Cahiers Lyonnais d'AnthropoBiométrique, 1, 2012 / Lyon-France ISSN 2260-0442

L'identification faciale du vivant

Raoul PERROT[123]

1 - Expert honoraire en Anthropologie d'Identification, Cour d'Appel de Lyon
2 - Laboratoire d'Anthropologie Anatomique et de Paléopathologie de Lyon
3 - Contact : PERROT.L2APLYON1@live.fr

Résumé :

A côté des techniques sophistiquées d'identification telles empreintes digitales, empreintes génétiques, examen de l'iris, voix, réseaux capillaires, etc.., l'identification la plus basique d'un individu vivant, se fait par reconnaissance faciale. Dans cet article l'Auteur passe en revue les techniques actuelles d'identification du visage allant de l'examen morphologique comparatif de photographies d'identité aux différentes méthodes anthropométriques et en particulier celle lyonnaise faisant appel à la biométrique de similarité. Les tentatives d'automatisation de l'identification sont également envisagées.

Mots-clés : identification faciale / vivant / méthodes actuelles / méthodes morphologiques comparatives de photographies d'identité / méthodes anthropométriques comparatives / biométrique de similarité / identification automatisée.

Abstract : **Facial identification of the alive person.**

Beside the sophisticated techniques of identification such digital fingerprints, genetic prints, examination of the iris, voices, networks of blood capillaries, etc. , the basic identification of an alive individual, is done by facial recognition. In this article the Author reviews the current techniques of identification of the face going from the comparative morphological examination of photographs to the various anthropometric methods and in particular that Lyons calling upon biometric similarity. The attempts at automation of the identification are also considered.

Key-words : identification of the face /alive person / current methods / comparative morphological methods of passport photographs/comparative anthropometric methods/biometric of similarity / automated identification.

1 - Introduction

Si on laisse de côté les techniques sophistiquées d'identification telles empreintes digitales, empreintes génétiques, examen de l'iris, voix, réseaux capillaires, etc.., l'identification la plus basique d'un individu, se fait en fonction du visage : en effet dès sa plus tendre enfance l'être humain est capable d'identifier une personne d'après ce dernier. On comprend donc facilement que les méthodologies d'identification par reconnaissance faciale soient les plus classiques : en effet pour tout un chacun le visage « *cristallise l'identité de l'individu* »[17].

La reconnaissance d'un visage est le fait d'une tierce personne ou d' une caméra vidéo de

surveillance. Dans les deux cas le processus est le même et, une reconnaissance positive implique obligatoirement :

- un « apprentissage » préalable entraînant une mémorisation des traits du sujet,
- une analyse du visage nouvellement vu, dont les données faciométriques sont comparées (par le cerveau ou par l'ordinateur) à celles mémorisées.

Ce qui peut se résumer par le schéma suivant :

Apprentissage ¬>Mémorisation ¬>Reconnaissance

En d'autres termes le cerveau humain (via l'œil et les aires psychovisuelles cérébrales) ou la caméra vidéo (via la base de données mémorisées dans l'ordinateur) ne pourront reconnaître que ce qu'ils connaissent déjà ! Le problème se pose donc lorsqu'il s'agit de la reconnaissance d'individus dont le visage ne correspond à aucune information déjà intégrée : c'est le cas de l'expert en anthropologie d'identification, dont la mission est d' identifier l'auteur d'un vol à main armée [VMA][1].

2 - Les techniques actuelles d'identification du visage

Les techniques d'identification faciale utilisées actuellement reposent toujours sur une analyse comparative de deux visages : le visage *candida*t [par exemple le prévenu dans une affaire de VMA] étant comparé au visage *référence*[par exemple l'auteur du VMA] en faisant appel à des critères morphologiques ou morphométriques voire les deux couplés. Les différentes méthodologies, de manuelles au début, essaient de s'orienter progressivement vers une automatisation qui, bien que de nombreux progrès dans le domaine aient été faits, demeurent complexes et encore peu maniables pour leur assurer la praticité qu'on est en droit d'attendre.

2.1 - L'examen comparatif de photographies du visage

Il représente la plus classique des méthodes d'identification d'un sujet [10-11-14-15], même si sa fiabilité est moins évidente que les empreintes digitales, mais ces dernières supposent l'intervention d'un spécialiste ce qui n'est pas le cas de photographies : tout fonctionnaire de police étant apte à comparer deux photographies [21]. En effet il est relativement simple de superposer la photographie du prévenu et celle de l'inconnu, mises à la même échelle. Ensuite est comparé l'éloignement plus ou moins grand des contours ce qui permet de déterminer la plus ou moins grande similarité entre les deux et la possibilité d'identifier l'inconnu comme étant le prévenu. Un certain nombre d'auteurs ont utilisé cette méthode [1-2-7-16-20-24]**.** Il est important de noter que parfois, l'utilisation d'un recalage non rigide (= *morphing*), permet de déformer l'image du prévenu pour la faire "coller" avec celle de l'auteur du VMA : ce qui entraîne le risque, non négligeable, de créer de fausses acceptations d'identification [2]!

La photographie d'identité est particulièrement devenue incontournable depuis l'attaque en

2001, des Twin Towers de New York et l'obligation depuis le 28 août 2006, pour les nationaux européens du passeport biométrique (e-passeport) pour entrer aux USA [a noter que depuis 2009 les empreintes digitales sont ajoutées à la photographie du visage]. Cette nécessité a généré de nombreux travaux de recherches dont le but est d'augmenter la qualité de la photographie du visage et son inviolabilité, afin de déjouer les inévitables tentatives de leurrage [4][3]

Les Pays Bas développent depuis les années 2004 une importante activité de recherche portant sur la biométrie du visage et sur les empreintes digitales dans le but de les associer au niveau du passeport biométrique [23]

En 2007 est mis en route le projet MBIoD (*Multimodal Biometrics for Identity Documents*) qui prend en compte tous les aspects de l'identification (empreintes digitales, iris, signature en ligne, voix et bien sur le visage). Pour ce dernier, il est recommandé, entre autre, dans le cas d'une acquisition 2D, de prendre cinq clichés de face avec une caméra haute définition, (Fuji Finepix S2 pro). Trois flashs sont également utilisés de manière à supprimer toute ombre portée. Par ailleurs seront strictement contrôlés : environnement de la photo du sujet, l'expression du visage, l'orientation de la tête, et l'éclairage ambiant [6]**.**

En 2008, une autre équipe démontrent que la distance idéale entre la caméra et le sujet pour obtenir une bonne photographie de passeport est 2m [26] **!** Cette conclusion nous agrée particulièrement, nous qui depuis de nombreuses années tentons, mais en vain, de démontrer que les caméras de surveillance des établissements bancaires sont situées trop loin et de plus, en contre plongée !

2.2 - L' identification automatique

L' utilisation de la biométrie couplée à des techniques informatiques entraîne tout logiquement à envisager la possibilité d'un traitement automatique des données, en particulier faciales [le système étant applicable également à l'iris et aux empreintes digitales, il pourra l'être dans un avenir relativement proche, à la voix, à la thermographie du corps, à la géographie veineuse de la main], conduisant à la possibilité d'identification de l'individu. L'identification faciale automatique est un axe de recherche emprunté par de nombreux auteurs [3-8-9-12-13-22-23].

Classiquement un système biométrique automatique comporte une unité d'acquisition des données (caméra, dans le cas du visage), un extracteur de celles jugées comme caractéristiques, un comparateur [les données sont comparées à celles mémorisées], une unité de décision dont le rôle est fondamental : elle doit, en effet, décider d'accepter ou pas, la personne sujet de l'analyse biométrique [20]. Il est évident que dans l'identification des auteurs de VMA, il n'existe pas de banque de données et le système devra s'adapter au coup par coup, en comparant les données acquises du criminel avec celles provenant du (ou des) prévenu(s) : ce verrou technologique justifie une plus grande difficulté pour automatiser le système. De nombreux auteurs travaillant dans le domaine de l'identification

automatique notent l'obligation de prendre en compte, non seulement, la position, la forme du visage par rapport au capteur, le port éventuel de lunettes ou d'une moustache mais également l'éclairage ambiant [13-23]. Par rapport aux trois plans de l'espace, la tête (et par conséquent le visage) représente en effet une forme complexe très difficile à définir en termes géométriques. Différentes tentatives ont essayé de contourner ce verrou anatomique depuis les années 70.

Les méthodes de reconnaissance automatique de la face peuvent être classées en trois groupes [22-23] :

- celles prenant en compte certains détails du visage (yeux, nez, bouche) dont l'emplacement et la géométrie sont utilisés pour la reconnaissance. Ces méthodes requièrent des images de haute résolution [22]
- celles *holistiques* prenant en compte la surface totale du visage : un bon résultat dépendant d'une position adéquate de la tête et de conditions normalisées pour l'éclairement,
- celles dites « combinées » car regroupant plusieurs approches [3-22].

Trois techniques méritent, en fonction de leur originalité, d'être détaillées :

- Des chercheurs japonais proposent une méthode d'identification basée sur une carte des lignes d'isodensité obtenue à partir des images faciales : la similarité entre deux visages est établie par la comparaison des lignes d'isodensité prises deux à deux. Les résultats obtenus sont prometteurs : 92,5% de discrimination correcte pour un pannel de 50 personnes [12]
- Des chercheurs espagnols utilisent une approche mathématique intéressante (que l'on retrouve d'ailleurs dans le domaine de l'anthropologie anatomique, en particulier dans la diagnose sexuelle du squelette) il s'agit de faire appel à une approche bayésienne proposant un cadre logique à l'analyse probabilistique des méthodes biométriques utilisées dans le domaine des sciences forensiques. Dans le cadre de l'identification faciale la méthodologie utilisée consiste à ne prendre en compte que la surface elliptique inscrivant les points remarquables du visage : iris, nez, bouche [9]
- Les chercheurs français (Telecom, Lille ; LIRIS-EC Lyon ; EURECOM, Sophia Antipolis ; THALES, Palaiseau) travaillent depuis de nombreuses années dans ce domaine. Lors du RFIA (Reconnaissance des Formes et Intelligence Artificielle) qui s'est tenu à Lyon du 24 au 27 janvier 2012, ils ont apporté une contribution fondamentale en démontrant l'importance d'une biométrie faciale 3D qui soit "robuste" aux déformations en associant plusieurs autres méthodologies (experts , matcheurs) à celle classique (qui est donc l'expert de référence) : l'algorithme de recalage rigide ICP. En prenant en compte en plus : les courbes radiales élastiques, une version étendue multi-échelle de l'opérateur LBP, l'algorithme de recalage non-rigide, le taux d'identification peut dépasser 99%! [3]

2.3 - L' anthropométrie

2.3.1 -Les méthodes développées à l'étranger

L' anthropologue anatomiste est habitué à pratiquer des calculs d'indice et de mesures angulaires à partir de points de référence repérés sur le squelette et, en particulier, sur le crâne. Si, de plus, il est expert judiciaire ces techniques vont tout naturellement être utilisées lors des demandes d' identification d'individus inconnus réduits à l'état squelettique. L'extension ultérieure se faisant vers l'identification de sujets vivants à partir de leur visage. Glenn Porter et Greg Doran ont développé une méthodologie anthropométrique différente car basée sur un agrandissement des photographies comparées, correspondant à un écartement interpupillaire de 6cm. A partir de là sont pris en compte, et comparées la largeur de la face entre les oreilles, la largeur du nez et de la bouche. Les mesures sont prises classiquement avec un pied à coulisse digital (descendant jusqu'à 0.05mm) sur les photographies. Par contre les auteurs n'abordent pas les critères retenus dans l'assimilation positive de deux visages comparées [21]

De son côté une équipe japonaise bien que partant de points de repères anthropométriques du visage (*nodes*) abandonne ensuite la réalité anatomique pour ne conserver que l'image géométrique : 30 points sont répartis sur le visage [obligatoirement de face] depuis la racines des cheveux jusqu'au contour du menton, en passant par les sourcils, les yeux, le nez et la bouche. Ces points sont ensuite reliés entre eux, formant ce que les auteurs appellent le *graphique facial* qui offre l'avantage d'être robuste aux variations lumineuses. Dans le cas d'une identification faciale ce sont donc les deux « face graph » qui vont donc être comparés. Les résultas obtenus peuvent être remarquables, les auteurs obtenant un taux de 99% [13]

L'anthropométrie est présente également dans la prise en compte des photos destinées aux passeports. C'est le cas d'une équipe allemande [26] qui testant la meilleure distance (allant de 1m à 5 m) pour obtenir la meilleure photo d'identité, a comparé la photographie de la même personne prise aux cinq distances déjà indiquées : 34 indices anthropométriques faisant intervenir les paramètres classiques du visage tels hauteur faciale, largeur bizygomatique, largeur du nez et de la bouche, etc…ont donc été utilisés. La comparaison des valeurs obtenues montre que la meilleure identification est obtenue pour la photographie prise à 2m, preuve s'il en était besoin que les caméras de surveillance des établissements bancaires sont situées trop loin et de plus, en contre plongée !

2.3.2 - La méthode lyonnaise : la biométrique de similarité

Depuis les années 1990, à la suite de demandes répétées des autorités judiciaires dans le domaine de l'identification des auteurs de VMA, nous avons développé dans le cadre du L2AP une méthode manuelle de comparaison biométrique de plans fixes provenant de la vidéo avec des photographies du (ou des) prévenu(s). Elle consiste, à prendre des **points**

anatomiques dont la **position** et le **nombre ne sont pas prédéfinis** : en effet **ils sont entièrement tributaires de la qualité (nombre de pixels et orientation)** du cliché de l'auteur du VMA, **et sont donc adaptés à chaque cas** [ce qui est un avantage indéniable par rapport à certaines méthodes d'analyse anthropométrique, qui ne satisfont pas toujours leurs auteurs qui s'en tiennent à une série de points immuables, qui peuvent ne pas être utilisables si l'orientation de la photographie de l'auteur du VAM ne permet pas de les prendre][15]. La méthodologie utilisée dite "*BIOMETRIQUE DE SIMILARITE*" consiste à comparer deux à deux des photographies des visages **A** et **B** : le but étant de déterminer si le visage **B** est **A**. Sur chaque cliché est établi un descripteur local correspondant à une signature invariante utilisant des points anatomiques qui reliés entre - eux fournissent des paramètres, des indices et des valeurs angulaires. Il est important de noter que n'est jamais prise en compte la comparaison des valeurs brutes d'un même paramètre sur les deux clichés mais celle des *invariants géométriques* [*rapports indiciaires* confrontant les paramètres deux à deux (formule générale d'un indice : paramètre 1 x 100 / paramètre 2) , *valeurs angulaires*) **ce qui offre l'avantage considérable de pouvoir travailler sur des instantanés n'étant pas à la même échelle** [5-19]!

La ressemblance (ou *similarité*) entre **B** et **A** va être établie en prenant en compte la différence algébrique des valeurs indiciaires (ou angulaires), selon la modalité suivante :

- la valeur sera positive (+) si la valeur indiciaire (ou angulaire) de **B** est supérieure à celle de **A**,
- la valeur sera négative (-) si la valeur indiciaire (ou angulaire) de **B** est inférieure à celle de **A**.

Ensuite la somme algébrique de l'ensemble des intervalles indiciaires et angulaires est calculée puis divisée par le nombre (N) d'indices et de valeurs angulaires pris en compte : le résultat ainsi obtenu (qui est donc une moyenne algébrique) représente le *score de similarité* qui varie de 0 à 10. A chaque score est attribué un *% d'assimilation (= ressemblance) des deux visages* (tableau, p.7) :

- pour un score de 0, le % d'assimilation des deux visages est de 100%. Les deux visages présentent donc 100% de similitude ce qui permet de conclure que **B est manifestement A,**
- pour un score de 1, le % d'assimilation des deux visages est de 90%. Les deux visages présentent donc 90% de similitude ce qui permet de conclure **qu'il existe une forte probabilité que B puisse être A ,**
- à l'opposé pour un score de 10, le % d'assimilation des deux visages est de 0% ! Les deux visages ne présentent aucune similitude ce qui permet de conclure que **B n'est manifestement pas A.**
- à noter que, très logiquement, l'augmentation de la moyenne algébrique est inversement proportionnelle à la ressemblance (assimilation positive) : pour une moyenne algébrique de 2, le % de ressemblance tombe à 80, pour une moyenne

algébrique de 3, le % de ressemblance tombe à 70 et ainsi de suite.

Tableau - Score de similarité et % d'assimilation pris en compte dans la comparaison

Score	%	Score	%	Score	%	Score	%	Score	%	Score	%
0	100	1.7	83	3.4	66	5.1	49	6.8	32	8.5	15
0.1	99	1.8	82	3.5	65	5.2	48	6.9	31	8.6	14
0.2	98	1.9	81	3.6	64	5.3	47	7	30	8.7	13
0.3	97	2	80	3.7	63	5.4	46	7.1	29	8.8	12
0.4	96	2.1	79	3.8	62	5.5	45	7.2	28	8.9	11
0.5	95	2.2	78	3.9	61	5.6	44	7.3	27	9	10
0.6	94	2.3	77	4	60	5.7	43	7.4	26	9.1	9
0.7	93	2.4	76	4.1	59	5.8	42	7.5	25	9.2	8
0.8	92	2.5	75	4.2	58	5.9	41	7.6	24	9.3	7
0.9	91	2.6	74	4.3	57	6	40	7.7	23	9.4	6
1	90	2.7	73	4.4	56	6.1	39	7.8	22	9.5	5
1.1	89	2.8	72	4.5	55	6.2	38	7.9	21	9.6	4
1.2	88	2.9	71	4.6	54	6.3	37	8	20	9.7	3
1.3	87	3	70	4.7	53	6.4	36	8.1	19	9.8.	2
1.4	86	3.1	69	4.8	52	6.5	35	8.2	18	9.9	1
1.5	85	3.2	68	4.9	51	6.6	34	8.3	17	10	0
1.6	84	3.3	67	5	50	6.7	33	8.4	16		

Pour conclure il convient de distinguer deux paradigmes, à savoir l'***identification*** et *l'**authentification** :*

- la première (domaine de l'expertise biométrique effectuée par le LA2P) propose une identité : la probabilité que le prévenu soit l'auteur du VMA est de tant de %,
- la seconde (domaine des autorités judiciaires) va confirmer cette identité : le prévenu EST l'auteur du VMA

Il est bon de noter que la comparaison prend en compte également des caractères morphologiques, qui, bien que non quantifiables, vont apporter un complément d'information non négligeable.

3 - Conclusion

Les techniques d'identification faciale utilisées actuellement reposant sur une analyse comparative de deux visages représentent la plus classique des méthodes d'identification d'un

sujet, même si leur fiabilité est moins évidente que les empreintes digitales, mais ces dernières supposent l'intervention d'un spécialiste ce qui n'est pas le cas de photographies : tout fonctionnaire de police étant apte à comparer deux photographies. En effet il est relativement simple de superposer la photographie du prévenu et celle de l'inconnu, mises à la même échelle, afin de les comparer. La photographie d'identité est particulièrement devenue incontournable depuis l'attaque en 2001, des Twin Towers de New York avec l'obligation depuis le 28 août 2006, pour les nationaux européens du passeport biométrique (e-passeport) pour entrer aux USA. Cette nécessité a généré de nombreux travaux de recherches dont le but est d'augmenter la qualité de la photographie du visage et son inviolabilité, afin de déjouer les inévitables tentatives de leurrage. En 2007 est mis en route le projet MBIoD (*Multimodal Biometrics for Identity Documents*) qui prend en compte tous les aspects de l'identification (empreintes digitales, iris, signature en ligne, voix et bien sur le visage). Pour ce dernier, il est recommandé, entre autre, dans le cas d'une acquisition 2D, de prendre 5 clichés de face avec une caméra haute définition. Par ailleurs sont également contrôlés : environnement de la photo du sujet, l'expression du visage, l'orientation de la tête, et l'éclairage ambiant **.**

L' utilisation de la biométrie couplée à des techniques informatiques entraîne tout logiquement à envisager la possibilité d'un traitement automatique des données, en particulier faciales [le système étant applicable également à l'iris et aux empreintes digitales, il pourra l'être dans un avenir relativement proche, à la voix, à la thermographie du corps, à la géographie veineuse de la main], conduisant à la possibilité d'identification de l'individu.

L'identification faciale automatique est un axe de recherche emprunté par de nombreux auteurs : classiquement un système biométrique automatique comporte une unité d'acquisition des données (caméra, dans le cas du visage), un extracteur de celles jugées comme caractéristiques, un comparateur [les données sont comparées à celles mémorisées], une unité de décision dont le rôle est fondamental : elle doit, en effet, décider d'accepter ou pas, la personne sujet de l'analyse biométrique. Il est évident que dans l'identification des auteurs de VMA, il n'existe pas de banque de données et le système devra s'adapter au coup par coup, en comparant les données acquises du criminel avec celles provenant du (ou des) prévenu(s) : ce verrou technologique justifie une plus grande difficulté pour automatiser le système. C'est pour cette dernière raison que nous parait particulièrement utilisable et fiable (de nombreuses expertises l'ayant démontré)l'appel à la biométrique de similarité, méthodologie développée par l'Auteur dans le cadre du Laboratoire d'Anthropologie de Lyon depuis une vingtaine d'années. L'étape ultérieure pour laquelle plusieurs tentatives ont déjà été effectuées[4] sera d'intégrer cette méthodologie dans un processus mi manuel /mi automatique. En effet il ne nous parait pas souhaitable de laisser à une machine la décision finale de dire si le prévenu est ou n'est pas responsable du VMA!

Notes

1 - Il en est de même lors de l'identification faciale d'un squelette ou d'un portrait peint. A ce sujet cf. : *CLAB /* 2012 / Editorial

2- Nous avons personnellement été confronté à ce cas lors d'une contre - expertise de VMA. Dans un premier temps le prévenu avait été reconnu responsable suite aux conclusions d'un expert photographe. Cependant des doutes subsistaient d'où l'appel à deux contre-expertises :

- la première utilisant justement, ce que nous critiquons, à savoir super-imposition et morphing, allait dans le sens de l'expertise initiale
- la seconde - la notre - utilisant la méthodologie de biométrique de similarité (cf. plus haut § 2.3.2) démontra les erreurs commises dans des expertises basées sur la seule morphologie, en particulier le tout-premier expert ayant assimilé une vue de 3/4 avec une vue de profil.

En conclusion signalons qu'après notre intervention, le prévenu n'était finalement plus retenu comme auteur du VMA dont il avait été accusé!

3 - Le réseau de vidéosurveillance qui enregistre l'identité dématérialisée de l'individu et son acte (vol à main armée), est l'un des éléments centraux du dispositif global d'identification. Autre élément central est la procédure d'identification de l'expert basée sur sa double analyse anthropomorphique et anthropométrique. L'expert suit une démarche minutieuse et difficile en raison des éléments matériels (photo du délit/crime et des suspects) souvent de mauvaise qualité avec des variabilités [conditions d'éclairage, angle de vue, sans oublier les tentatives de dissimulation des traits du visage (capuche, chapeau, bonnet de marin, perruque, foulard, lunettes, faux nez, fausse barbe, etc…] effectuées par le contrevenant qui se sait filmer par la caméra : les photographies (cf. page suivante) proposent quatre exemples de tentative de dissimulation des traits du visage.

4 - Depuis quelques années un partenariat a été développé entre notre laboratoire et le Laboratoire d'InfoRmatique en Image et Systèmes d'information (LIRIS/ECL) du Pr. Liming Chen. A noter que trois projets présentés conjointement par les deux labos n'ont malheureusement par été retenus (ANR IDASOR 2008/ ANR VIDOC 2009/ Projet HERMES 2010-2011 pour le Grand Emprunt).

Bibliographie :

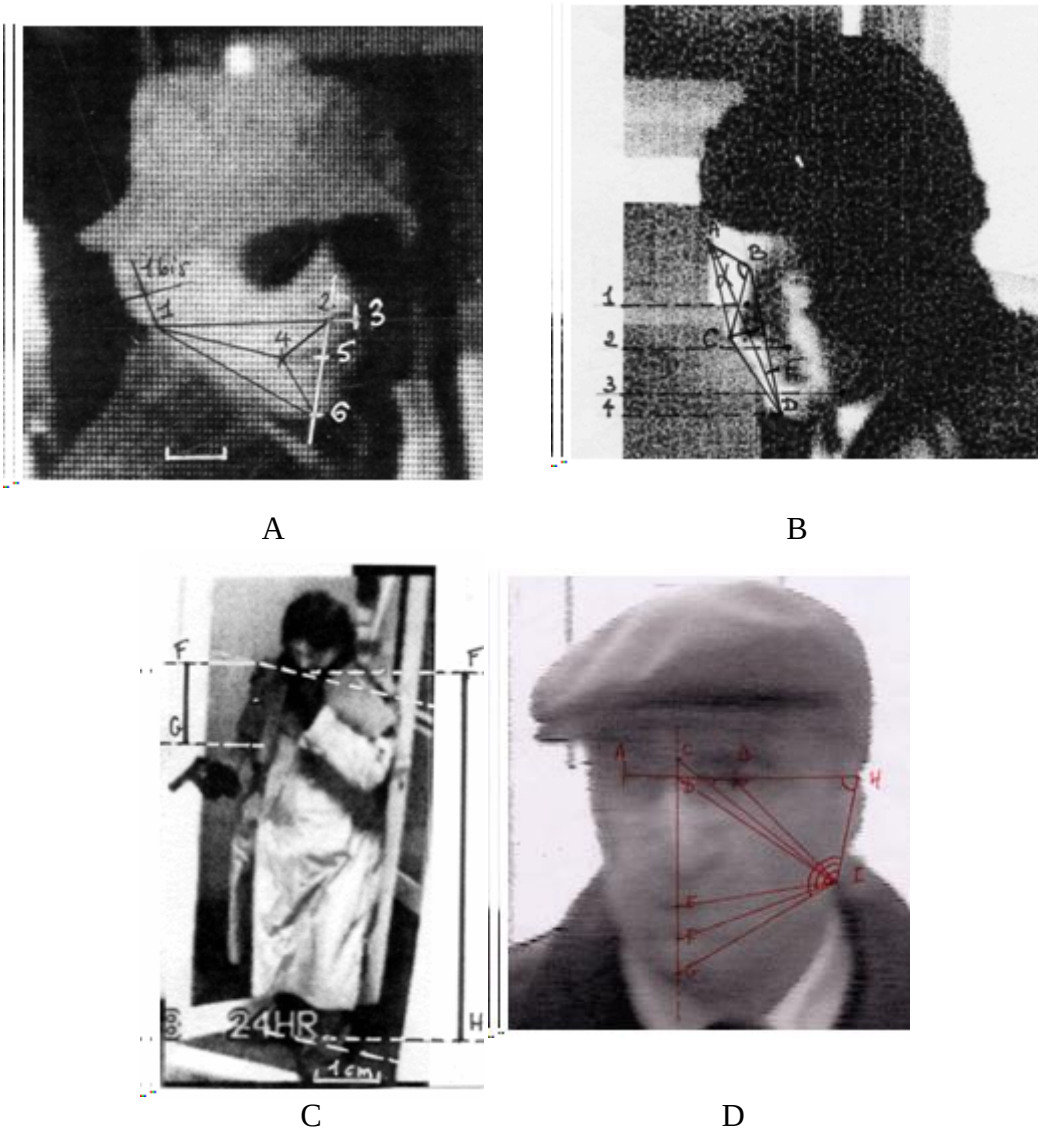
[1] Aulsebrook WA, Iscan MY, Slabbert JH & Becker P, 1995.Superimposition and reconstruction in forensic facial identification : a survey. *Forensic Sci Int*, 75 :101-120.

[2] Austin-Smith D, 1999.Video superimposition at the C.A. Pound Laboratory 1987 to 1992. *J Forensic Sci,* 44,4 (abstract).

[3] Ben Amor B., Drira H., Daoudi M., Ardabilian M., Ben Soltana W., Lemaire P., Chen L., Erdogmus N., Dugelay JL. & Colineau, 2012. Fusion d'Experts pour une Biométrie Faciale 3D Robuste aux Déformations. *Reconnaissance des Formes et Intelligence Artificielle (RFIA)*, Lyon 24/27 janvier 2012

[4] Biometrics and Identity Fraud, Biometric Technology Today (February 2008) 7-11. [http://www.biometricgroup.com/]

[5] Desbois Y. & Perrot R., 2008. Une méthode de vidéo-photo comparaison développée au laboratoire d'Anthropologie Anatomique de Lyon1 et appliquée à l'identification des auteurs de vol à main armée. A propos d'un cas.*Biom.Hum.et Anthropol.* 26, 1-2,63-67 [Texte de la communication faite à Paris, en novembre 2007, au colloque de la Société de Biologie Humaine *"Identification et authentification des personnes "*].



Quatre exemples de tentative de leurrage : bob et lunettes (A), bonnet de marin (B), perruque et foulard (C), casquette et bas de soie (D). On constatera, au passage, la piètre qualité des images 2D fournies par les caméras de surveillance!

[6] Dessimoz D, Richiardi J, Champod Ch & Drygajlo A, 2007. Multimodal Biometrics for Identity Documents (MbiOD), *Forensic Sc. Int.* 167, 154-159.

[7] Dorin RBJ,1983 . Photographic superimposition. *J Forensic Sci* , 28:724-734.

[8] Everingham M & Zisserman A, 2005 . Automated detection and identification of persons

in video using a coarse 3D head model and multiple texture maps. *Vision, Image and Signal Processing, IEE Proceedings*, 152, 6 :902-910.

[9] Gonzales-Rodriguez J, Fierrez-Aguilar J, Ramos-Castro D & Ortega-Aguilar J, 2005. Bayesian Analysis of Fingerprint, Face and Signature Evidences with Automatic Biometric Systems, *Forensic Sc. Int*. 155, 126-140.

[10] Goos MIM, Alberink IV & Ruifrok ACC, 2006. 2D/3D image (facial) comparison using camera matching. *Forensic Sc Int*, 163 :10-17.

[11] Halberstein RA, 2001. The application of anthropometric indices in forensic photography : three cases studies. *J Forensic Sc*, 46,6 (abstract).

[12] Hirano T, Ikeda M & Nakamura O, 2003. Facial Identification System Based on a High-Speed Matching Algorithm for Isodensity Lines, *Electrical Engineering in Japan*, 143, 4, 31-41.

[13] Hirayama T, Iwai Y & Yachida M, 2007. integration of facial position estimation and person identification for face authentification, *Systems and Computers in Japan*, 38, 5, 276-290.

[14] Iscan MY . Introduction of techniques for photographic comparison : potential and problems. in Iscan MY and Helmer RP, 1993. *Forensic Analysis of the Skull. Craniofacial Analysis, Reconstruction, and Identification* .Wiley-Liss,pp.57-70.

[15] Kleinberg KF, Vanezis P & Burton AM, 2007. Failure of anthropometry as a facial identification technique using high-quality photographs. *J Forensic Sci* .,52(4):779-83.

[16]]Koelmeyer TD, 1982 . Videocamera superimposition and facial reconstruction as an aid to identification. *Am J Forensic Med Pathol*, 3,45.

[17] Le Breton D & Grosbois Ph, 1993 . Le visage, symbole de notre identité. *Le journal des Psychologu*es, n° 105 :14-18.

[18] Luis-Garcia R de, Alberola-Lopez C, Aghzout O & Ruiz-Alzola J, 2003. Biometric Identification Systems, *Signal Processing*, 83, 2339-2557.

[19] Perrot R, 1996. Use of anthropological methods in the identification of unknown individuals.*14 th Meeting of the International Association of Forensic Sciences*, Tokyo, Japan

[20] Pesce Delfino V, Colonna M, Potente E, Vacca E & Introna F Jr (1986). Computer aided skull-face superimposition. *Am J Forensic Med Pathol*, VII,201.

[21] Porter G & Doran G, 2000.An Anatanomical and Photographic Technique for Forensic Facial Identification, *Forensic Sc Int*, 114, 97-105

[22] Schouten B & Jacobs B,2009 . Biometrics and Their Use in e-passports, *Image and Vision Computing*, 27, 305-312.

[23] Sumi Y & Ohta Y, 1996 .Human Face Analysis Based on Distributed Two-Dimensional

Appearance Models, *Systems and Computers in Japan*, 27, 7, 97-108.

[24] Vanezis P & Brierkey C, 1996. Facial image comparison of crime suspects using video superimposition. *J Forensic Sci Soc*, 36:27-33.

[25] Ventura F, Zacheo A, Ventura A & Pala A, 2004. Computerised anthropomorphometric analysis of images : case report. *Forensic Sc Int*, 146S :S211-S213.

[26] Verhoff M A, Witzel C, Kreutz K & Ramsthaler F, 2008.The Ideal Subject Distance for Passport Pictures, *Forensic Sc. Int.* 178, 153-156.