Error exponent analysis of person identification based on fusion of dependent/independent modalities

Oleksiy Koval, Sviatoslav Voloshynovskiy, and Thierry Pun*

ABSTRACT

In this paper we analyze performance limits of multimodal biometric identification systems. We consider impact of the inter-modal dependencies on the attainable probabilities of error and demonstrate that an expected performance gain from fusion of dependent modalities is significantly higher than in the case when one fuses independent signals. Finally, in order to demonstrate the efficiency of dependent modality fusion, we perform the problem analysis in the Gaussian formulation and show the performance enhancement versus the independent case.

1. INTRODUCTION

Establishing of the person identity has become a crucial requirement of our modern society. Access to various services, facilities and infrastructers is granted based on the answers to the following questions: "Is the person really who he/she claims to be?," "Is this person authorized to use this facility?," or "Is he/she in the watchlist posted by the government?" that are habitually posed in multiple everyday scenarios. Evidently, in order to ensure that an impostor or illegal user will be able to fool the control procedure, person identification systems should be introduced that satisfies challenging simultaneous requirements to the verification security and reliability in constantly developing and improving modern communications infrastructure including mobile communication networks.[1]

Definitely, classical person identification techniques that are based on what the person knows (password/pin/key) or on what the person possesses (passport/ID card) cannot in a complete scale satisfy the mentioned requirements especially with respect to security. The posibility that the possessed person identification documents can be stolen or lost and the secure access data can be forgotten, guessed or maliciously intercepted open a wide secure hole for their illegal misuse.[2,3]

That is why modern person identification is performed based on biometrics, which refer to unique physiological or behavioral characteristics, i.e., to "something what you are or you do".[4] The kinds of biometric data that is used for person identification include face, fingerprint, iris, DNA, voice sample, signature, hand geometry, keystroke, etc. Since every individual has a unique set of biometric features, they cannot be stolen or forgotten, they are very hard to distribute, copy and share, the security concern of identification systems exploiting these data is significantly relaxed versus traditional identification systems.

Depending on a particular identification protocol requirements, various instances of biometric traits can be used.[4] A decision about the use of a particular underlying biometric feature is usually made based on the level of its "universality (do all people have it?), distinctiveness (can people be distinguished based on an identifier?), permanence (how permanent are the identifiers?), and collectable (how well can the identifiers be captured and quantified?), performance (matching speed and accuracy), acceptability (willingness of people to accept), and circumvention (foolproof)".[5] Unfortunately, there is no biometric feature that meets all requirements. Every biometric has strong and weak points with respect to the presented factors. Identification performance that can be attained based on a particular biometric features is one of the most important among them. It was shown that every biometric has a theoretical upper bound in terms of its ability to distinguish individuals. For instance, hand geometry and face biometrics can be used to reliably distinguish 10^5 and 10^3 instances, respectively.[6] Fingerprints are justified to have a very high matching accuracy,[7] however their permanence for people who are doing some manual job is questionable as well as collectability, since a high quality fingerprint can be obtained not for everyone.[8]

©O. Koval, S. Voloshynovskiy, and T. Pun are with CUI-University of Geneva, Stochastic Image Processing Group, 24 rue General-Dufour, 1211 Geneva, Switzerland. The contact author is S. Voloshynovskiy (email: svolos@cui.unige.ch). http://sip.unige.ch

As a natural solution to overcome shortcomings of particular biometrics non-optimality, multibiometric systems were proposed[9–11] that are attempting to benefit in terms of achieved performance from the presence of several biometric modalities or multibiometrics. Fusion of multibiometrics can be performed on various structural levels of an identification system[5]: sensor level, feature level, match score level, rank level and decision level. Due to the data processing inequality,[12] expected performance improvement will be the highest if fusion is performed on the sensor level and will not be necessarily monotonically decreasing to the decision level. Usually it is very difficult to apply on practice due to various technological aspects. That is why very few results are known today demonstrating the efficiency of such systems.[13] Mostly, the fusion in practical multibiometric person identification systems is accomplished on match score or decision levels.[14, 15] The analysis is usually performed in within the Bayessian statistical framework.[16, 17] Thus, the problem of theoretical performance limit analysis of identification systems based on fusion of multimodal biometrics open. Secondly, the influence of the dependence/independence of the fused multimodal signals on the attained system theoretical performance was not addressed yet to our best knowledge. The existing results in this direction concern the correlation structure of these data. Surprisingly, but there does not exist a unique point of view on this problem. For instance, it is reported in[18] that fusion of correlated biometrics does not always lead to the fusion performance improvement versus combining independent signals. Contrarily, it is demonstrated in [17] that taking into account correlation between the biometric modalities one can obtain an improvement. Additionally, no impact of the modality vector length on the identification performance was reported.

Motivated by the existing gap in the theoretical performance analysis of a binary multimodal biometric person identification systems, we formulate the goal of this paper as follows in the justification of their performance in terms of error exponents for both cases of dependent and independent multimodal fusion setup cases.

The remaining part of the paper is organized as follows. We formulate the problem of the theoretical analysis of binary multimodal biometric person identification in Section 2. Performance analysis of multimodal biometric fusion is performed in Section 3. Finally, conclusion and future research perspectives are formulated in Section 4.

Notations We use capital letters to denote scalar random variables X and corresponding small letters x to denote their realizations. The superscript N is used to designate length-N vectors $x^N = [x[1], x[2], ..., x[N]]$ with k^{th} element $x[k]$. We use $X \sim p_X(x)$ or simply $X \sim p(x)$ to indicate that a random variable X is distributed according to $p_X(x)$. The mathematical expectation of a random variable $X \sim p_X(x)$ is denoted by μ_X and σ_X^2 denotes the variance of X. We use Σ to denote a covariance matrix. Correlation coefficient between two random variables is designated by ρ. Calligraphic fonts $\mathcal{X}$ denote sets $X \in \mathcal{X}$ and $|\mathcal{X}|$ denotes the cardinality of set $\mathcal{X}$. Superscript T stays for matrix transposition.

2. PROBLEM FORMULATION

We model a problem of binary multimodal biometric person identification as a binary hypothesis testing problem (Fig. 1). According to this set-up, the source of biometric multimodal signals governed by a joint probability distribution $p(x^N, y^N)$ produces a pair of length N vectors $X^N \in \mathcal{X}^N$ and $Y^N \in \mathcal{Y}^N$ such that $(X^N, Y^N) \sim q(x^N, y^N)$. In general, the length of the observed data vectors is not necessary equal (Fig. 2). This particular choice was made for the sake of analysis simplicity. The hypothesis testing block observing this pair of vectors performs a test η in order to decide if the set of multimodal signals belongs to a legal user or to an impostor. Thus, a binary multimodal biometric person identification system consists of the set $\left\{X^N, Y^N\right\}$ and a hypothesis test:

$$\eta : \mathcal{X}^N \times \mathcal{Y}^N \to \{0, 1\}, \tag{1}$$

where 0,1 stay to indicate the case of assigning the user to a class of legals or impostors, respectively. We will refer to the hypothesis that correspond to the latter case as H_0 and to the former case as H_1. Therefore, the task of multimodal biometrics binary person identification as a hypothesis testing is to decide which of the two hypotheses is true given (X^N, Y^N). It is assumed that the test is performed as:

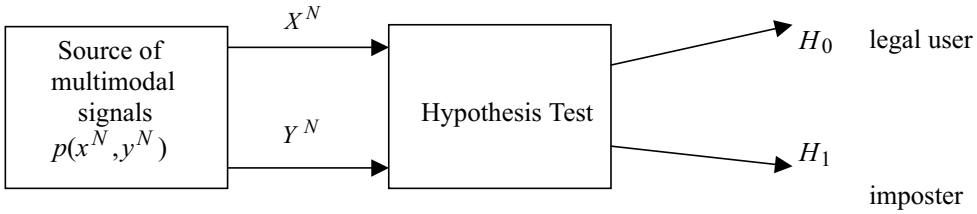

Figure 1. Multimodal biometric person identification: binary hypothesis testing formulation.

$$\begin{cases} H_0, (X^N, Y^N) \sim p^0(x^N, y^N), \\ H_1, (X^N, Y^N) \sim p^1(x^N, y^N), \end{cases} \tag{2}$$

where a priori statistical models on alternative hypotheses are denoted by $H_0 \sim p^0(x^N, y^N) = \prod_{i=1}^N p^0(x_i, y_i)$, $H_1 \sim p^1(x^N, y^N) = \prod_{i=1} p^1(x_i, y_i)$.

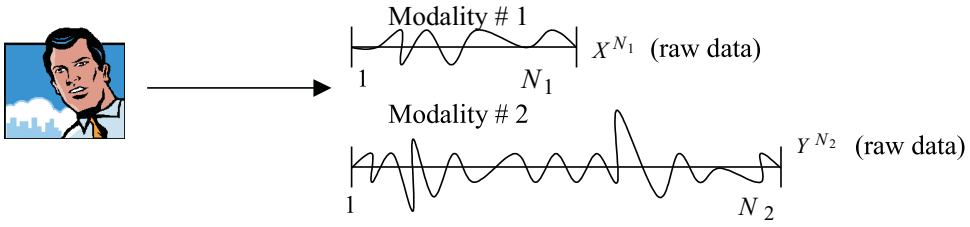

Figure 2. Multimodal observations: the vectors of different lengths might be observed.

Various tests can be performed to solve the above identification problem, i.e., Bayessian, minimax or Neyman-Pearson, however we will use the optimal Neyman-Pearson test in our formulation in order to attain the lowest probabilities of misclassification. These errors are of two kinds, type I error or a false alarm, denoted as P_f, occurs if a legal user is approved to be an impostor, and type II error or a miss, denoted as P_m, occurs in the opposite case defined as:

$$P_m = \Pr[\eta \leq T | H_1], \tag{3}$$

$$P_f = \Pr[\eta \geq T | H_0]. \tag{4}$$

It is stated by the Neyman-Pearson lemma that for a given maximal tolerable probability P_f, P_m can be minimized by stating hypothesis H_0 in the case the log-likelihood ratio defined as:

$$\eta = N \left\{ D(q(x,y) \,||\, p^1(x,y)) - D(q(x,y) \,||\, p^0(x,y)) \right\} \geq \log_2 T, \tag{5}$$

where it is supposed that the source $p(x^N, y^N)$ is memoryless, i.e., $p(x^N, y^N) = \prod_{i=1}^N p(x_i, y_i)$, and thus the empirical distribution is defined as $q(x^N, y^N) = \prod_{i=1}^N q(x_i, y_i)$, $p^0(x^N, y^n) = \prod_{i=1}^N p^0(x_i, y_i)$, $p^1(x^N, y^n) =$

$\prod_{i=1}^{N} p^1(x_i, y_i)$; $D(.\,||\,.)$ stays for a relative entropy between two distributions[12] and T designates a preifined threshold.

In case error probabilities of false alarm and miss are defined according to (3) and (4), the following inequality is valid[19]:

$$P_m \log \frac{P_m}{1-P_f} + (1-P_m) \log \frac{1-P_m}{P_f} \leq D(p^1(x^N, y^N)\,||\,p^0(x^N, y^N)) \tag{6}$$

Fixing in (6) probability $P_m = 0$, one obtains a lower bound on P_f that increases with decrease of relative entropy $D(p^1(x^N, y^N)\,||\,p^0(x^N, y^N))$:

$$P_m \leq 2^{-D(p^1(x^N, y^N)||p^0(x^N, y^N)))}. \tag{7}$$

Thus, in order to maximize the performance of a multimodal person identification, one should try to maximize $D(p^1(x^N, y^N)\,||\,p^0(x^N, y^N)$. In order to achieve optimal performance in terms of the Bayessian probability of error, $P_e = \pi_I P_f + \pi_{II} P_m$, where π_I, π_{II} stay for costs of making the error of type I and II, respectively, the so-called J-divergence, $J = D(p^1(x^N, y^N)\,||\,p^0(x^N, y^N)) + D(p^0(x^N, y^N)\,||\,p^1(x^N, y^N))$ should be maximized.[20]

Finally, the complete system performance analysis can be performed based on Stein lemma.[12] According to this lemma the performance of the Neyman-Pearson classifier is defined as:

$$P_f \sim 2^{-N\left[D(p^1(x,y))||D(p^0(x,y))\right]}, \text{for a fixed } P_m, \tag{8}$$

$$P_m \sim 2^{-N\left[D(p^0(x,y))||D(p^1(x,y))\right]}, \text{for a fixed } P_f. \tag{9}$$

Thus, the overall system performance is determined by the corresponding relative entropies defined with respect to the prior distributions on alternative hypotheses.

In the following sections we will consider the impact of modality dependence on the corresponding probabilities of error.

3. PERFORMANCE ANALYSIS

3.1. Independent modalities

In this case a priori models for alternative hypotheses can be written as $p^1(x, y) = p^1(x)p^1(y); p^0(x, y) = p^0(x)p^0(y)$. Thus, applying a chain rule for relative entropies, one has:

$$D(p^1(x, y))\,||\,D(p^0(x, y)) = D(p^1(y)\,||\,p^0(y)) + D(p^1(x)\,||\,p^0(x)), \tag{10}$$

$$D(p^0(x, y))\,||\,D(p^1(x, y)) = D(p^0(y)\,||\,p^1(y)) + D(p^0(x)\,||\,p^1(y)). \tag{11}$$

The corresponding bounds on the probabilities of error are:

$$P_f \sim 2^{-N\left[D(p^1(y)||p^0(y)) + D(p^1(x)||p^0(x))\right]}, \text{for a fixed and arbitrary small } P_m, \tag{12}$$

$$P_m \sim 2^{-N\left[D(p^0(y)||p^1(y)) + D(p^0(x)||p^1(y))\right]}, \text{for a fixed and arbitrary small } P_f. \tag{13}$$

Therefore, performance of the multibiometric person identification system measured in terms of error exponents enhnances with a number of fused signals.

3.2. Dependent modalities

In this case $p(x,y) \neq p(x)p(y)$. Thus, the bounds on the probabilities of error are determined by (8) and (9).

According to the chain rule for the relative entropy one has:

$$D(p^1(x,y)\,||\,p^0(x,y)) = D(p^1(y)\,||\,p^0(y)) + D(p^1(x\,|y)\,||\,p^0(y\,|x)), \tag{14}$$

$$D(p^0(x,y)\,||\,p^1(x,y)) = D(p^0(y)\,||\,p^1(y)) + D(p^0(x\,|y)\,||\,p^1(x\,|y)). \tag{15}$$

Thus, in order to compare the bounds for dependent (8) and (9) and independent (14) and (15) cases one should compare two quantities:

$$D(p^0(x)\,||\,p^1(x)) \text{ vs. } D(p^0(x\,|y)\,||\,p^1(x\,|y)), \tag{16}$$

$$D(p^1(x)\,||\,p^0(x)) \text{ vs. } D(p^1(x\,|y)\,||\,p^0(x\,|y)). \tag{17}$$

In the case,

$$D(p^0(x)\,||\,p^1(x)) \leq D(p^0(y\,|x)\,||\,p^1(x\,|y)), \tag{18}$$

$$D(p^1(x)\,||\,p^0(x)) \leq D(p^1(x\,|y)\,||\,p^0(x\,|y)). \tag{19}$$

one can conclude that fusion of dependent modalities has a better performance than one can obtain by fusing independent signals.

Lemma: Conditioning does not reduce relative entropy.

Proof.

$$\begin{aligned}
&D(p^0(y\,|x)\,||\,p^1(y\,|x)) - D(p^0(x)\,||\,p^1(x)) \\
&= \textstyle\sum_x \sum_y p^1(x,y) \log \frac{p^1(x|y)}{p^0(x|y)} - \sum_x p^1(x) \log \frac{p^1(x)}{p^0_X(x)} \\
&= \textstyle\sum_x \sum_y p^1(x,y) \log \frac{p^1(x|y)}{p^0(x|y)} - \sum_x \sum_y p^1(x,y) \log \frac{p^1(x)}{p^0(x)} \\
&= \textstyle\sum_x \sum_y p^1(x,y) \log \frac{p^1(x|y)p^0(x)}{p^0(x|y)p^1(x)} \\
&\geq 1 - \textstyle\sum_x \frac{p^1(x)}{p^0(x)} \sum_y p^1(y) p^0(x\,|y) \\
&= 1 - \textstyle\sum_x \frac{p^1(x)}{p^0(x)} p^0(x) \\
&= 0,
\end{aligned} \tag{20}$$

where the only inequality in (7) is due to $\log(x) \geq 1 - \frac{1}{x}$.

Thus, based on (6) one can conclude that fusion of independent modalities gives the lower limit of performance enhancement in multimodal fusion classification problem. When modalities are dependent, the gain due to the fusion is higher in terms of reduction of error probabilities.

3.3. Bivariate Gaussian case.

In order to evaluate quantitatively the performance gain one can expect from fusion of dependent modalities in binary multimodal biometric identification systems, it was assumed that the priors on alternative hypotheses follow bivariate Gaussian distributions:

$$p^1(x,y) = \frac{1}{2\pi\sqrt{\det(\Sigma_1)}} \exp\Big\{ -\frac{1}{2} \left[x-\mu_{X_1}, y-\mu_{Y_1}\right]^T \Sigma_1^{-1} \left[x-\mu_{X_1}, y-\mu_{Y_1}\right] \Big\}; \tag{21}$$

$$p^0(x,y) = \frac{1}{2\pi\sqrt{\det(\Sigma_0)}} \exp\Big\{ -\frac{1}{2} \left[x-\mu_{X_0}, y-\mu_{Y_0}\right]^T \Sigma_0^{-1} \left[x-\mu_{X_0}, y-\mu_{Y_0}\right] \Big\}, \tag{22}$$

with mean vectors $[\mu_{X_1}, \mu_{Y_1}]$, $[\mu_{X_0}, \mu_{Y_0}]$ and covariance matrices

$$\Sigma_1 = \begin{pmatrix} \sigma_{X_1}^2 & \rho\sigma_{X_1}\sigma_{Y_1} \\ \rho\sigma_{X_1}\sigma_{Y_1} & \sigma_{Y_1}^2 \end{pmatrix};$$

$$\Sigma_0 = \begin{pmatrix} \sigma_{X_0}^2 & \rho\sigma_{X_0}\sigma_{Y_0} \\ \rho\sigma_{X_0}\sigma_{Y_0} & \sigma_{Y_0}^2 \end{pmatrix},$$

where ρ is a correlation coefficient.

Therefore, the joint relative entropies that define corresponding probabilities of error are given by:

$P_f : D(p^1(x,y) \,||\, p^0(x,y)) =$

$$\frac{1}{2}\Big\{ \log_2 \frac{\det(\Sigma_1)}{\det(\Sigma_0)} + tr\left[\Sigma_1^{-1}\Sigma_0\right] + \left[\mu_{X_0}-\mu_{X_1}, \mu_{Y_0}-\mu_{Y_1}\right] \Sigma_0^{-1} \left[\mu_{X_0}-\mu_{X_1}, \mu_{Y_0}-\mu_{Y_1}\right]^T \Big\}; \tag{23}$$

$P_m : D(p^0(x,y) \,||\, p^1(x,y)) =$

$$\frac{1}{2}\Big\{ \log_2 \frac{\det(\Sigma_0)}{\det(\Sigma_1)} + tr\left[\Sigma_0^{-1}\Sigma_1\right] + \left[\mu_{X_1}-\mu_{X_0}, \mu_{Y_1}-\mu_{Y_0}\right] \Sigma_1^{-1} \left[\mu_{X_1}-\mu_{X_0}, \mu_{Y_1}-\mu_{Y_0}\right]^T \Big\}, \tag{24}$$

where inverse covariance matrices Σ_1^{-1} and Σ_0^{-1} defined in the following way:

$$\Sigma_1^{-1} = \frac{1}{\sigma_{X_1}^2\sigma_{Y_1}^2(1-\rho^2)} \begin{pmatrix} \sigma_{Y_1}^2 & -\rho\sigma_{X_1}\sigma_{Y_1} \\ -\rho\sigma_{X_1}\sigma_{Y_1} & \sigma_{X_1}^2 \end{pmatrix},$$

$$\Sigma_0^{-1} = \frac{1}{\sigma_{X_0}^2\sigma_{Y_0}^2(1-\rho^2)} \begin{pmatrix} \sigma_{Y_0}^2 & -\rho\sigma_{X_0}\sigma_{Y_0} \\ -\rho\sigma_{X_0}\sigma_{Y_0} & \sigma_{X_0}^2 \end{pmatrix}.$$

To exemplify a possible gain, the parameters of a priory distributions $p^1(x,y)$ and $p^0(x,y)$ where fixed to $\mu_{X_0} = 10, \mu_{X_1} = 20, \sigma_{X_0}^2 = 36, \sigma_{X_1}^2 = 16, \mu_{Y_0} = 4, \mu_{Y_1} = 8, \sigma_{Y_0}^2 = 4, \sigma_{Y_1}^2 = 6$. The behavior of $D(p^1(x,y) \,||\, p^0(x,y))$ and $D(p^0(x,y) \,||\, p^1(x,y))$ as functions of the correlation coefficient ρ was analyzed. The obtained results are shown in Figure 3. They completely confirm our theoretical findings.

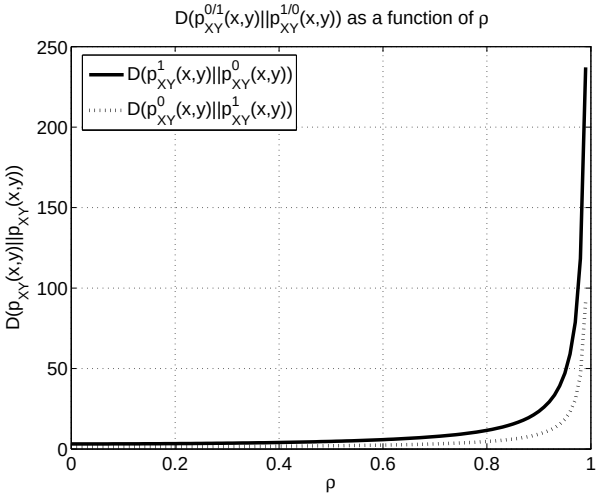

Figure 3. $D(p^1(x,y)\,||\,p^0(x,y))$ and $D(p^0(x,y)\,||\,p^1(x,y))$ as functions of ρ.

4. CONCLUSIONS AND FUTURE RESEARCH PERSPECTIVES

In this paper we considered the problem of performance analysis of binary multimodal biometric person identification. In particular, we considered two setups where fusion of independent and dependent modalities is performed. We developed a bound on the probabilities of miss and false alarm in terms of error exponents for both setups and theoretically proved that dependence between multimodal signals leads to the enhanced biometric fusion performance versus the setup with independent modalities. For demonstration purpose, we analyzed the bivariate Gaussian formulation of the problem and quantified the expected performance improvement. Since in the case of Gaussian data independence is equivalent to the uncorrelation, one can conclude that fusion of correlated modalities leads to a higher accuracy in classification problem. In particular, relative entropies that define the corresponding probability of errors, i.e., probability of false alarm and probability of miss, are non-decreasing monotonic functions of the correlation coefficient ρ on the interval [0,1].

As a natural extension of the obtained result we see its application to the domain of secure documents where we would like to develop a general system architecture and analyze multiple hypothesis formulation (Fig. 4).

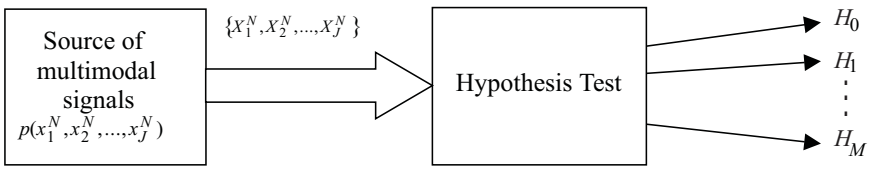

Figure 4. Multimodal biometric person identification: multiple hypothesis testing formulation.

Another potential future research line consists in the extension of the developed framework to the multimodal person identification using ID cards that contain embedded biometric data and personal data. Our goal is to develop a general system structure and to evaluate its performance.

5. ACKNOWLEDGEMENTS

This paper was partially supported by SNF Professeur Boursier grant PP002–68653, by the European Commission through the IST Programme under contract IST-2002-507932-ECRYPT and European Commission through

sixth framework program under the number FP6-507609 (SIMILAR) and Swiss IM2 projects. The authors are thankful to the members of SIP group, University of Geneva for many stimulating and interesting discussions.

REFERENCES

1. R. Bolle and S. Pankanti, *Biometrics, Personal Identification in Networked Society: Personal Identification in Networked Society*, Kluwer Academic Publishers, Norwell, MA, USA, 1998.
2. A. M. de Alvaré, "How crackers crack passwords, or what passwords to avoid," Tech. Rep. UCID-21515, Lawrence Livermore National Laboratory, Septiembre 1988.
3. D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Unix Security Workshop*, pp. 5–14, The USENIX Association, Agosto 1990.
4. J. L. Wayman, A. K. Jain, D. Maltoni, and D. Maio, *Biometric Systems: Technology, Design and Performance Evaluation*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2004.
5. A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. on Information Forensics and Security* **1**, pp. 125–143, June 2006.
6. M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans. on attern Analysis Machine Intelligence* **19**, pp. 786–796, July 1997.
7. A. K. Jain and D. Maltoni, *Handbook of Fingerprint Recognition*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.
8. A. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition?," in *First international conference on Biometric Authentication*, pp. 561–572, 2004.
9. L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?," Tech. Rep. MSU-CSE-99-39, Department of Computer Science, Michigan State University, East Lansing, Michigan, December 1999.
10. L. Hong and A. K. Jain, "Integrating faces and fingerprints for personal identification," in *ACCV '98: Proceedings of the Third Asian Conference on Computer Vision-Volume I*, pp. 16–23, Springer-Verlag, (London, UK), 1997.
11. A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics (International Series on Biometrics)*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.
12. T. Cover and J. Thomas, *Elements of Information Theory.*, Wiley and Sons, New York, 1991.
13. A. Ross, R. G. Hong, A. K. Jain, and S. Pankanti, "Feature level fusion using hand and face biometrics," in *SPIE Conf. Biometric Technology for Human Identification II*, pp. 196–204, 2005.
14. B. Ulery, W. Fellner, A. H. P. Hallinan and, and C. Watson, "Evaluation of selected biometric fusion techniques," tech. rep. http://www.itl.nist.gov/iad/894.03/pact/ir_7346_C.pdf.
15. R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Trans. Pattern Anal. Mach. Intell.* **17**(10), pp. 955–966, 1995.
16. E. S. Bigun, J. Bigun, B. Duc, and S. Fischer, "Expert conciliation for multi modal person authentication systems by bayesian statistics," in *AVBPA '97: Proceedings of the First International Conference on Audio- and Video-Based Biometric Person Authentication*, pp. 291–300, Springer-Verlag, (London, UK), 1997.
17. O. Ushmaev and S. Novikov, "Biometric fusion: Robust approach," in *Workshop on Multimodal User. Authentication (MMUA 2006)*, (Toulouse, France), 2006.
18. N. Poh and S. Bengio, "ow do correlation and variance of base classifiers affect fusion in biometric authentication tasks?," *IEEE Transactions on Signal Processing* **53**, pp. 4384–4396, November 2005.
19. R. E. Blahut, *Principles and practice of information theory*, Addison Wesley Publ. Co., 1987.
20. H. V. Poor, *An Introduction to Detection and Estimation Theory*, Springer-Verlag, 1994.