettivamente dell'immagine 1 e dell'immagine2.

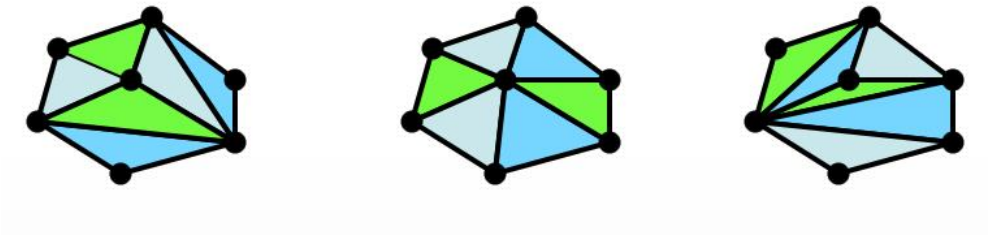
T = 0	*T = 0.25*	*T = 0.5*	*T = 0.75*	*T = 1*
P = (1 – 0)S1 + 0S2	*P = (1 – .25)S1 + .25S2*	*P = (1 – .5)S1 + .5S2*	*P = (1 – .75)S1 + .75S2*	*P = (1 – 1)S1 + 1S2*

Figura 2 (Dissolvenza incrociata tra due immagini)

Requisiti fondamentali per la buona riuscita della tecnica sono la corrispondenza delle dimensioni delle immagini da processare ed il loro allineamento. Tramite operazioni di trasformazione affine è possibile correggere tali problemi e garantire il successo della dissolvenza.

1.2 Warping

Il warping è la seconda tecnica utilizzata per la creazione di immagini morphed e consiste nella "*generazione di una maglia triangolare, a partire da un insieme di punti nel piano, che costituisce una partizione del guscio convesso in triangoli i cui vertici sono i punti sono i punti e non contiene altri punti*".

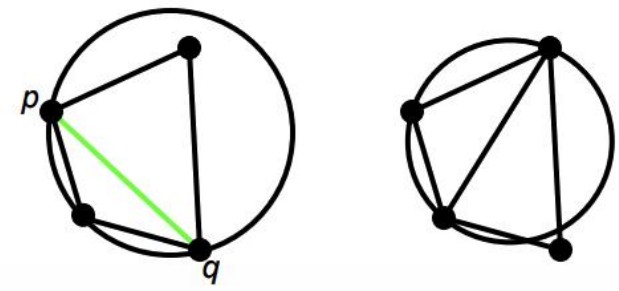


Maglia sufficiente *Maglia buona* *Maglia scadente*

Figura 3

Una maglia triangolare di buona qualità richiede che gli angoli presenti nel guscio convesso siano più grandi possibili.

Definito $\alpha(T) = (\alpha 1, \alpha 2, \ldots, \alpha 3n)$ come il vettore degli angoli, in ordine crescente, all'interno della maglia, una triangolazione T_1 è migliore di una T_2 se $\alpha(T_1) > \alpha(T_2)$. Non tutti i segmenti che uniscono due vertici sono legali, infatti un segmento è legale se e solo se uno dei suoi vertici opposti, appartenenti al poligono, è interno alla circonferenza individuata dagli altri tre vertici.



Segmento illegale *Segmento legale*

Figura 4

La maglia finale “ottima” è chiamata triangolazione di Delaunay ed è legale se e solo se contiene solamente spigoli legali. Inoltre i punti di un triangolo appartenente alla maglia di Delaunay individuano una circonferenza che non contiene altri punti.

Un modo per generare in maniera efficiente la triangolazione di Delaunay è tramite l’utilizzo dei diagrammi di Voronoi.

Dato un insieme finito di punti S, la decomposizione di Voronoi consiste nel partizionamento di un piano in n poligoni V(p) a cui viene associato un punto principale, in modo tale che ogni punto del poligono sia più vicino al punto p che ad ogni altro punto appartenente all’insieme S.

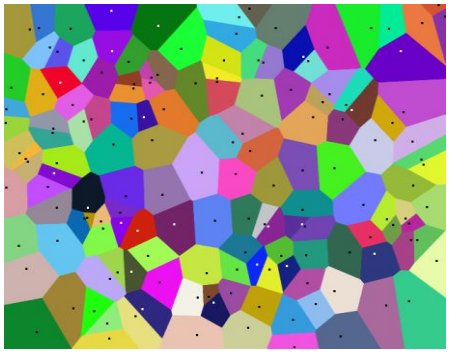


Figura 5 (Esempio di diagramma di Voronoi)

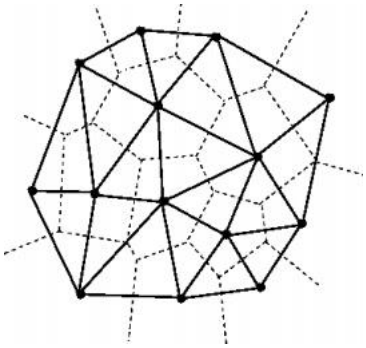


Figura 6 (Triangolazione Delaunay a partire da quello di Vorronoy)

Il grafo duale, che associa un solo punto ad ogni regione V(p) ed un solo arco per ogni arco del grado del diagramma di Voronoi è la triangolazione di Delaunay, che sarà la maglia finale di warping.

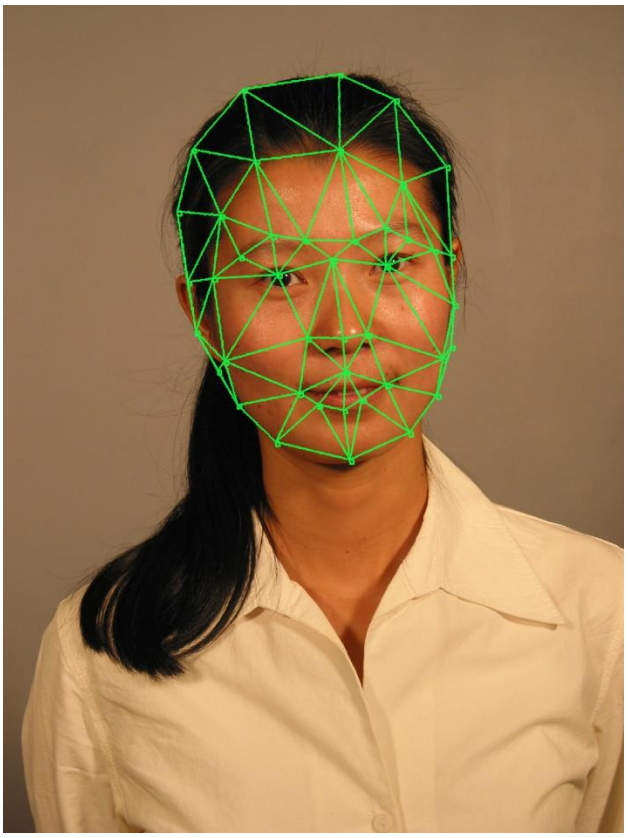


Figura 7 (Esempio warping)

La tecnica di warping necessita di alcuni punti “chiave” mappati all’interno delle immagini da processare, utili alla generazione della mesh triangolare. L’assegnazione di tali coordinate viene analizzata nel capitolo 3.2.

Capitolo 2.
Obiettivo

Nel caso del problema in esame è stata utilizzata la tecnica di morphing per la realizzazione di immagini morphed a partire da sorgenti contenenti volti di soggetti. Il fine ultimo era la costruzione di un piccolo database di fotografie alterate, ognuna delle quali rappresentava una potenziale immagine contenuta all'interno di un eMRTD ed utilizzata per ingannare i sistemi automatici ABC impiegati all'interno degli aeroporti. L'obiettivo finale era la realizzazione di 100 immagini morphed, di cui 50 di sesso femminile e 50 di sesso maschile.

Per riprodurre le reali condizioni in cui il sistema avrebbe dovuto operare, sono state selezionate due immagini per ogni soggetto a partire da un database contenente 899 fotografie suddivise equamente tra uomini e donne. La prima immagine è stata fornita in input al processo di morphing, mentre la seconda è stata utilizzata per eseguire il test di verifica.

Ogni morphed generata doveva essere in grado di ottenere uno score maggiore della soglia minima prefissata per il tool con il quale si stava eseguendo il test di verifica. La valutazione di tale limite è analizzata nel capitolo 4.1.

Capitolo 3.

Generazione di immagini Morphed

Per la generazione di morphed ci si è avvalsi di due tools semi-automatici che hanno permesso di ottenere buoni risultati su tutti campioni analizzati. E' da sottolineare il fatto che l'intero lavoro è stato svolto tramite software reperibile liberamente da chiunque.

Il fine ultimo era l'ottenimento di un'immagine che avesse le caratteristiche di entrambe le sorgenti, ma che fosse particolarmente somigliante a solamente una delle due. La valutazione del risultato è stata effettuata tramite i tools *"VeryLook/MegaMatcher Faces Identification"*, sviluppato da Neurotechnology, e *"LuxandSDK 5.0"* sviluppato dall'omonima azienda. Gli strumenti in questione, prese in esame due immagini contenenti i volti dei soggetti, restituivano un risultato empirico in grado di descrivere la differenza tra i due individui analizzati.

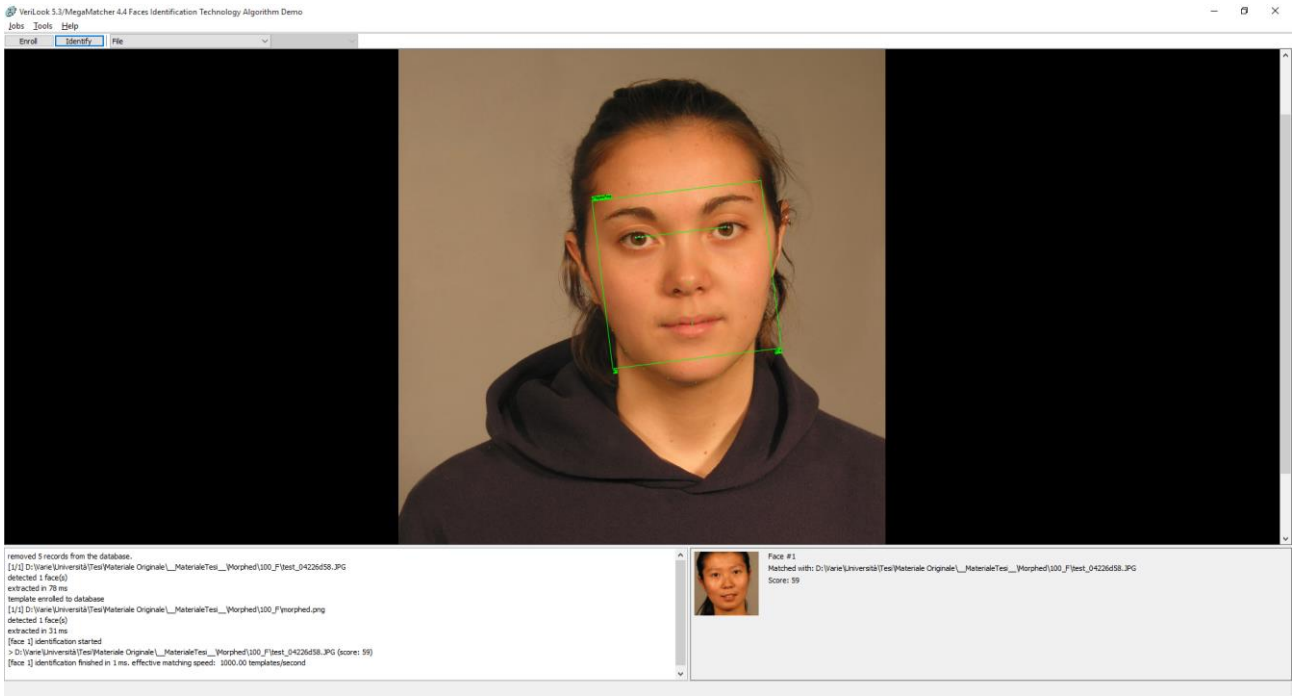


Figura 8 (Esempio di valutazione della bontà dell'immagine morphed con il tool VeryLook)

3.1 Scelta delle sorgenti

Per ogni persona sottoposta al test sono state selezionate due sorgenti che garantissero una qualità tale da permettere al software di estrarre le caratteristiche del soggetto. Ove l'immagine era insufficiente allo scopo, si è cercato di migliorarne la qualità tramite operazioni di equalizzazione e contrast stretching.

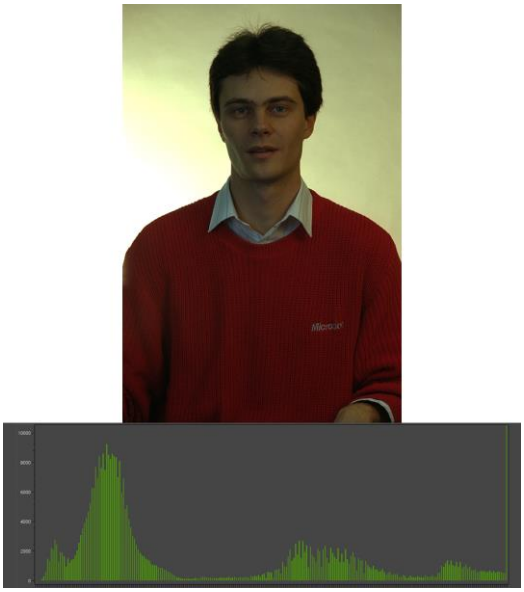


Figura 9 (Immagine originale)

Figura 10 (Immagine equalizzata)

L'obiettivo di ottenere un'immagine morphed che superasse la soglia limite definita per ogni tool ha indotto ad eseguire test preventivi, tra le sorgenti originali, per constatare che tale soglia non fosse superata già prima del morphing.

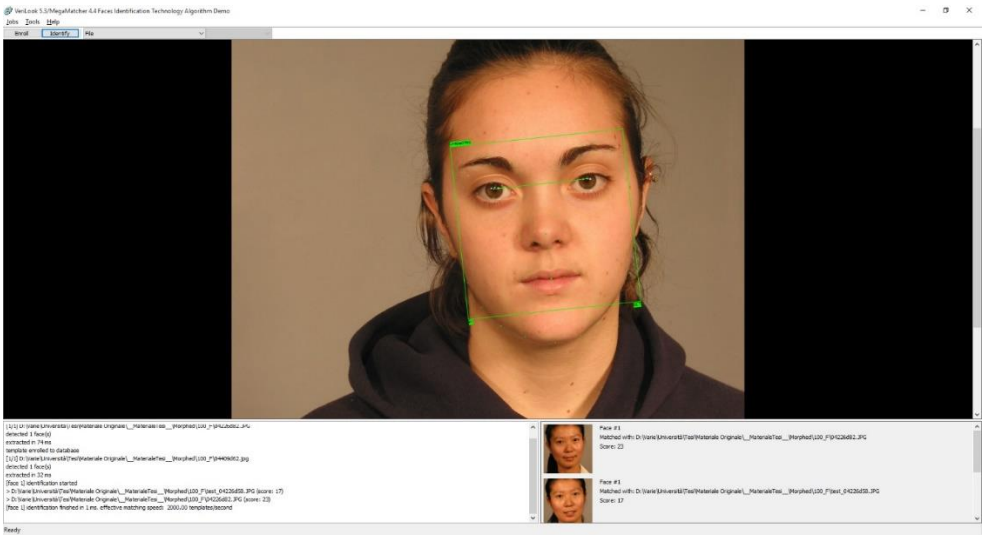


Figura 11 (Test preventivo delle immagini sorgenti con il tool VeryLook)

3.2 Mappatura

Come accennato nel capitolo 1.2 il processo di morphing richiede l'assegnazione di alcuni punti "chiave" utilizzati durante l'elaborazione delle immagini. La mappatura di tali coordinate tra le sorgenti è il processo più importante e delicato per ottenere una morphed finale di qualità.

Al fine della generazione ci si è avvalsi di "Squirlz Morph", uno strumento semi-automatico in grado di creare una serie di frame, ognuno ad un determinato stadio di iterazione, a partire da due sorgenti fornite in input.

Uno dei primi problemi presentatosi consisteva nel processare immagini con scale differenti, le quali avrebbero portato a mappare i punti in maniera imprecisa, generando un risultato insufficiente e non in grado di superare il test finale. Per tale motivo ogni coppia di fotografie è stata preventivamente ridimensionata, tramite operazioni di trasformazione affine, per garantire una corretta assegnazione delle coordinate.

Figura 12 (Vista del tool per la generazione di immagini morphed)

La mappatura è stata eseguita individuando le caratteristiche comuni tra le immagini, prestando particolare attenzione nella selezione di punti facilmente individuabili in entrambe le sorgenti.

In generale si è notato che le zone più sensibili, in grado di influire maggiormente sul risultato finale, risiedevano lungo la parte centrale del viso.

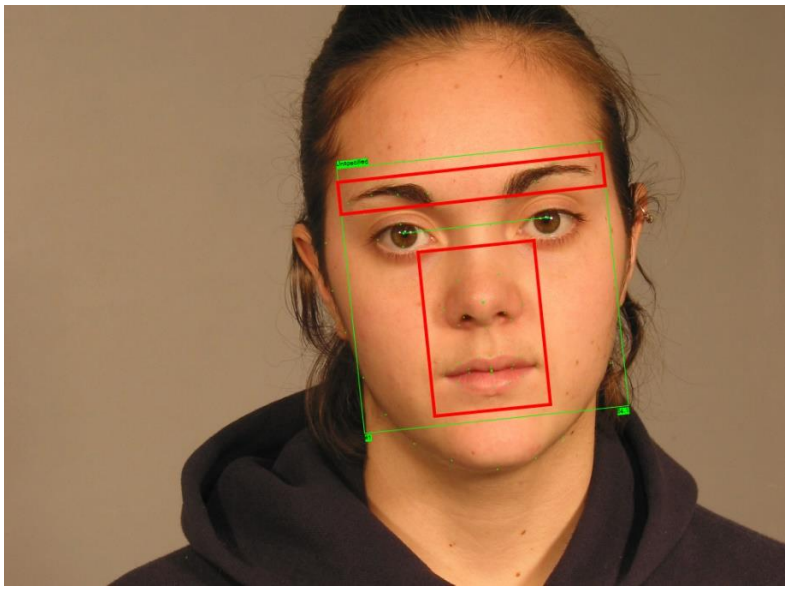


Figura 13 (In rosso sono evidenziate le zone sensibili)

Figura 14 (Esempio di assegnazione delle coordinate)

Per ogni nuovo punto assegnato, una finestra di anteprima mostrava il risultato parziale in modo da permettere la valutazione della correttezza della nuova coordinata.

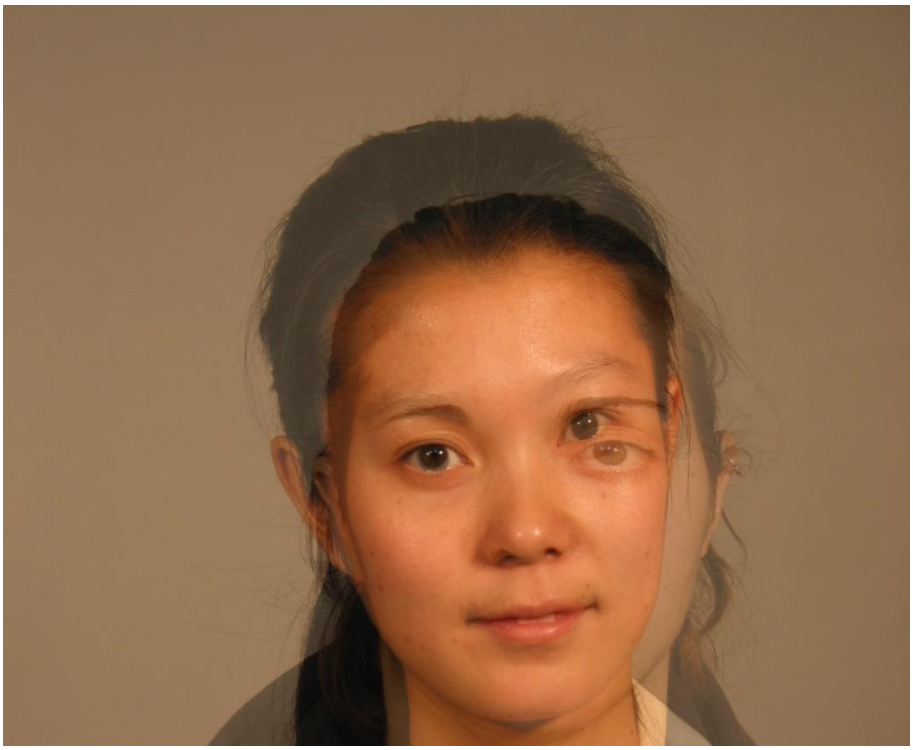


Figura 15 (Anteprima morphed utilizzando le coordinate in Figura 14)

Una delle principali caratteristiche che rendono la tecnica del morphing particolarmente apprezzata, consiste nella possibilità di generare morphed a partire da immagini con contenuti disposti in maniera differente. L'ottenimento di un buon risultato però è vincolato alla corretta mappatura dei punti chiave, i quali, se non fossero assegnati correttamente, porterebbero a generare le caratteristiche di entrambi i soggetti sovrapposte l'un l'altra con la conseguente degenerazione dell'indice di valutazione nel test di verifica.

La Figura 14 mostra l'assegnazione di alcuni punti, localizzati attorno all'occhio sinistro, utilizzati nella creazione della morphed in Figura 15. La non corretta mappatura ha comportato la creazione di un'immagine con caratteristiche sovrapposte, insufficiente a superare la soglia minima nel test di verifica finale.

In questo caso l'unica soluzione possibile è la ridisposizione dei punti chiave.

Figura 16 (Coordinate ridisposte correttamente)

Le figure 16 e 17 mostrano la ridisposizione dei punti che ha garantito la corretta interpolazione delle caratteristiche delle due sorgenti.

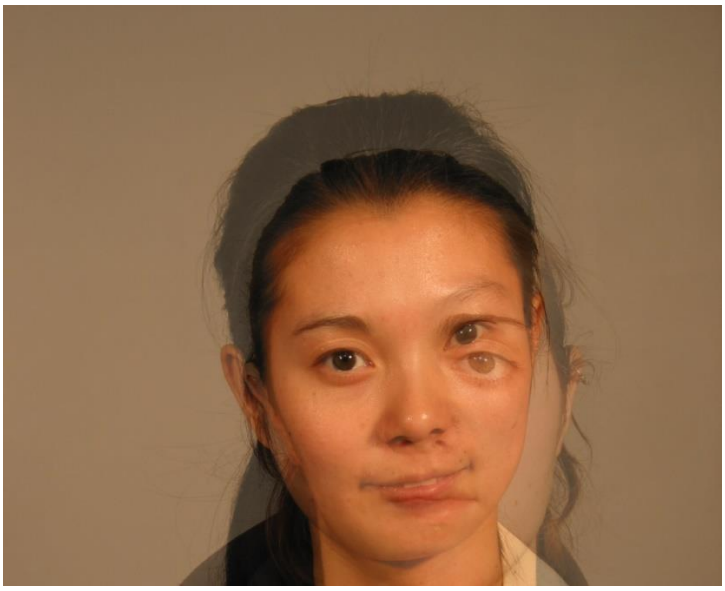


Figura 17 (Anteprima Morphed)

La figura 19 mostra come, nonostante le due immagini abbiano pochi punti in comune, il test di verifica effettuato sul frame centrale (quindicesimo frame di trenta) generato dal tool, abbia ottenuto un buon risultato parziale. E' da sottolineare il fatto che in fase finale non è mai stato selezionato il frame mediano in quanto l'obiettivo era l'ottenimento di un'immagine particolarmente simile ad uno dei due soggetti. Il fotogramma centrale contiene il numero massimo di caratteristiche di entrambe le sorgenti, ma non vi è un soggetto predominante sull'altro per cui la morphed finale risulterà evidentemente manipolata.

Figura 18 (Test di verifica con coordinate approssimative tramite tool VeryLook)

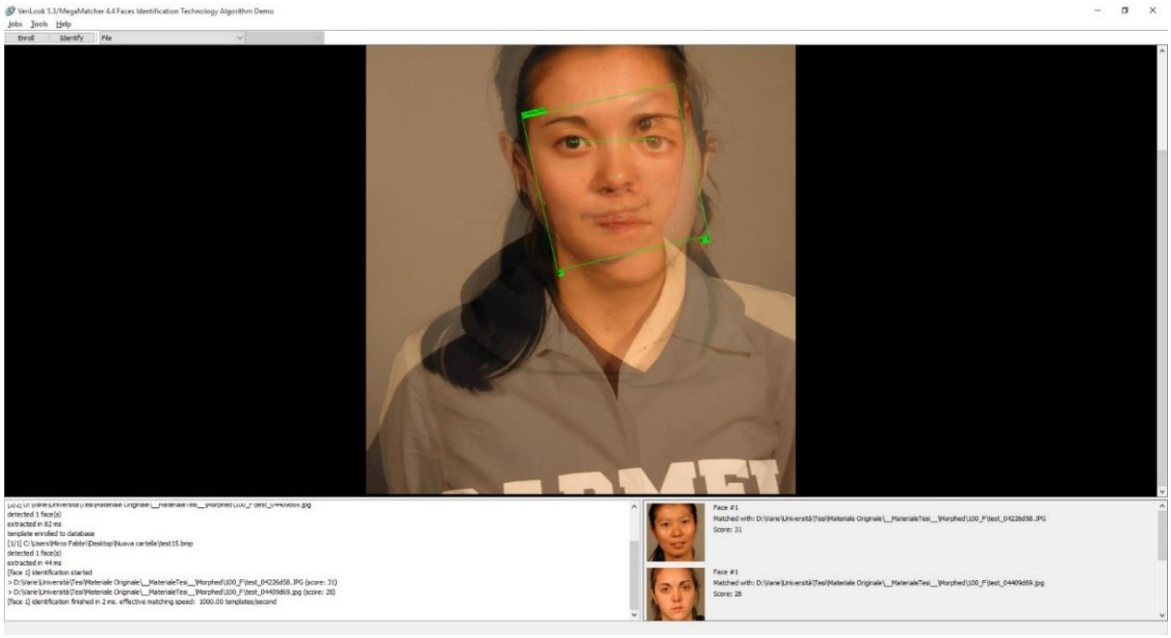


Figura 19 (Test di verifica con coordinate ridisposte (Frame centrale) tramite tool VeryLook)

La ridistribuzione delle coordinate (figura 19) ha migliorato notevolmente il risultato finale permettendo ad entrambe le sorgenti di ottenere uno score simile, utilizzando il tool *"VeriLook"*. Infatti sono state ottenute valutazioni di 31 e 28 rispettivamente con la prima e la seconda immagine di test.

Figura 20 (Test di verifica delle due immagini sorgenti originali)

La scelta di generare 30 fotogrammi da parte del tool Sqirlz Morph, ha consentito di selezionare in ogni situazione il frame con le caratteristiche desiderate.

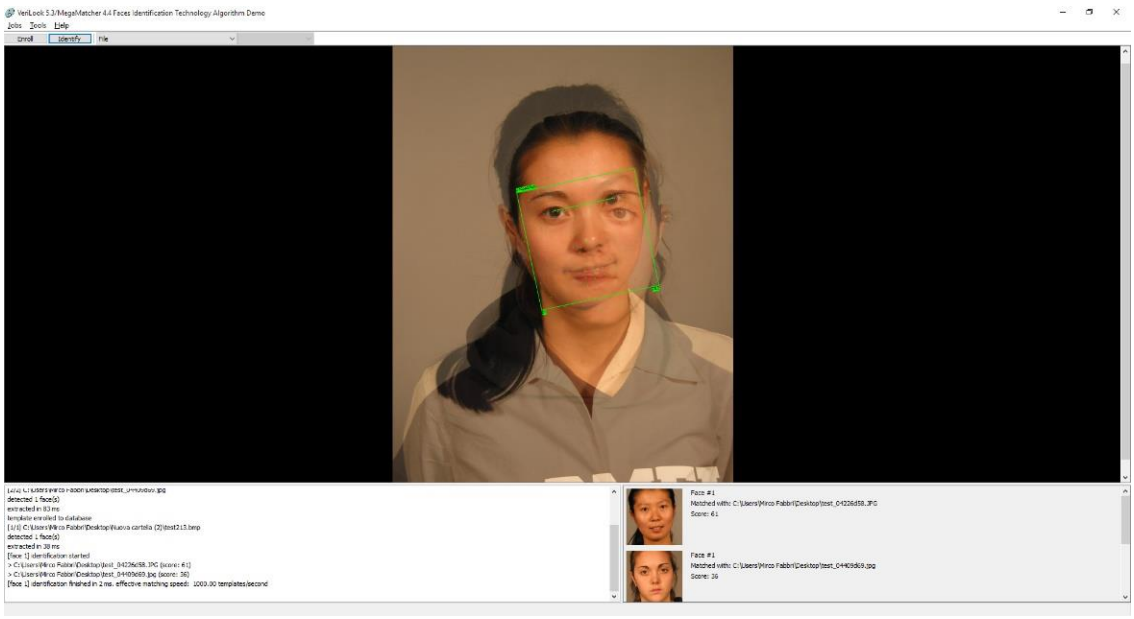


Figura 21 (Test di verifica con frame #13 / 30)

Nell'esempio in esame, il fotogramma numero tredici ha permesso di ottenere uno score notevolmente superiore rispetto a quelli avuti in precedenza. Il risultato finale indica perciò, che entrambe le immagini sono da considerarsi potenzialmente valide per essere utilizzate come morphed in quanto hanno ottenuto valutazioni superiori di trentasei con *"VeryLook"*.

Si è notato inoltre che, nella maggior parte dei casi, l'immagine morphed, era posta nell'intervallo 9-11 e 19-21 dei frame generati dal tool Squirlz Morph.

Figura 22 (Punti chiave disposti su entrambe le sorgenti)

Figura 23 (Frame morphed generati con i relativi score)

Nel caso in esempio (figura 23) il frame, contenente le caratteristiche desiderate, più indicato a diventare l'immagine finale è il numero nove. Lo score ottenuto, con il tool "VeriLook", dalla morphed confrontata con la sorgente uno è 271 mentre quello ottenuto con la seconda sorgente è 46. Il fotogramma selezionato soddisfa quindi i parametri richiesti ma, risultando evidentemente manipolato, richiede alcune modifiche tramite programmi di fotoritocco con cui sarà possibile eliminare le caratteristiche indesiderate ed ottimizzare la resa dalla morphed finale.

Source 1 score: 238
Source 2 score: 60

Source 1 score: 262
Source 2 score: 51

Morphed non ritoccata *Morphed ritoccata*

Figura 24

Com'è possibile notare la rimozione delle caratteristiche non desiderate ha comportato, nella maggior parte dei casi esaminati, una riduzione dello score con la sorgente secondaria.

Per incrementare il punteggio ottenuto, è stato necessario estrarre manualmente alcune caratteristiche dal secondo frame ed applicarle all'immagine morphed. La conseguenza è stata un incremento dello score di matching con il secondo fotogramma ed una riduzione

con l’immagine primaria. Ciò ha permesso di ottenere una crescita significativa del punteggio più debole passando da 51 a 59 con il tool di verifica *“VeriLook”*.

Source 1 score: 254
Source 2 score: 59

Figura 25

Capitolo 4.
Verifica risultati

Il database, da cui sono state prelevate le immagini sorgente fornite in input nel processo di morphing, era costituito da 899 fotografie di volti maschili e femminili. Ogni fotografia, ritraente un soggetto, era identificata univocamente dal codice dell'individuo e dalla data di acquisizione dell'immagine.

Una persona, per essere utilizzata nella creazione di morphed, doveva possedere almeno due sorgenti, acquisite in momenti diversi, utilizzate per la generazione dell'immagine alterata e per il successivo test di verifica.

La valutazione della qualità delle immagini morphed generate è stata effettuata tramite due diversi tool di riconoscimento del volto.

- *VeryLook:* utilizza un algoritmo sviluppato da NeuroTechnology
- *LuxandSDK:* utilizza un algoritmo sviluppato dall'omonima azienda (Luxand, Inc.)

Ogni algoritmo, esaminate due sorgenti, restituiva un punteggio che descriveva la somiglianza dei due soggetti in input. Maggiore era il punteggio ottenuto dal matching tra una sorgente e la morphed, maggiore era la probabilità che il risultato finale riuscisse ad ingannare l'algoritmo di verifica.

Per ogni soggetto coinvolto nel processo di morphing, è stata utilizzata un'immagine del volto per la generazione della morphed, ed un'altra per il test di verifica. Questo ha permesso di simulare condizioni reali di utilizzo, come descritto nel capitolo 4.1.


Sorgente 1
Sorgente 2
Morphed
Test sorgente 1
Score: 272
Test sorgente 2
Score: 54

Figura 26

4.1 Valutazione della soglia

Per analizzare correttamente e verosimilmente la bontà di un'immagine morphed generata, era necessario ricreare le condizioni reali in cui un sistema di riconoscimento usualmente lavora. Per fare ciò sono stati utilizzati due tool, definiti capitolo 4, che applicano i requisiti definiti da FRONTEX (Agenzia europea per la gestione di cooperazione operativa) in fatto di verifica dell'identità.

In particolar modo è stato utilizzato il falso tasso di accettazione (FAR) reale che deve essere di almeno 0.1% per garantire che il sistema ABC operi correttamente.

La soglia è definita come il limite minimo oltre il quale un'immagine morphed è considerata appartenente ad un soggetto di test. Per ogni algoritmo ne sono state utilizzate due:

a) ThrP è indicata dal fornitore del tool.
b) ThrC è la soglia, che permette di ottenere un FAR = 0.1%, individuata all'interno di una serie di confronti *genuine* ed *impostor*.

Lo score minimo indicato dal fornitore di VeryLook è 36 (ThrP) mentre quello calcolato è 39 (ThrC). Il tool LuxandSDK 5.0 utilizza una soglia indicata dal produttore di 0,9990000128 (ThrP), mentre quella calcolata è 0,9658 (ThrC).

Le morphed finali, confrontate con quelle di test, che hanno superato il limite minimo indicato sono state considerate attendibili e potenzialmente valide per ingannare il sistema.

Nel capitolo 5. sono state riportate le percentuali di successo ottenute durante la fase di verifica.

Capitolo 5.

Risultati

Nella tabella sottostante sono riportati i punteggi ottenuti tramite gli algoritmi di verifica indicati nella sezione “Verifica risultati”.

Per entrambi gli algoritmi sono riportate le percentuali in base al tipo di soglia utilizzata.

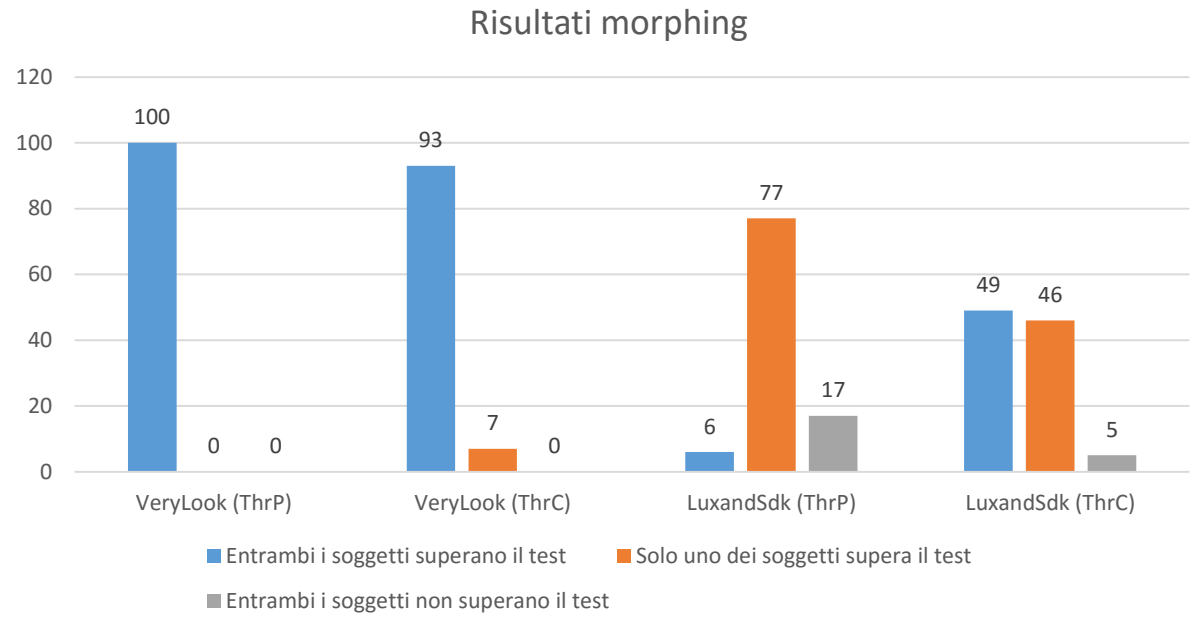


Figura 27 (Risultati Morphing)

L’algoritmo VeryLook con soglia indicata dal fornitore (ThrP) ha permesso di ottenere un successo in tutte e 100 le valutazioni con una percentuale del 100%. In questo caso ogni singola immagine morphed è da considerarsi in grado di ingannare un sistema di verifica dell’identità che utilizzi l’algoritmo di VeryLook con la soglia ThrP. Utilizzando la soglia calcolata (ThrC) invece, il numero di morphed che hanno superato il punteggio minimo scende a 93 garantendo comunque un ottimo risultato.

L’algoritmo LuxandSdk con limite indicato dal fornitore (ThrP) ha individuato 94 immagini su 100, permettendo solamente a 6 delle 100 coppie di superare la valutazione minima, mentre la restante parte è suddivisa tra “Solo uno dei soggetti supera il test” (77/100) e “Entrambi i soggetti non superano il test” (17/100).

I dati sono migliorati sensibilmente utilizzando la soglia calcolata (ThrC) in quanto 49 coppie di immagini test ha superato il punteggio minimo, mentre della restante parte solamente 3 coppie non hanno ottenuto il risultato minimo.

Come evidenziato dal grafico in Figura 27, l’utilizzo di un limite differente per l’algoritmo *VeryLook* non ha avuto conseguenze significative consentendo alla maggior parte dei campioni di superare il test, mentre solamente lo score ThrC ha garantito risultati sufficienti con l’algoritmo di LuxandSDK.

E’ evidente che in tutte e quattro le verifiche il numero di coppie campione in cui nessuno dei due soggetti supera il test è esiguo, mentre risulta abbastanza elevato il numero di casi in cui solamente uno dei due soggetti supera il test. Per questo motivo è stata effettuata un’ulteriore analisi sulla modalità di distribuzione del numero di campioni in cui solamente un soggetto supera il test.

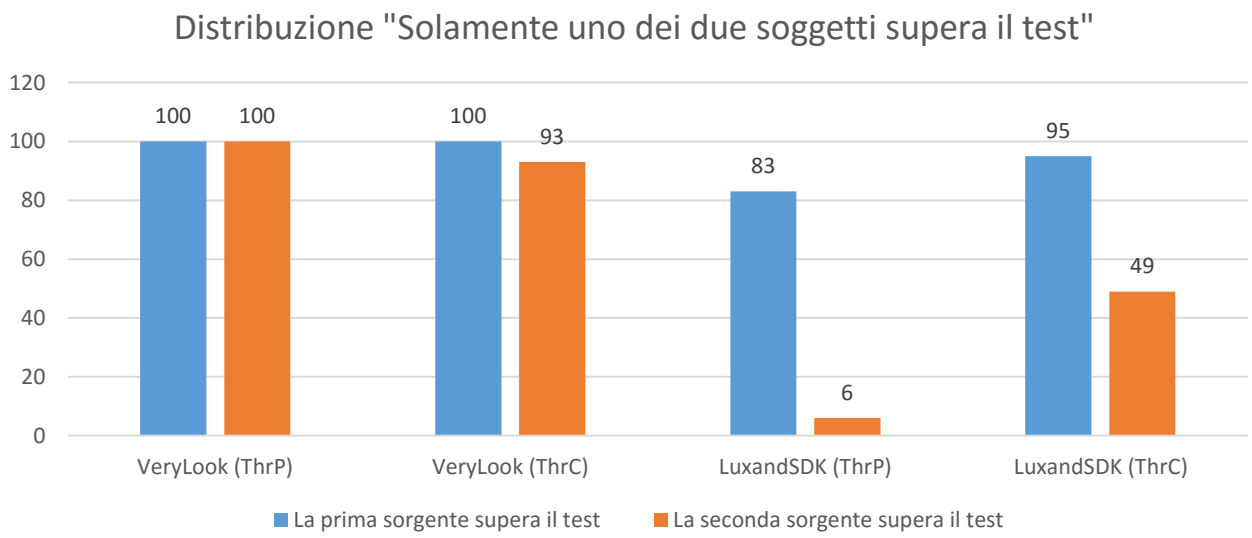


Figura 28

Come ci si poteva attendere in tutte e quattro le valutazioni, la prima sorgente supera facilmente il limite minimo, mentre il risultato della seconda sorgente è incostante.

La figura 27 mostra una forte presenza di campioni in cui solamente uno dei due soggetti supera il test ma non è chiaro come questi siano disposti. La figura 28 illustra come la distribuzione sia fortemente sbilanciata verso la prima sorgente. Questo indica che, in tutti i campioni in cui solamente uno dei due soggetti supera il test, è l'immagine principale (prima sorgente) a superare la valutazione.

Gli esiti ottenuti con l'algoritmo *VeryLook* rafforzano la tesi in cui è effettivamente possibile costruire un'immagine morphed in grado di ingannare strumenti automatici per la verifica dell'identità. In particolar modo la scelta di persone con tratti somatici simili garantisce score elevati con un minimo intervento di ritocco.

E' inoltre da notare che alcune immagini morphed generate non sono effettivamente applicabili al dominio del problema in quanto i soggetti di partenza hanno caratteristiche oltremodo dissimili. Il test 032_M (Figura 29) è un esempio particolarmente significativo in quanto le persone raffigurate nelle immagini sono talmente diverse da risultare appariscenti. In un caso reale è molto improbabile che i due soggetti in foto, vengano associati per la generazione di un'immagine morphed.

Figura 29 (Esempio di morphing non applicabile alla realtà)

Capitolo 6.
Conclusioni

I dati ottenuti dai test mostrano che il problema è reale ed occorre individuare contromisure.

I risultati garantiti dall'algoritmo *VeryLook* hanno evidenziato chiaramente come sia possibile generare immagini contraffatte in grado di ingannare i sistemi automatici di verifica dell'identità. Le soglie utilizzate con entrambi gli algoritmi sono state selezionate in modo tale da riprodurre le medesime condizioni presenti in situazioni reali.

VeryLook, con limite minimo indicato dal fornitore, ha permesso a tutte e 100 le immagini di test di superare la soglia minima, per cui ogni singola morphed è da ritenersi in grado di ingannare il sistema. Lo stesso strumento è stato in grado di discriminare sette immagini contraffatte quando è stata utilizzata una soglia ricalcolata, ottenendo un risultato comunque insufficiente a garantire un'affidabile identificazione di immagini morphed.

L'utilizzo dell'algoritmo LuxandSDK, con le soglie indicate dai fornitori (ThrP), ha portato all'individuazione di un numero soddisfacente di morphed. La verifica è stata superata solamente da sei immagini di test, mentre le restanti 77 sono state classificate come "solamente uno dei due soggetti supera il test". Di queste la totalità è appartenente alla prima sorgente, avvalorando la robustezza ed affidabilità del tool.

Utilizzando la soglia calcolata (ThrC) con il tool LuxandSDK sono state discriminate 51 coppie su 100, consentendo a 49 morphed di superare il test.

L'algoritmo VeryLook ha denotato una bassa propensione al riconoscimento delle immagini alterate ottenendo risultati significativamente contrastanti rispetto a

LuxandSDK. Allo stato attuale l'algoritmo non è in grado di individuare correttamente immagini reali e contraffatte, esponendosi pericolosamente a potenziali attacchi.

LuxandSDK 5.0 è quello che ha ottenuto risultati migliori durante tutto l'arco dei test discriminando 94 immagini morphed delle 100 sottoposte. Nonostante sia stato ingannato da 6 soggetti, ha denotato ottime potenzialità in grado di riconoscere la maggior parte delle fotografie contraffatte, anche quando la soglia minima è stata variata. Il 6% di morphed riconosciute non è ancora sufficiente a consigliarne un impiego in situazioni reali, ma il proseguo dello sviluppo potrebbe portare in breve tempo ad un incremento della robustezza ed affidabilità dell'algoritmo.

I risultati ottenuti indicano perciò che ingannare sistemi automatici di verifica dell'identità, tramite immagini morphed, è possibile ed alla portata di tutti.