Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.889 – 894

RESEARCH ARTICLE

A Multi View Face Recognizer for Authentication

Dr. C.Immaculate Mary[1], S.V.Rashyaa Verma[2], A.Jensila Smile[3]

[1]Associate Professor, Department of Computer Science,
Sri Sarada College for Women (Autonomous) Salem, India
[23]Lecturer, Department of Computer Science,
Sri Sarada College for Women (Autonomous) Salem, India
cimmaculatemary@gmail.com [1], rashyagayu@gmail.com [2]

Abstract— One emerging technology that is becoming more spread in a variety of organizations is biometrics. The term `biometrics' comes from the Greek words bios (Life) and metrikos (Measure).To make a personal recognition, biometrics relies on who you are or what you do--as opposed to what you know (such as password) or what you have (such as ID card).Biometric systems, which use people's physiological characteristics for identification or authentication, have become increasingly popular for countering fraud.

Biometrics offers greater security and convenience than traditional methods of personal recognition. Biometrics is used for many applications inside and outside the scope of computer security. In some applications, biometrics can replace or supplement the existing technology. In this paper, we describe a face recognition system that uses a new distance measure (Significance-based Multi View Hausdorff Distance) for authentication. It performs matching on a fusion of multiple views of each person's face. We have also analysed the performance of the system and listed out the areas where it can be applied.

Keywords— Biometric, Hausdorff Distance, Matlab

I. INTRODUCTION

Traditional person recognition methods do not meet today's needs. So, the need increases for fast, accurate, and user friendly automatic person recognition systems, ones that don't need human attention. In recent years, biometrics has gained importance as a research area. In this paper, we focus on face recognition – one of the least intrusive forms. To select the right biometric for our situation, we will need to navigate through some complex vendor products and keep an eye on future developments in technology and standards. In this paper, we have described a face recognition system that uses a new distance measure (Significance-based Multi View Hausdorff Distance) for authentication.

To improve system robustness, others have developed multimodal approaches that fuse together different biometrics. However, we believe optimizing a single-modal system minimize deployment costs and could benefit an multimodal system. We can improve a face recognition system's robustness by taking multiple views of a person's face at different angles using essentially the same equipment as frontal only analysis. Here, we have developed a multi view face recognizer for authentication that meets the following design objectives.

- Robust against variations. Operates under different conditions and applies to a high percentage of population.
- Cost effective. Incurs minimal deployment costs.
- Accurate and reliable. Has excellent performance distinguishing people and excellent EER performance.
- User-friendly. Is nonintrusive and fast.

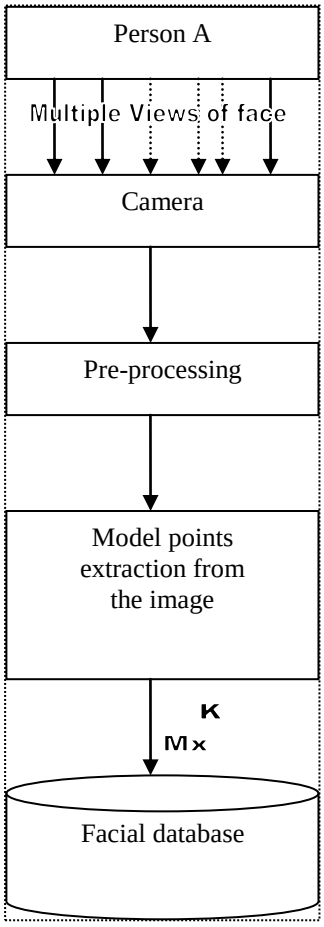
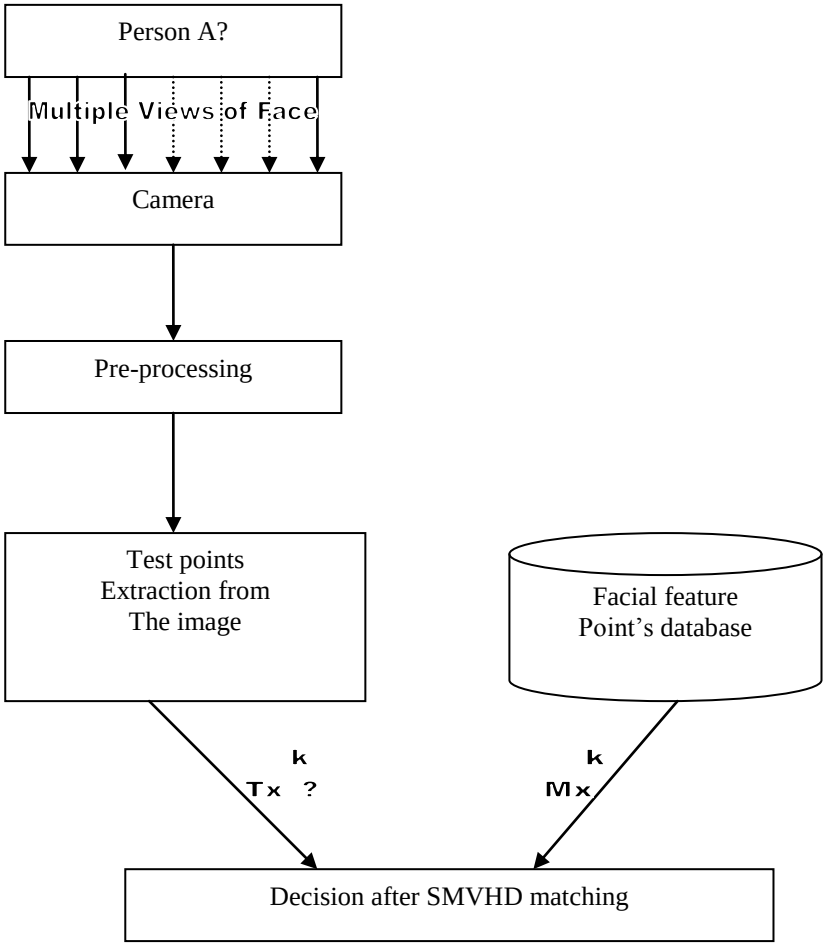


Fig 1. OVERVIEW OF OUR SYSTEM (a) Enrolment

As shown in the figure, we capture multi views of person X's face during enrolment. Pre-processing is done to reduce the effect of hair and clothing. We store the extracted model points in a database. We target our solution towards the authentication of the users who are willing to have an enrolment process capture images of their

faces. These captured images form a knowledge base used for subsequent authentication by comparing person X's stored image with the image of a person claiming to be X.

In the normal face recognition procedures, all Hausdorff Distance (**HD**) variants do not address each point's unequal contribution. In practice, each point's prominence in representing a facial image will likely be different. In this paper, we apply a new HD variant — Significance-based Multi View Hausdorff Distance (**SMVHD**). This considerably improves the authentication process's robustness even with the introduction of non- rigid distortions to the facial image, such as when a person speaks.



(b) Authentication (Fused Multi view Analysis)

II. SIGNIFICANCE-BASED MULTI VIEW HAUSDROFF DISTANCE (SMVHD)

Suppose a set of feature vectors(nodes)**NA**, or model points, represents an image **A** and another set **NB**, or test points, represents image **B**. Traditional methods that assign the same weight to all points in **NA** and **NB** clearly lead to suboptimal results because different feature points contribute differently toward an overall face description. Here, we apply a new variant of Hausdorff distance.

SMVHD differs from other **HD** variants in two ways.

- First, we apply the notion of significance associated with each point.
- Second, we fuse together multiple views of same non-rigid object (the face) taken from different viewpoints.

Using Multiview images for facial analysis is not entirely new. However, those methods which rely on neural network technology might account for a relatively long computational time.

Let us consider

$$\mathbf{M}^{1} = \{m1^{1}, m2^{1}, \ldots\ldots, mp1^{1}\},$$

$$\mathbf{M}^{2} = \{m1^{2}, m2^{2}, \ldots\ldots, mp2^{2}\}, \ldots\ldots\ldots,$$

$$\mathbf{M}^{n} = \{m1^{n}, m2^{n}, \ldots\ldots, mpn^{n}\}$$

are n point sets representing the features in object M's n model views and

$$\mathbf{T}^{1} = \{t1^{1}, t2^{1}, \ldots\ldots, tq1^{1}\},$$

$$\mathbf{T}^{2} = \{t1^{2}, t2^{2}, \ldots\ldots, tq2^{2}\}, \ldots\ldots\ldots,$$

$$\mathbf{T}^{n} = \{t1^{n}, t2^{n}, \ldots\ldots, tqn^{n}\}$$

Are the corresponding n point sets representing the features in test object **T**'s n views from the same viewpoints as in the model **M**. In this formulation, $p_1, p_2, \ldots\ldots, p_n$ and $q_1, q_2, \ldots\ldots, q_n$ are the point numbers, which are used for indexing, in the model and test views. So, we must let only the ith point in the kth view point $t_i^k \in \mathbf{T}^k$ match with the points in **M** , the kth view of **M**.

Let us define **SMVHD** between **M** and **T** as

H**SMVHD** (**M,T**) =max(h**SMVHD**(**M,T**),h**SMVHD**(**T,M**)).

In turn, we define the directed **SMVHD** from **M** to **T** and from **T** to **M** as

$$h_{SMVHD}(\mathbf{M},\mathbf{T}) = \left(1/\sum_{k=1}^{n} \sum_{m^k_i \in \mathbf{M}^k} \mathbf{Sig}\, m^k_i\ t^k_j\right) * \left(\sum_{k=1}^{n} \sum_{m^k_i \in \mathbf{M}^k} \mathbf{Sig}\, m^k_i\ t^k_j . \min_{t^k_j \in \mathbf{T}^k} \| m^k_i - t^k_j \|\right)$$

$$h_{SMVHD}(\mathbf{T},\mathbf{M}) = \left(1/\sum_{k=1}^{n} \sum_{t^k_i \in \mathbf{T}^k} \mathbf{Sig}\, t^k_i\ m^k_j\right) * \left(\sum_{k=1}^{n} \sum_{t^k_i \in \mathbf{T}^k} \mathbf{Sig}\, t^k_i\ m^k_j . \min_{m^k_j \in \mathbf{M}^k} \| t^k_i - m^k_j \|\right)$$

where, $\mathbf{Sig}\, m^k i\ t^k j = (1/2)*(\mathbf{Sig}\, m^k i + \mathbf{Sig}\, t^k j)$ is the average significance(within the range 0…….. ∞) of point m_i^K and its corresponding point t_j^k.

It selects them in three steps.

- First, it eliminates points with small merit, as compared to their neighbours.
- Next, it reinstates a number of points to avoid over elimination. It chooses the points from any points not covered by a strip selected in the first step.
- Finally, it deletes points that align approximately on a straight line, except for the curve's two endpoints.
- The remaining points are the feature points extracted.

III. PERFORMANCE ANALYSIS

Here, we analyze our system's performance by comparing MHD and SMVHD . Table below summarizes the results.

	MHD		SMVHD	
Expression	**Frontal view (%)**	**Three-quarter view (%)**	**Profile view (%)**	**All views(fused) (%)**
Neutral	96.5	96.0	90.0	100.0
Smiling	71.1	80.5	64.5	93.6
Speaking	87.1	80.6	58.1	93.5

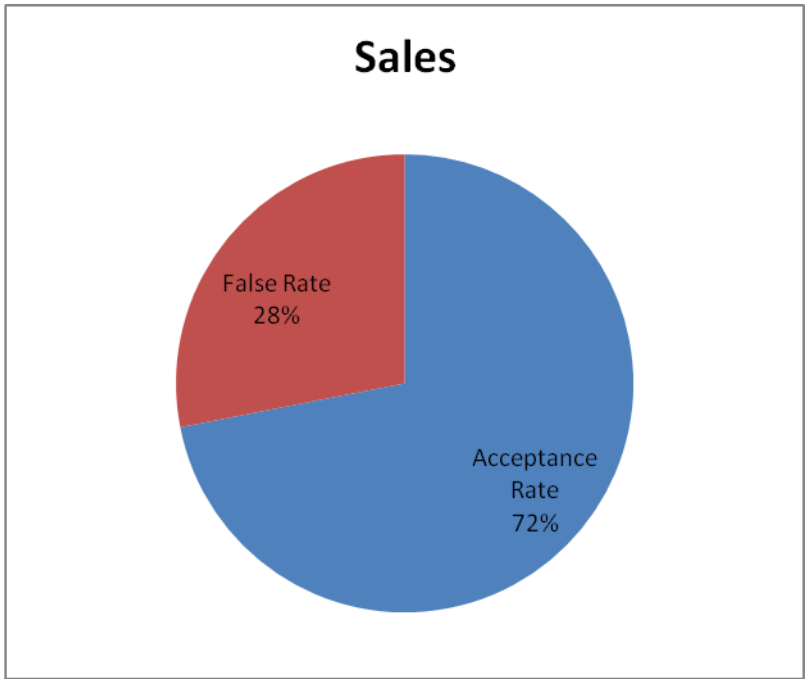
ACCURACY (in %)

Our results show that SMVHD performs significantly better than MHD in terms of accuracy. The average computational time per person was also found to be very low.

A. *Experimental Protocol*

In addition to the above analysis, we aimed to measure the authentication performance using a "leave-one-out and rotation" scheme. Our experimental protocol follows.

We perform enrolment process by capturing the multiple views of many persons (say 100 persons).



Then we must conduct authentication process. For this, we must label a person as an imposter with others acting as clients . The number of times that each imposter gained access under someone else's identity contributed to the FAR. The clients also tried to gain access under their own identity, contributing to the FRR. The figure shown above gives the ROC plot for the system. Even with non-rigid distortions caused by speaking during authentication, the EER was still reasonably good.

B. *Applications*

- ***Commercial applications***, such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit cards, physical access control, cellular phones, PDAs, medical records management, and distance learning;
- ***Government applications*** such as national ID cards, correctional facilities, driver's licenses, social security, border control, passport control, and welfare-disbursement; and
- ***Forensic applications*** such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

IV. CONCLUSIONS

Thus the process of designing a multiview face recognition system for authentication was done successfully and effectively. Furthermore, we have decided to fine tune our algorithm to increase the system's stability. Really speaking, biometrics has built a formidable security barrier for the world. It has indeed integrated itself into humanity and it will continue to do so hopefully.

REFERENCES

[1] L.Wiskott et al . , *"Face recognition By elastic bunch graph matching*", IEEE Trans .PAMI,july 1997.
[2] M.K.H.Leung and Y.H.Yang. ,"*Dynamic two-strip algorithm in curve fitting*", Pattern recognition, feb 1990.
[3] S.Pankanti, R.M.Bolle, and A.Jain, "*Biometrics: Personal identification in networked security,"* Kluwer Academic Publishers, 1999.
[4] E.Newham, "*The Biometric Report,* tech report", SBJ Services, 1995.
[5] John.D.Jr.Woodward, Christopher Horn, "Biometrics: A Look at Facial Recognition".

