Privacy-Preserving Multimodal Person and Object Identification *

Oleksiy Koval
CVML,CUI - University of Geneva
7, route de Drize,
1227, Geneva, Switzerland
koval@cui.unige.ch

Sviatoslav Voloshynovskiy
CVML,CUI - University of Geneva
7, route de Drize,
1227, Geneva, Switzerland
svolos@cui.unige.ch

Thierry Pun
CVML,CUI - University of Geneva
7, route de Drize,
1227, Geneva, Switzerland
pun@cui.unige.ch

ABSTRACT

In this paper we investigate multimodal biometric person and object identification. We model this process of multimodal identification as multimodal multiple hypothesis testing with independent modalities. We analyze theoretical performance limits that can be attained in such a multimodal protocol in terms of exponents of average error probability. Furthermore, we address a privacy related issues in this paper. In particular, we consider performance/privacy trade-off due to the indirect multimodal identification performed in a secret subspace and approximate the obtained performance limits using properties of random projections. Finally, a set of experiments exemplifies our findings.

1. INTRODUCTION

Problem of identifying people related to the answer to the following questions like "Is this person who he/she claims to be?", "Should this individual be granted access to the system?", "Does this employee have rights to performs this action?", *etc.*, has become an unavoidable security feature in our society targeting establishing legitimacy of a user or customer. Evidently, that granting such access rights should be reliable meaning that the probability of unauthorized user to be accepted by identification procedure should be minimized.

To provide such an accurate yet a reliable performance identification, a system should be designed based on a specific information or features referred to as *identifier* that potentially are strongly related to separate individuals and satisfy the following requirements of *universylity* (does everyone have it ?), *distinctiveness* (can people be distinguished based on an identifier?), *permanence* (how permanent are the identifiers?), *collectability* (how well can the identifiers be captured and quantified?) *performance* (matching speed and accuracy), *acceptability* (willingness of people to accept), *circumvention* (foolproof) [1].

*(Further information: contact S. Voloshynovskiy, e-mail: svolos@cui.unige.ch)

MM&Sec'08, September 22-23, 2008, Oxford, UK.

Evidently, identification of persons performed knowledge-based, i.e., based on what the person knows (password, pin) or possession-based, i.e., based on what the person owns (passport, ID card), cannot nowadays address all the referred issues first of all due to the absence of the mentioned link to between the identifier and a person. This absence opens a possibility of illegal use of the identifier by the eavesdropper.

Contrarily, biometrics as physical or behavioral features of humans (like face, fingerprint, iris, DNA, voice sample, signature, hand geometry, keystroke, etc.) represent an inevitable replacement of these classical security tokens due to certain advantages. The major one concerns their inherent link with a user and thus infeasibility to be stolen, forgotten or lost. Moreover, they provide a good solution to the above presented requirement trade-off. Indeed, they are capable of providing sufficient accuracy of identification procedure in terms of producing an error during identity verification. Finally, biometrics are omnipresent, easy to acquire, sufficiently permanent and universal in the sense that are in possession of all people.

However, it is necessary to admit that there is no biometric feature that meets all above requirements. Every type of biometric has advantages and disadvantages with respect to the presented factors. Identification performance that can be attained based on a particular biometric feature is one of the most important among these requirements. Recently it was demonstrated 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 discriminate among 10^5 and 10^3 instances, respectively [2]. Fingerprints are proved to provide a high matching accuracy [3], 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 [4].

A natural solution to overcome shortcomings of a particular biometric identifier is coming with multibiometric systems [5, 6, 7] attempting to benefit from exploiting of several biometric modalities or multibiometrics. Fusion of multibiometrics can be performed on various structural levels of an identification system [1]: sensor level, feature level, match score level, rank level and decision level. Due to the data processing inequality [8], the highest performance is expected if fusion is performed on the sensor level. However, various technological limitations made practical applicability problematic. That is why very few results are known today demonstrating the efficiency of such systems [9, 10]. Mostly, the fusion in practical multibiometric person identification systems is accomplished on the match score or decision levels [11, 12]. The analysis is usually performed within the Bayessian statistical framework [13, 14].

Biometric storage represents another problem that should be addressed with a special care. In many protocols (like those that are used to grant the access to laptops, mobile phones, and portable hard drives) it is required to store the original biometric template. Thus, physical access to the device permits the attacker to obtain the access to the mentioned original templates that leads to multiple security and privacy compromised issues like creating of faked biometrics, system impersonalization, or even illegal people tracking.

This security fraud was recently realized [15] in biometric person authentication and it was suggested to formulate the problem of biometric-based authentication as extraction of "common randomness" [16, 17] that is performed using the fundamentals of distributed source coding [18]. However, this approach assumes the availability of the original biometric template as a secret shared by distributed encoder and decoder. Thus, one can conclude that the realized security hole is not completely overpassed. At the same time, the use of hashes increases the probability of collusions.

An attempt of securing unimodal biometric person identification was recently performed by the authors [19]. For this purpose it is suggested to perform person identification not directly but using projection of the original biometric data to a secret domain targeting efficient compromise between attainable performance, privacy protection and computational complexity. The authors were able to demonstrate that a reasonable solution to this trade-off exists for the case when performance is measured in terms of exponent of the average probability of error and a secret subspace has a reduced cardinality with respect to the cardinality of the original data set.

Protection of physical objects that is an another challenging and important security problem of our society is currently suffering from similar technological shortcomings. Main proposed protection mechanisms are based on various proprietary technologies (material science) and recent technological developments (RFID). An impressive progress of reproducing technologies makes proprietary secrets outdated while the use of technological know-how for brand protection might be prohibitively expensive for the mass market scale.

Fortunately, it was recently realized [20] that physical objects possess similar unique characteristics as humans known as physical unclonable functions (PUF) that cannot be controlled by the manufacturer. A possible example of such a function is a fiber structure of a paper. Being a natural analog of biometrics, these functions allow to design object identification systems based on similar underlying principles as those targeting reliable biometric person identification where a solution to identification performance accuracy-security-computational efficiency trade-off is of a special interest. Despite unclonability property of a PUF, the necessity to protect the identifiers might come from the technological requirements of performing low cost/resolution acquisition of these identifiers compromising the infeasibility to produce a fake (for instance, in the case when a fiber structure of a paper is acquired by a low-resolution optical device like an embedded VGA-resolution camera of an habitual portable device).

This justification allows us generalize the main subject of this paper as the analysis of multimodal item identification where under item we consider a person or a physical object and will refer to an identifier as to biometric. In our analysis we perfom an attempt to extend the analysis of attained performance-security/privacy-computational complexity trade-off presented in [10] to multimodal formulation. The main goal of the current analysis is to justify the impact of security/privacy protecting transformations that allow simultaneous dimensionality reduction on the identification performance.

In the scope of our analysis we assume that multimodal signals used for item identification are independent. This choice is justified by the design of currently deployed person identification and authentication systems as well as by mutual independence of main biometric modalities like iris, fingerprint, hand geometry [21]. Similar justification can be applied to PUFs. For instance, fiber structures of different fragments of a common sheet of paper tends to possess mutual independence too.

The remaining part of the paper is organized in the following way. The problem of multimodal item identification is formulated in Section 2. Performance analysis of the multimodal identification protocol in the diirect mode and based on random projections are analyzed in Section 3 versus direct identity verification. Experimental validation results are presented in Section 4. Finally, Section 5 contains conclusions and draws some future extensions of the obtained results.

Notations. We use capital letters to denote scalar random variables X, bold capital letters to denote vector random variables $\mathbf{X}$, corresponding small regular letters x and small bold letters $\mathbf{x}$ to denote the realizations of scalar and vector random variables, respectively. The superscript N is used to denote length-N vectors $\mathbf{x} = \{x(1), x(2), ..., x(N)\}$ with i^{th} element $x(i)$. 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 $E_{p_X}[X]$ or simply by $E[X]$ and σ_X^2 denotes the variance of X. Calligraphic fonts $\mathcal{X}$ denote sets $X \in \mathcal{X}$ and $|\mathcal{X}|$ denotes a cardinality of set. Finally, $\mathbb{I}_N$ denotes a $N \times N$ identity matrix.

2. PROBLEM FORMULATION

A general diagram of identity verification based on multimodal secure biometrics and random projections is presented in Figure 1.

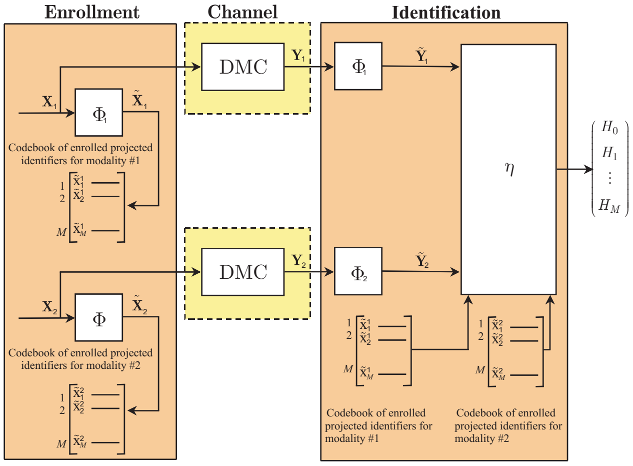


Figure 1: Multimodal item identification based on random projections: $\Phi_i, i = \{1, 2\}$ are a key-dependent random projection operators.

According to the presented problem formulation, the biometric identifiers are deduced during an enrollment stage based on the original independent templates $\{\mathbf{X}_1, \mathbf{X}_2\} \sim p(\mathbf{x}_1, \mathbf{x}_2) = p(\mathbf{x}_1)p(\mathbf{x}_2)$ transformed into a secret key-dependent reduced dimensionality domain via applying a random projection operator $\Phi = [\Phi_1, \Phi_2]$, where Φ_1, Φ_2 are $L_1 \times N_1$ and $L_2 \times N_2$ random matrices with $L_1 \le N_1, L_2 \le N_2$. The role of operators Φ_1 and Φ_2 is twofold. First, they are serving for security/privacy enhancement of the protocol via protection of the original identifiers $\mathbf{X}_1$ and $\mathbf{X}_2$. Second, they are used to reduce the identifier dimensionalities by factors $\frac{L_1}{N_1}$ and $\frac{L_2}{N_2}$, respectively. Without loss of generality, it is assumed in this paper that $N_1 = N_2 = N$.

These sequences $\tilde{\mathbf{x}}_j(i), i \in \{1, 2, ..., M\}, j \in \{1, 2\}$, are stored in the corresponding identification data bases that are made available for identification. It is supposed in the set-up under the analysis that the identification is performed based on the outputs of the corresponding independent acquisition channels discrete memoryless channels (DMC) modeled by transition probability matrixes $p(y_j|x_j)$, $j \in \{1, 2\}$. Thus, one should guarantee that the number of such indexes being limited by the maximum rate of reliable communications of the corresponding channels modeling the acquisition distortions. According to the channel coding theorem [8], $M \le \min\{2^{NI(X_1;Y_1)}, 2^{NI(X_2;Y_2)}\}$.

At the identity verification stage, in order to provide compatibility of the acquired data with a stored codebookes, $\mathbf{Y}_j, j \in 1, 2$ are projected to the mentioned secrete key-dependent transform domains $\tilde{\mathbf{Y}}_j = \Phi_j \mathbf{Y}_j$, $j \in \{1, 2\}$. Finally, a statistical test η is applied to decide which identifier pair out of $M = \min\{2^{NI(X_1;Y_1)}, 2^{NI(X_2;Y_2)}\}$ alternatives is observed by the identity verification system.

In order to achieve the main our goal in the scope of this paper formulated in the Introduction, we perform evaluation of the impact of the random projection on the system performance in terms of identification accuracy and involved computational complexity. For this purpose, the problem of multimodal item identification is modeled as multimodal multiple hypothesis testing [22]. In particular, we assume that a source of multimodal identifiers represented by a joint probability distribution $p(\mathbf{x}_1, \mathbf{x}_2)$ produces a pair of length N vectors $\{\mathbf{X}, \mathbf{X}_2\} \in \mathcal{X}_1^N \times \mathcal{X}_2^N$. The ultimate goal of the hypothesis test η that observes a pair of distorted acquisition channel outputs $\{\mathbf{Y}_1, \mathbf{Y}_2\} \in \mathcal{Y}_1^N \times \mathcal{Y}_2^N$ is to decide, which out of M possible cases is observed. We define an M-ary multimodal biometric person identification system as composed of a product set $\mathcal{Y}_1^N \times \mathcal{Y}_2^N$ and a hypothesis test:

$$\eta : \mathcal{Y}_1^N \times \mathcal{Y}_2^N \to \{1, 2, ..., M\}, \tag{1}$$

where $\{1, 2, ..., M\}$ is a collection of possible alternatives.

The test is accomplished assuming the following prior distributions on respective hypotheses:

$$H_i = \begin{cases} \mathbf{Y}_1 \sim p^i(\mathbf{y}_1), \\ \mathbf{Y}_2 \sim p^i(\mathbf{y}_2), \end{cases} \tag{2}$$

where $i \in \{1, 2, ..., M\}$, $H_i \sim p^i(\mathbf{y}_1)p^i(\mathbf{y}_2) = \prod_{k=1}^{N} p^i(y_1(k)) \cdot \prod_{k=1}^{N} p^i(y_2(k))$.

Performance accuracy of the defined multimodal M-ary hypothesis test is measured using Bayesian average probability of error:

$$C(\eta) = \sum_i \pi_a \sum_{b \ne a} P_{ab}^E, \tag{3}$$

where η designates a selected decision rule, P_{ab}^E stays for the probability of falsely accepting hypothesis H_b in the case when H_a is in "true" and π_a is the prior probability of the hypothesis H_a.

Finally, we define the respective exponent of this average probability of error as follows:

$$\theta(\eta) = \lim_{N \to \infty} -\frac{1}{N} \log C(\eta). \tag{4}$$

It was realized [23, 24] that theoretical performance analysis of multiple hypothesis testing for the case of more than two hypotheses under the selected performance criterion of the average probability of error does not lead to the tractable results. In order to overcome this problem, the analysis is usually conducted based on certain strategies simplifying further considerations. One such an approximative solution was firstly introduced in [24], where for the sake of analysis tractability multiple hypothesis testing was replaced by a set of binary tests (Figure 3). It is known that in this case, the optimal decision rule follows the multiple maximum a posteriori (MMAP) strategy:

$$\eta^{MMAP} = \arg \max_{i \in \{1,2,\ldots,M\}} \pi_i p^i(\mathbf{y}_1, \mathbf{y}_2). \tag{5}$$

In the following Sections it will be assumed that the prior hypothesis distribution is uniform, $\pi_i = \frac{1}{M}$, and the MMAP decision rule will be simplified to multiple maximum likelihood (MML) decision rule:

$$\eta^{MML} = \arg \max_{i \in \{1,2,\ldots,M\}} p^i(\mathbf{y}_1, \mathbf{y}_2). \quad (6)$$

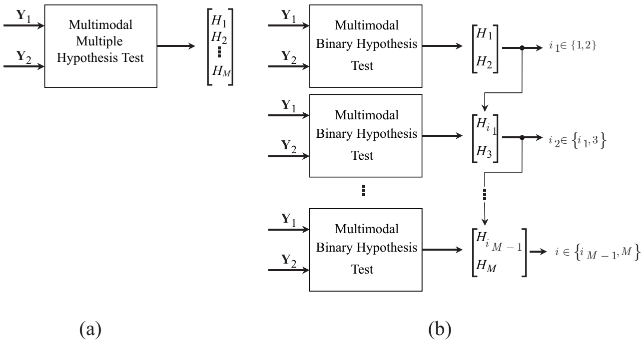


Figure 2: Multimodal multiple hypothesis testing (a) vs its approximation by a set of multimodal binary tests (b).

It was demonstrated [24] for the memoryless case that the average probability of making an error in the multiple hypothesis test is bounded as follows:

$$C(\eta^{MMAP}) \leq \frac{M(M-1)}{2} \max_{m \neq n} P^E_{mn}(\eta^{MAP}), \quad (7)$$

where $P^E_{mn}(\eta^{MAP})$ denotes the probability of falsely accepting hypothesis H_n using maximum a posteriori (MAP) decision rule η^{MAP}, when hypothesis H_m is in force.

Based on (7) and Chernoff theorem [8] one can obtain a limit on the behavior of the exponent of $C(\eta^{MMAP})$ [24]

$$\theta(\eta^{MMAP}) \leq D^*, \quad (8)$$

where $\theta(\eta^{MAP})$ stays for the MAP decision rule applied in a multimodal binary hypothesis testing formulation and:

$$D^* = \min_{(m,n) \in \{1,2,\ldots,M\}, m \neq n} D_s(p^m(y_1, y_2), p^n(y_1, y_2)), \quad (9)$$

where $D_s(p^m(y_1, y_2), p^n(y_1, y_2))$ designates the Chernoff distance [8] between two distributions $p^m(y_1, y_2)$ and $p^n(y_1, y_2)$ defined in the following way:

$$D_s(p^m(y_1, y_2), p^n(y_1, y_2)) =$$

$$\max_{0 \leq s \leq 1} -\log \int_{\mathcal{Y}_1} \int_{\mathcal{Y}_2} p^n(y_1, y_2) \left\{ \frac{p^m(y_1, y_2)}{p^n(y_1, y_2)} \right\}^s dy_1 dy_2, \quad (10)$$

where s, $0 \leq s \leq 1$, is the optimisation parameter.

Therefore, the performance of multimodal item identification system modeled as the mutimodal M-ary hypothesis testing and measured in terms of exponent of the average probability of error can be accurately approximated by a set of multimodal binary tests and upper limited by the worst pairwise Chernoff distance between alternative hypothesis prior distributions $p^m(y_1, y_2)$ and $p^n(y_1, y_2)$.

3. PERFORMANCE ANALYSIS

Direct identification. In this Section we perform analysis of the problem of multimodal item identification formulated in the previous Section assuming Gaussian formulation and availability of the observation of the acquired genuine biometric template at verification. In fact, we suppose that $p^i(\mathbf{y}_1, \mathbf{y}_2) = \mathcal{N}(\mathbf{x}_1(i), \sigma^2_{Z_1}\mathbb{I}_N)\mathcal{N}(\mathbf{x}_2(i), \sigma^2_{Z_2}\mathbb{I}_N)$. Such a formulation is justified by the assumption that different distortions are introduced in the original multimodal identifiers during acquisition. This assumption allows to rewrite prior hypothesis model (1) in the following way:

$$H_i = \begin{cases} \mathbf{y}_1 = \mathbf{x}_1(i) + \mathbf{z}_1, \\ \mathbf{y}_2 = \mathbf{x}_2(i) + \mathbf{z}_2, \end{cases} \quad (11)$$

where $i \in \{1, 2, ..., M\}$ and the channel impacts are modeled as $\mathbf{Z}_1 \sim \mathcal{N}(\mathbf{0}, \sigma^2_{Z_1}\mathbb{I}_N)$ and $\mathbf{Z}_2 \sim \mathcal{N}(\mathbf{0}, \sigma^2_{Z_2}\mathbb{I}_N)$.

For such a formulation of the multimodal item identification problem and following the strategy of multimodal multiple hypothesis testing performance limitation by a multimodal binary test applied to the pair of hypotheses m and n that are characterized by the closest Chernoff distance, the corresponding MML test (6) can be restated using maximum likelihood (ML) strategy as follows:

$$\eta^{ML} = \arg \max_{i \in \{m,n\}} p^i(\mathbf{y}_1, \mathbf{y}_2). \quad (12)$$

It is known that log likelihood ratio minimizes probability of error. Thus, taking the logarithms of the likelihood functions, one obtains the rule that accepts the hypothesis m being in force:

$$\log(p^m(\mathbf{y}_1, \mathbf{y}_2)) - \log(p^n(\mathbf{y}_1, \mathbf{y}_2)) \geq 0. \quad (13)$$

Due to the mutual independence of multimodal identifiers, (13) can be rewritten as:

$$\log(p^m(\mathbf{y}_1)) + \log(p^m(\mathbf{y}_2)) - \log(p^n(\mathbf{y}_1)) - \log(p^n(\mathbf{y}_2)) \geq 0. \quad (14)$$

Therefore, (14) can be rewritten using sufficient statistics in the following way:

$$t(\mathbf{y}_1, \mathbf{y}_2) = \mathbf{y}_1^T(\mathbf{x}_1(m) - \mathbf{x}_1(n)) - \frac{1}{2}(\epsilon_1(m) - \epsilon_1(n))$$

$$+\frac{\sigma^2_{Z_1}}{\sigma^2_{Z_2}}(\mathbf{y}_2^T(\mathbf{x}_2(m) - \mathbf{x}_2(n)) - \frac{1}{2}(\epsilon_2(m) - \epsilon_2(n))), \quad (15)$$

where $\epsilon_1(m) = \mathbf{x}_1(m)^T\mathbf{x}_1(m)$, $\epsilon_1(n) = \mathbf{x}_1(n)^T\mathbf{x}_1(n)$, $\epsilon_2(m) = \mathbf{x}_2(m)^T\mathbf{x}_2(m)$, $\epsilon_2(n) = \mathbf{x}_2(n)^T\mathbf{x}_2(n)$ are the energies of vectors $\mathbf{x}_j(m)$ and $\mathbf{x}_j(n)$, $j \in \{1, 2\}$, respectively.

The obtained sufficient statistics allow to express the corresponding prior models on the multimodal binary hypotheses as follows:

$$\begin{cases} H_n : T(\mathbf{Y}_1\mathbf{Y}_2) \sim \\ \quad \mathcal{N}\Big(-\frac{1}{2}\Big(d_1^2 + \frac{\sigma^2_{Z_1}}{\sigma^2_{Z_2}}d_2^2\Big), \sigma^2_{Z_1}\Big(d_1^2 + \frac{\sigma^2_{Z_1}}{\sigma^2_{Z_2}}d_2^2\Big)\Big), \\ H_m : T(\mathbf{Y}_1\mathbf{Y}_2) \sim \\ \quad \mathcal{N}\Big(\frac{1}{2}\Big(d_1^2 + \frac{\sigma^2_{Z_1}}{\sigma^2_{Z_2}}d_2^2\Big), \sigma^2_{Z_1}\Big(d_1^2 + \frac{\sigma^2_{Z_1}}{\sigma^2_{Z_2}}d_2^2\Big)\Big), \end{cases} \quad (16)$$

where $d_1^2 = \|\mathbf{x}_1(m) - \mathbf{x}_1(n)\|^2$ and $d_2^2 = \|\mathbf{x}_2(m) - \mathbf{x}_2(n)\|^2$ are square distances between original item identifiers $\mathbf{x}_j(m)$ and $\mathbf{x}_j(n)$, $j \in \{1, 2\}$, respectively.

Therefore, under the memoryless assumption and according to (10) the exponent of the average probability of error that one can expect to attain in the multimodal item identification modeled as multimodal multiple hypothesis testing is bounded by Chernoff distance $D_s(p^m(y_1,y_2),p^n(y_1,y_2))$ that for the case of Gaussian statistics of hypothesis priors with equal variances can be expressed as:

$$D_s(p^m(y_1,y_2),p^n(y_1,y_2)) = \frac{d_1^2}{8\sigma_{Z_1}^2} + \frac{d_2^2}{8\sigma_{Z_2}^2}. \quad (17)$$

Furthermore,

$$d_j^2 = \|\mathbf{x}_j(m) - \mathbf{x}_j(n)\|^2$$
$$= \|\mathbf{x}_j(m)\|^2 + \|\mathbf{x}_j(n)\|^2 - 2\mathbf{x}_j(m)^T\mathbf{x}_j(n) = 2\|\mathbf{x}_j\|^2 \quad (18)$$

supposing that all identifiers for the same modality $j \in \{1,2\}$ have equal energy, i.e., $\|\mathbf{x}_j(m)\|^2 = \|\mathbf{x}_j(n)\|^2 = \|\mathbf{x}_j\|^2$, and all of them are pairwise orthogonal, i.e., $\mathbf{x}_j(m)^T\mathbf{x}_j(n) = 0$. Finally, using this assumption, one can reduce (17) as follows:

$$D_s(p^m(y_1,y_2),p^n(y_1,y_2)) = \frac{\|\mathbf{x}_1\|^2}{4\sigma_{Z_1}^2} + \frac{\|\mathbf{x}_2\|^2}{4\sigma_{Z_2}^2}. \quad (19)$$

Random projection-based identification. In this subsection of the paper, we assume that genuine multimodal templates are not available for the identification due to the security/privacy and computational complexity reasons and identity verification is performed using the data projected to a certain secret domain via applying a secure random projection operators Φ_j, $j \in \{1,2\}$:

$$\mathbf{y}'_j = \Phi_j\mathbf{y}_j. \quad (20)$$

As it was already mentioned earlier, the projection operators Φ_j serve to convert an original length-N vectors to a vectors of lower dimensionality $L_1, L_2, L_1 \le N, L_2 \le N$. These operators are random matrices with elements generated from a certain densities. In the scope of this paper, we assume that the elements of Φ_1 and Φ_2 are generated from a zero mean Gaussian distribution with a variance $\frac{1}{N}$, i.e., $\mathcal{N}(0,\frac{1}{N})$.

Following similar argument used in the previous subsection in the analysis of direct item identification, it is possible to demonstrate that the corresponding prior probabilities of the worst case binary hypothesis test in indirect identification problem formulation can be defined as follows:

$$\begin{cases} H'_i: & T(\tilde{\mathbf{Y}}_1,\tilde{\mathbf{Y}}_2) \sim \mathcal{N}(-\frac{1}{2}d'^2, \sigma_{Z_1}^2 d'^2), \\ H'_j: & T(\tilde{\mathbf{Y}}_1,\tilde{\mathbf{Y}}_2) \sim \mathcal{N}(\frac{1}{2}d'^2, \sigma_{Z_1}^2 d'^2), \end{cases} \quad (21)$$

where $d'^2 = (\mathbf{x}_1(m)-\mathbf{x}_1(n))^T\Phi_1^T(\Phi_1\Phi_1^T)^{-1}\Phi_1(\mathbf{x}_1(m)-\mathbf{x}_1(n)) + \frac{\sigma_{Z_1}^2}{\sigma_{Z_2}^2}\Big((\mathbf{x}_2(m)-\mathbf{x}_2(n))^T\Phi_2^T(\Phi_2\Phi_2^T)^{-1}\Phi_2(\mathbf{x}_2(m)-\mathbf{x}_2(n))\Big)$ and Φ_j^T, $j \in \{1,2\}$ is the result of transposition of projection operator Φ_j.

Therefore, similarly to (19), the exponent of the average probability of error for indirect item identification is limited by:

$$D'_s(p^m(y_1,y_2),p^n(y_1,y_2)) = \frac{d_1'^2}{8\sigma_{Z_1}^2} + \frac{d_2'^2}{8\sigma_{Z_2}^2}, \quad (22)$$

where $d_1'^2 = (\mathbf{x}_1(m)-\mathbf{x}_1(n))^T\Phi_1^T(\Phi_1\Phi_1^T)^{-1}\Phi_1(\mathbf{x}_1(m)-\mathbf{x}_1(n))$ and $d_2'^2 = (\mathbf{x}_2(m)-\mathbf{x}_2(n))^T\Phi_2^T(\Phi_2\Phi_2^T)^{-1}\Phi_2(\mathbf{x}_2(m)-\mathbf{x}_2(n))$.

In the case one assumes that these operators possess orthonormality property, i.e., $\Phi_j\Phi_j^T = \mathbb{I}_{L_j}$, $j \in \{1,2\}$, the distances d'_j can be expressed in the following way:

$$d_j'^2 = (\mathbf{x}_j(m) - \mathbf{x}_j(n))^T\Phi_j^T\Phi_j(\mathbf{x}_j(m) - \mathbf{x}_j(n))$$
$$= \|\Phi_j(\mathbf{x}_j(m) - \mathbf{x}_j(n))\|^2.$$

Besides security/privacy and computational complexity issues, attractiveness of projecting onto a randomized bases is justified by the performance analysis simplification. As it was for the first time proved by Johnson and Linderstrauss [25], in the case the projection is performed from a certain vector space onto a random subspace of sufficiently high dimension, the distance between the space elements will be approximately preserved. Then, the following sandwich of inequalities is valid:

$$(1-\delta_1)\sqrt{\frac{L_1}{N}}\|\mathbf{x}_1(m) - \mathbf{x}_1(n)\| \le \|\Phi_1(\mathbf{x}_1(m) - \mathbf{x}_1(n))\|$$
$$\le (1+\delta_1)\sqrt{\frac{L_1}{N}}\|(\mathbf{x}_1(m) - \mathbf{x}_1(n))\| \quad (23)$$

$$(1-\delta_2)\sqrt{\frac{L_2}{N}}\|\mathbf{x}_2(m) - \mathbf{x}_2(n)\| \le \|\Phi_2(\mathbf{x}_2(m) - \mathbf{x}_2(n))\|$$
$$\le (1+\delta_2)\sqrt{\frac{L_2}{N}}\|(\mathbf{x}_2(m) - \mathbf{x}_2(n))\| \quad (24)$$

for a sufficiently small δ_1 and δ_1. Then, under the orthonormality assumption about random projectors, i.e., $\Phi_j\Phi_j^T = \mathbb{I}_{L_j}$, $j \in \{1,2\}$ one can approximate (22) as it is presented below:

$$D'_s(p^m(y_1,y_2),p^n(y_1,y_2)) \approx \frac{L_1}{N}\frac{\|\mathbf{x}_1(m) - \mathbf{x}_1(n)\|^2}{8\sigma_{Z_1}^2}$$
$$+\frac{L_2}{N}\frac{\|\mathbf{x}_2(m) - \mathbf{x}_2(n)\|^2}{8\sigma_{Z_2}^2}. \quad (25)$$

Finally, assuming that $\mathbf{x}_j(m), \mathbf{x}_j(n)$, $j \in \{1,2\}$, are orthogonal sequences of equal energy, i.e., condition (18) is valid, one obtains:

$$D'_s(p^m(y_1,y_2),p^n(y_1,y_2)) \approx \frac{L_1}{N}\frac{\|\mathbf{x}_1\|^2}{4\sigma_{Z_1}^2} + \frac{L_2}{N}\frac{\|\mathbf{x}_2\|^2}{4\sigma_{Z_2}^2}. \quad (26)$$

4. EXPERIMENTAL VALIDATION

The main goal of this Section is fourfold. First of all, we would like to evaluate the impact of the use of complementary modality on the performance of item identification versus unimodal framework. Secondly, we will try to investigate the behavior of exponent of the average probability of error as a function of operational geometric signal-to-noise ratio (SNR) defined as $SNR = 10\log_{10}\left(\sqrt{\left(\frac{\|\mathbf{x}_1\|^2}{\sigma_{Z_1}^2}\frac{\|\mathbf{x}_2\|^2}{\sigma_{Z_2}^2}\right)}\right)$ that is used in the analysis of multicarrier channels [26] for the direct identification case (17). Thirdly, we would like to estimate the impact of indirect multimodal identification, i.e., use of random projections (20), on the attainable performance. Finally, we would like to see the accuracy of performance approximation (20) using Johnson-Linderstrauss result (23).

For this purposes we run a set of experimental simulations according to the following setup: the length of all vectors N was selected to be equal 1024, the operational geometric SNR range was fixed to the interval $[-15; 25]$ dB. The templates $\mathbf{x}_j$, $j \in \{1, 2\}$ were generated from a zero-mean, unit variance Gaussian distribution, while the elements of random projector operator Φ_j are i.i.d. zero-mean Gaussian with the variance $\frac{1}{N}$. The dimensionality reduction ratio $\frac{L_j}{N}$ was set to $[0.9; 0.8; 0.7; 0.6; 0.5]$. Since the obtained results revealed similar behavior of error exponent of the average probability of error for all selected $\frac{L}{N}$, only the cases of $\frac{L_j}{N} = [0.9; 0.7; 0.5]$ are presented in the paper (Figure 3-6). The obtained experimental result allows to conclude the superiority of multimodal item identification versus unimodal one. A possible gain from the presence of second modality is measured by 3 dB (Figure 3) for the above experimental setup and equal energy of multimodal identifiers. The results also demonstrate that in multimodal multiple hypothesis testing item identification problem formulation under the stationary acquisition conditions a certain loss in performance of random projection based identification versus a direct one is observed in terms of exponent of the average probability of error due to the impact of the projection operator. These results also confirm a high accuracy of Johnson-Linderstrauss approximation of performance of the random projection-based identification.

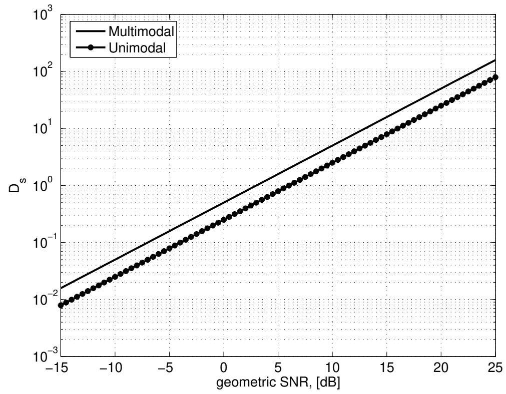
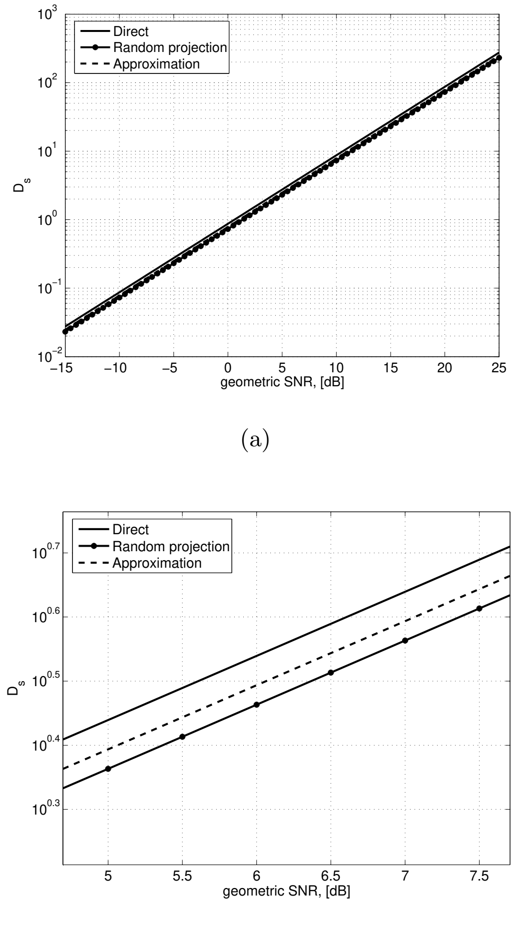


Figure 3: Chernoff distance for multimodal versus unimodal item identification.

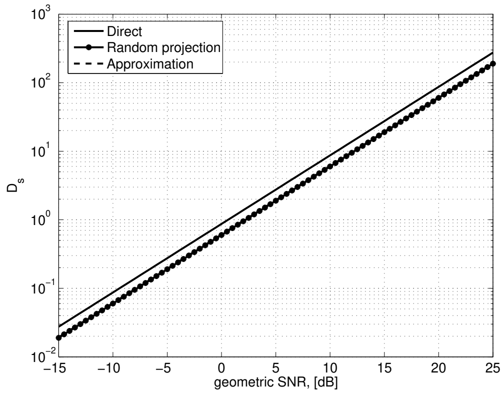


(b)

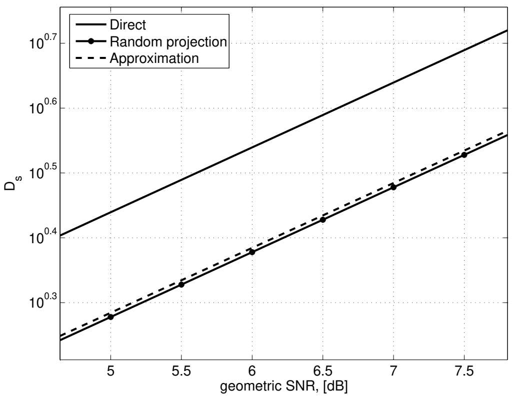
Figure 4: Behavior of exponent of average probability of error for multimodal direct identification, random projection-based identification and approximation of random projection-based identification, $\frac{L}{N} = 0.9$: (a) full-size plot and (b) magnified fragment.

5. CONCLUSIONS AND FUTURE RESEARCH PERSPECTIVES

In this paper, we considered the problem of privacy preserving/security enhanced item identification from the performance perspective. We propose to protect genuine independent multimodal identifiers used for verification by projecting them onto secret randomize subsets. The performed analysis of the identification accuracy in the multimodal case versus a unimodal setup revealed the advantages of the former approach measured in terms of the exponent of the average probability of error attained in the multiple hypothesis testing. Furthermore, we compared the performance of random projection-based multimodal identification versus the direct one in terms of the mentioned performance measure. In the former case, we were able to provide approximations

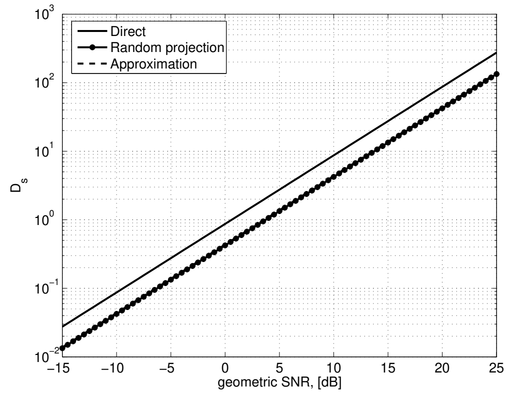


(a)

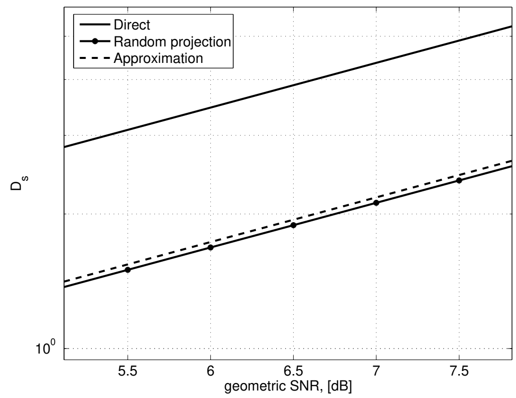


(b)

Figure 5: Behavior of exponent of average probability of error for multimodal direct identification, random projection-based identification and approximation of random projection-based identification, $\frac{L}{N} = 0.7$: (a) full-size plot and (b) magnified fragment.



(a)



(b)

Figure 6: Behavior of exponent of average probability of error for multimodal direct identification, random projection-based identification and approximation of random projection-based identification $\frac{L}{N} = 0.5$: (a) full-size plot and (b) magnified fragment.

of performance limits using properties of random projections. By means of computer simulations we demonstrated a certain performance loss versus direct identity verification that is linearly proportional to the dimensionality reduction ratio. Finally, a high accuracy of Johnson-Linderstrauss approximation of performance of projection-based multimodal identification was demonstrated.

In our future research we will extend the performed analysis to the case of direct and indirect multimodal item identification with dependent modalities.

6. ACKNOWLEDGMENTS

This paper was partially supported by SNF PB grant 114613 and SNF projects 200021-111643 and 200021–1119770, by the EU projects IST-2002-507932-ECRYPT, FP6-507609-SIMILAR and Swiss IM2 project.

7. REFERENCES

[1] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, June 2006.

[2] M. Golfarelli, D. Maio, and D. Maltoni, "On the error-reject tradeoff in biometric verification systems," *IEEE Trans. on attern Analysis Machine Intelligence*, vol. 19, no. 7, pp. 786–796, July 1997.

[3] A. K. Jain and D. Maltoni, *Handbook of Fingerprint Recognition.* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2003.

[4] A. K. Jain, S. C. Dass, and K. Nandakumar, "Can soft biometric traits assist user recognition?" in *First international conference on Biometric Authentication*, 2004, pp. 561–572.

[5] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?" Department of Computer Science, Michigan State University, East Lansing, Michigan, Tech. Rep. MSU-CSE-99-39, December 1999.

[6] 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.* London, UK: Springer-Verlag, 1997, pp. 16–23.

[7] A. A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics (International Series on Biometrics).* Secaucus, NJ, USA: Springer-Verlag New York, Inc., 2006.

[8] T. Cover and J. Thomas, *Elements of Information Theory.* Wiley and Sons, New York, 1991.

[9] 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*, 2005, pp. 196Ű–204.

[10] O. Koval, S. Voloshynovskiy, and T. Pun, "Error exponent analysis of person identification based on fusion of independent modalities," in *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents III*, San Jose, CA, USA, January 2007.

[11] 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.

[12] R. Brunelli and D. Falavigna, "Person identification using multiple cues," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 17, no. 10, pp. 955–966, 1995.

[13] 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.* London, UK: Springer-Verlag, 1997, pp. 291–300.

[14] O. Ushmaev and S. Novikov, "Biometric fusion: Robust approach," in *Workshop on Multimodal User Authent. (MMUA 2006)*, Toulouse, France, 2006.

[15] E. Martinian, S. Yekhanin, and J. Yedidia, "Secure biometrics via syndromes," in *43rd Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, USA, October 2005.

[16] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, 1993.

[17] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - part i: secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[18] D. Slepian and J. Wolf, "Noiseless encoding of correlated information sourcea," *IEEE Trans. Information Theory*, vol. 19, pp. 471–480, July 1973.

[19] O. Koval, S. Voloshynovskiy, and T. Pun, "Privacy-preserving biometric person identification," in *EUSIPCO'08*, Lausanne, Switzerland, August 2008.

[20] P. Tuyls, B. Skoric, and T. K. (Eds.), *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting.* Springer, 2007.

[21] A. Ross, "Information fusion in fingerprint authentication," Ph.D. dissertation, Michigan State University, Michigan , USA, 2003.

[22] O. Koval, S. Voloshynovskiy, and T. Pun, "Analysis of multimodal binary detection systems based on dependent/independent modalities," in *IEEE Int Workshop on Multimedia Sign. Proc. (MMSP-07)*, Chania, Crete, Greece, October 2007.

[23] H. van Trees, *Detection, Estimation, and Modulation Theory, Part I.* New York, Wiley, 1968.

[24] C.C.Leang and D.H.Johnson, "On the asymptotics of m-hypothesis bayesian detection," *IEEE Trans. on Information Theory*, vol. 43, no. 1, pp. 280–282, January 1997.

[25] W. B. Johnson and J. Lindenstrauss, "Extensions of lipschitz mapping into hilbert space," *Contemporary Mathematics*, no. 26, pp. 189–206, 1984.

[26] N. Al-Dhahir and J. M. Cioffi, "Optimum finite-length equalization for multicarrier transceivers," *IEEE Trans. on Inf. Com.*, vol. 44, no. 1, pp. 56–63, Jan. 1998.