Authentication of Biometric Identification Documents via Mobile Devices

Voloshynovskyy, Svyatoslav; Koval, Oleksiy; Villan Sebastian, Renato Fisher; Beekhof, Fokko Pieter; Pun, Thierry

Authentication of Biometric Identification Documents via Mobile Devices

Sviatoslav Voloshynovskiy,* Oleksiy Koval,†
Renato Villán,‡ Fokko Beekhof,§ and Thierry Pun¶
Stochastic Information Processing Group
Department of Computer Science, University of Geneva
24 rue du General-Dufour, 1211 Geneva 4, Switzerland

Abstract

In this paper, we consider the problem of authentication of biometric identification documents via mobile devices such as mobile phones or PDAs. We assume that the biometric identification document holds biometric data (e.g., face or fingerprint) in the form of an image and personal data in the form of text, both being printed directly onto the identification document. The proposed solution makes use of digital data-hiding in order to cross-store the biometric data inside the personal data and vice versa. Moreover, a theoretical framework is presented which should enable to analyze and guide the design of future authentication systems based on this approach. In particular, we advocate the separation approach which uses robust visual hashing techniques in order to match the information rates of biometric and personal data to the rates offered by current image and text data-hiding technologies. We also describe practical schemes for robust visual hashing and digital data-hiding that can be used as building blocks for the proposed authentication system. The obtained experimental results show that the proposed system constitutes a viable and practical solution.

*Contact author:svolos@cui.unige.ch; Visit:http://sip.unige.ch
†Electronic address: oleksiy.koval@cui.unige.ch
‡Electronic address: renato.villan@cui.unige.ch
§Electronic address: fokko.beekhof@cui.unige.ch
¶Electronic address: thierry.pun@cui.unige.ch

I. INTRODUCTION

Identifying people and protecting access or privileges to specific resources are among current needs of our modern society. Generally, an *authority* may *grant* certain rights to individuals, and provides these individuals with an *identification document*. When such a *person* desires to exercise these rights, there will be a *challenger* who, as the name suggests, defies the rights of the person. The person then presents the provided identification document to the challenger as a certificate that this person has the required rights. The challenger must then make a decision: either the presented identification document is valid, or it is not.

A problem is that technological advancements can be used by *attackers* for malicious purposes, including attempts to duplicate, alter or otherwise manipulate identification documents to circumvent the regular system of verification of rights. In order to make a correct decision, the procedures and technical aspects of identification documents must be sufficiently advanced to prevent attackers from succeeding.

Current systems for authorization of persons are based on secure identification documents. Ways to secure such documents include the use of special inks [1], special paper [2], anti-copying visible patterns [3], embedded holograms or microtext [4]. Besides the high cost of these methods, usually expensive equipment is required to perform a validation of a document that is protected with these methods; thus rendering the cost prohibitive for some applications, as well as limiting the possibility of verification to a restricted circle of authorized parties. Moreover, most of these techniques are based on proprietary designs, which considerably restricts the usage of cryptographic principles.

The security of person identification requires a theoretic investigation of several issues. The theoretic aspects of biometric fusion have been investigated thoroughly in [5]. However, any secure solution also needs to address the issue of document security. The current state-of-the-art in the domain of document authentication is lacking a thorough theoretical framework which guides the design of practical secure authentication systems with the required accuracy of performance, usually measured in terms of probability of error in decision making. Secondly, such a framework can be used for benchmarking of various existing techniques. We propose a novel low-cost approach to document security, and particularly authentication, based on data-hiding and perceptual hashing, biometrics and portable de-

vices with optic equipment and present an information-theoretic analysis of the proposed approach.

The rest of this paper is organized as follows. Section II presents an overview of existing identification frameworks. Section III states requirements to a modern approach to identification based on biometrics and identification documents. In Section IV a theoretic analysis of the problem and models of an identification framework are presented. A practical setup is proposed in Section V. To demonstrate the feasibility of the approach, Section VI shows experimental results. Finally, we draw conclusions and suggest future work in Section VII.

A. Notations

We use small or capital letters for constants, deterministic variables, and function names. We use capital letters, e.g., X, to denote scalar random variables, capital letters with a superscript, e.g., X^N, to denote vector random variables of length N, and corresponding small letters, e.g., x and x^N, to denote their realizations. The probability mass (respectively density) function or p.m.f. (respectively p.d.f.) of a discrete (respectively continuous) random variable X is denoted by $p_X(\cdot)$ (respectively $f_X(\cdot)$). When no confusion is possible we write $p(x)$ (respectively $f(x)$) instead of $p_X(x)$ (respectively $f_X(x)$). We use $X \sim p_X(\cdot)$ to indicate that the random variable X is distributed according to $p_X(\cdot)$. Calligraphic letters $\mathcal{X}$ denote sets and $|\mathcal{X}|$ denotes the cardinality of $\mathcal{X}$. The relative entropy between probability distributions $p(\cdot)$ and $q(\cdot)$ is denoted as $D(p||q)$, the mutual information between random variables X and Y by $I(X;Y)$. The concatenation of two vectors a^{N_1} and b^{N_2} is denoted as $[a^{N_1}, b^{N_2}]$.

II. IDENTIFICATION FRAMEWORKS

A. Biometrics

Historically, person identification has been based on: 1) what a person possesses, such as a document or a card; 2) what a person knows, for example, a password or personal identification number – PIN; or 3) biometrics, inherent physiological or behavioral characteristics. A classical identification document belongs to the first category. However, possessing a card is usually not sufficient to guaranty that a given person is its legitimate owner, since cards

can always be stolen and misused. This is why identification documents usually contain information that links them to their legitimate holder – usually a photograph, and possibly other biometric data such as a handwritten signature or a fingerprint.

In general, typical *biometrics* that can be used are: facial features, fingerprints, hand geometries, iris patterns, retinal scans, voice samples, handwritten signature dynamics or DNA characterization [6]. Biometric identification is based on the unique nature and extreme richness of the human features enumerated above. Photographs present on passports or ID cards can be seen as analog biometrics, as well as fingerprints, which have been used by the police for criminal investigation since the late 19th century.

Biometrics-based person identification is believed to achieve the highest security and reliability. It appears today that biometrics could be used for person identification and access control in banking, border control, loyalty programs, time and attendance monitoring, etc. During the last few years significant efforts have been devoted to theoretical investigations as well as to the development of practical methods for identification document security and biometrics-based person identification [7–9].

B. Personal Data

We refer to *personal data* as any information in an identification document that is not a representation of biometric data, but rather any information in text form. The personal data can typically include a name, position, date of birth, contact information, etc.; and one or more identifiers, such as any number, code or time-stamp. Such an identifier may be used to uniquely identify the document itself, where and when it was issued, the authority which issued it to the specified person; or to provide a link to other sources of information associated with the ID holder. The challenger might use this external information about either the identification document or the person in the decision process. Typically, personal data are printed in clear form on the document. More recently, personal data are additionally stored in an encrypted form for machine-based inspection.

C. Document-based Identification

A complete setup of the assumed framework for authorization of people is depicted in Figure 1. According to the assumed framework, the role of an identification document is to prove that a given person has been authorized by an authority. As such, the identification document is of critical importance to the proper functioning of the system.

For the challenger, the mere existence of an identification document should not be sufficient to consider it a proof that the person holding it is indeed authorized. As explained in Section II A, the document needs to be linked to the intended holder. Using biometrics, it is assumed that this task can be performed up to sufficient accuracy. In our assumed setup, the biometric data is present on the ID document and the challenger is expected to verify that this data is indeed linked to the person to be identified. This task could be performed with a mobile device with biometric verification capabilities similar to those of the SecurePhone [10]; the biometric data would be on the ID document instead of on a SIM card.

Once the challenger has established that the document is indeed related to the person, a decision could be made using the available information, as detailed in Section II B, regarding the authenticity of the document and the authorization of the person. We will not go into the details of the authorization here, but assume that this can successfully be handled once the identification document has been authenticated. The open issue to address is then to find a convenient *document security* framework that the challenger can use to verify that the presented document is authentic, i.e., it is truly an original document provided by the authority.

Even though a document might be an original provided by the authority, this does not mean that it is unmodified. We define *legitimate* distortions as modification such as normal wear and tear, scratching, and operations carried out as part of the normal handling such as printing and scanning. Legitimate distortions introduced by normal handling are expected to preserve a sufficient degree of quality of the document to carry out verification procedures; i.e. a few scratches are acceptable, but scratching out an entire image is clearly not.

An *illegitimate* document is a document that is not at all provided by the authority, or a document that has illegitimate distortions, by which we mean that is has undergone a modification that is not legitimate. This would be any form of modifications whereby insufficient document quality is preserved, leading the challenger to the wrong decision

regarding the document's authenticity. For example, a possible attack scenario would be to replace or modify the personal or biometric data on an identification document. Because in habitual identification documents a cross-link between the personal and the biometric data is absent, the probability of making an incorrect decision is increased. We propose to add such a protective link using digital data-hiding and robust perceptual hashing technologies in order to increase the accuracy of modern person identification systems.

D. Document Security

Modern achievements in digital technologies allowed enhancing the security of modern identification documents. Due to reasons of durability and security, these documents are often produced on plastic carriers using laser engraving. Moreover, plastic-based documents make it possible to easily and securely integrate electronic devices, such as smart chips, magnetic stripes or radio frequency identification devices (RFIDs) for the storage of biometrics and personal data. At the same time, all these innovations introduce some important open issues. First, there is the issue of privacy and disclosure of a person's biometrics. Secondly, devices such as RFIDs can leak information about the personal data, can be used for tracking people, or even can be used to activate a bomb when the document holder with a specified RFID is in the sensitivity zone, since the information stored in it can be read remotely [11]. Consequently, more secure cryptographic algorithms and identification protocols that additionally protect biometrics in digital form require high-capacity storage devices. To satisfy all these constraints various system architectures are deployed in practice.

The appearance of cheap but powerful computers, color printers and scanners implies that criminal groups are increasingly able to create fake identification documents.

At the same time, the technological advances allow the use of more advanced techniques in the design of authentication systems. Many analog security techniques such as holograms, security threads and optically variable material have been developed as countermeasures on proprietary bases. These techniques are becoming obsolete, as counterfeiters benefit from the progress in digital imaging technologies. This is why there has been a significant research effort in biometrics-based person identification these last years, which is believed to achieve higher security and reliability. The urgent need for a solution to these problems is recognized by the security industry and the research community. As a possible solution we

consider digital data-hiding, a well-established and powerful tool in many multimedia security applications, and robust perceptual hashing of biometrics and personal data. Moreover, we propose a framework where document authentication is performed on public omnipresent mobile devices, such as mobile phones or PDAs, contrary to proprietary devices available only for particular or experienced users.

III. REQUIREMENTS AND PROPOSED APPROACH

A. Mobile Device Architecture

The use of digital technologies, networks and computers, and the increasing dynamics and mobility in the modern world recently revealed unprecedented threats leading to an urgent need for securing identification documents. Among the major security issues, initially pointed out in Section II D, the most important are: the ease with which exact copies of digital content can be produced without authorization; the effectiveness with which high quality counterfeit identification documents can be made with common document editing tools; and the ease with which the true originator or owner of a document can be faked for fraudulent purposes. In spite of their different origins, all the above problems have many common features that can be exploited for the optimal design of security systems. Consequently, there is a great interest in the theoretical investigation of these systems and the main principles of their design.

Despite the increasing risk of fraud, identification documents still remain the most widely used means of person identification. Thus, there is a great need for systems that allow accurate and quick document authentication. In this work, we propose a unified system architecture dealing with the protection of identification documents and allowing to establish their authenticity.

Hence, any system that handles the verification procedure should be able to do this remotely. The proposed system architecture is shown in Figure 2. The identification document is acquired using the sensors of a portable device, e.g., a digital camera. The resulting image is sent to an authentication server, which either directly establishes the document's authenticity, or compares the sent data with those stored in a database in order to reach a decision. The verification result is sent back to the portable device and displayed for the

end-user.

B. Identity Document Designs: link between biometrics and personal data

As discussed in II C, the identification document should create a link between the physical person and the personal data. One can consider three practical variants of identification documents with a secure link between biometrics and personal data: 1) a *remote database* as in Figure 3(a), 2) an *on-document storage module* (SM) as in Figure 3(b) or 3) *self cross-storage* based on digital data-hiding and perceptual hashing, as in Figure 3(c).

In the first variant, the system performs a comparison of biometrics and personal data with those stored in a trusted remote database. This approach requires keeping a database and a real-time connection during the identity checking. Keeping a remote database can be impractical and raises privacy issues in many other common scenarios as gathering information about people is restricted under current laws in most of the western world [12].

The two remaining architectures consist in the storage of the link between the biometrics and of the personal data directly on the identification documents. In this case, the link should be stored in a way that is resistant against counterfeiting. The second system is based on a secure storage module, that can be an electronic chip (smart cards), a bar code printed or laser engraved on the document surface, readable optical storage modules and more recently RFIDs.

The third system does not need any additional physical modules or devices to link biometrics to personal data. It uses recently proposed digital data-hiding techniques that can create a reliable cross-link between biometrics and personal data. One of the main advantages of these two architectures is the possibility to adapt them to most existing classical frameworks based on authentication documents and smart cards. Additionally, it does not require a change of the document layout, which is an important factor for standardization. Another advantage of storing biometrics and the link to personal data on the document itself is the possibility to perform fast and convenient identity verification without the need for a direct link with a centralized database. Moreover, better privacy could be achieved by holding all the private information on the document itself. For example, since October 2004, the US Secretary of State requires machine readable passport for travelers entering the country without a visa under the Visa Waiver Program (VWP) [13]; the Departments

of Homeland Security and of State requested an extension consisting of the inclusion of biometric features in passports issued by countries-participants of the VWP. Identification documents based on self-stored or self-embedded biometrics to make them less vulnerable with respect to illegal use or tampering are probably the main trend to be followed by most governments.

Moreover, a multimodal biometrics system can benefit from data-hiding techniques to achieve *cross-modality* information embedding, meaning that the information from one mode can be embedded into one or several other modes [14], [15]. By making multiple links between the different modes, such cross-modality renders the system even more difficult to break. The basic idea of our framework is then to generate an identification document, which links the document with the authority who generated it and to the document's holder, and add a link between the biometric and personal data. This link is based on data-hiding in the different modalities, where each piece of information stores extra data about its complement. Taking into account the limited embedding rate compared to the available information to embed, we propose not to embed the entire data of one modality into the other, but either a compressed and encrypted form, or a hash. Based on the requirement for robustness against legitimate distortions, robust perceptual hashes are an interesting option, which will be explored further in Section V B.

One advantage of such a design is related to the document manufacturing and personalization that can be combined in one technological step. This facilitates document production and leads to cost reductions. Note that some of the elements from the two categories above are physically printed on the document in clear form for visual inspection. The printed elements could be textual personal data, the document ID, as well as a photograph of the face and the handwritten signature. The backward compatibility of the proposed approach with classical identification documents relies on these printed data, which we will refer to as "human-readable data". On the opposite, for automatic document verification *all* the data elements listed above need to be encoded in some way and embedded in the document using digital data-hiding. The watermark could be embedded either on the whole document area (including its background), into the printed photograph and in text data. The retained data hiding technique depends on its maximal embedding rate with respect to the amount of information to embed, as well as on the desired level of robustness.

The authentication relies on the encryption of the hidden data in an asymmetrical man-

ner with the private key of the authority issuing the document. Any asymmetrical cryptographic/digital signature scheme can be used for this purpose like RSA [16], DSA [17], or the more recent Elliptic Curve (EC) schemes [18]. Based on printed elements and hidden data, a system performs the authentication of a document. As was mentioned in Section II D, the authentication of an identification document should not rely on proprietary devices, which are difficult to standardize and distribute world wide. Recent trends in identification documents design consider publicly available devices such as mobile phones and PDAs. That is why one should match the security and storage requirements of identification protocols and digital data-hiding technologies with the imaging facilities of portable devices. Development of such protocols and data-hiding technologies is a great challenge and a subject of intensive research in the cryptographic and watermarking community [19].

Due to the desire to use portable devices such as mobile phones in the architecture, self cross-storage based on digital data-hiding is an attractive solution and will be explored in further detail.

IV. THEORETICAL ANALYSIS AND MODELS

We believe that despite the apparent variety of existing person identification systems based on biometrics, data-hiding, and robust perceptual hashing technologies, only a few powerful basic principles can be used to theoretically analyze and guide the design of these systems. The task of identifying, introducing and applying these fundamental principles is a great challenge. In this context, the goal of the present section is to develop a new framework for the theoretical analysis of document authentication systems using the strict apparatus of information theory and the recent advances in digital data-hiding. The necessity for such a general framework is dictated by the current requirements of document security systems that cannot be fulfilled based on the traditional means of analog and proprietary security.

A. Authentication of Biometric Identification Documents

We consider the problem of authenticating a document that holds biometric and personal data from an information-theoretic point of view. The generic block diagram of an authentication system meant to solve this problem is shown in Figure 4.

The authentication authority or encoder Φ has access to the uniquely assigned secret key K that is uniformly distributed over the set $\mathcal{K} = \{1, 2, \ldots, |\mathcal{K}|\}$, the non-causal realization of biometric data $X_1^{N_1} \in \mathcal{X}_1^{N_1}$, and the personal data $X_2^{N_2} \in \mathcal{X}_2^{N_2}$. As explained in Section II A, $X_1^{N_1}$ can be any personal biometric. On the other hand, as detailed in Section II B, $X_2^{N_2}$ corresponds to any personal information that can be represented in text form. The key K, the biometric data $X_1^{N_1}$, and the personal data $X_2^{N_2}$ are used at the encoder Φ to generate the tamper resistant data $Y_1^{N_1} \in {\mathcal{Y}_1}^{N_1}$ and $Y_2^{N_2} \in {\mathcal{Y}_2}^{N_2}$. The tamper resistant data $(Y_1^{N_1}, Y_2^{N_2})$ are communicated through a channel, which introduces some legitimate or illegitimate distortions described by two transition probabilities $p(v_1^{N_1}|y_1^{N_1})$ and $p(v_2^{N_2}|y_2^{N_2})$. The resulting distorted data are denoted $V_1^{N_1} \in {\mathcal{V}_1}^{N_1}$ and $V_2^{N_2} \in {\mathcal{V}_2}^{N_2}$. The challenger or decoder Υ makes a decision about the authenticity of the biometric identification document using $(V_1^{N_1}, V_2^{N_2})$ and K. Thus, the document authentication system consists of the set $\{\mathcal{X}_1^{N_1}, \mathcal{X}_2^{N_2}, \mathcal{K}, \mathcal{Y}_1^{N_1}, \mathcal{Y}_2^{N_2}, p(v_1^{N_1}|y_1^{N_1}), p(v_2^{N_2}|y_2^{N_2}), \mathcal{V}_1^{N_1}, \mathcal{V}_2^{N_2}\}$, the encoder's allowable distortions D^{E_i} between $X_i^{N_i}$ and $Y_i^{N_i}$, the attacking channel allowable distortions D^{A_i} between $Y_i^{N_i}$ and $V_i^{N_i}$, and the encoder-decoder pair $\Phi : \mathcal{X}_1^{N_1} \times \mathcal{X}_2^{N_2} \times \mathcal{K} \to \mathcal{Y}_1^{N_1} \times \mathcal{Y}_2^{N_2}, \Upsilon : \mathcal{V}_1^{N_1} \times \mathcal{V}_2^{N_2} \times \mathcal{K} \to \{0, 1\}$, where $i = 1, 2$.

The problem of deciding whether the received data $(V_1^{N_1}, V_2^{N_2})$ are authentic or not can be considered as a binary hypothesis testing problem. One can assume that H_0 corresponds to the hypothesis that the received data are authentic, and H_1 to the alternative hypothesis. Thus, the task of the authentication system is to decide which of the two hypotheses should be accepted given the realizations $(v_1^{N_1}, v_2^{N_2})$ and k. The hypothesis test problem can be stated as:

$$\begin{cases} H_0 : \ (V_1^{N_1}, V_2^{N_2}|K = k) \sim p^0_{V_1^{N_1}, V_2^{N_2}|K}(v_1^{N_1}, v_2^{N_2}|k), \\ H_1 : \ (V_1^{N_1}, V_2^{N_2}|K = k) \sim p^1_{V_1^{N_1}, V_2^{N_2}|K}(v_1^{N_1}, v_2^{N_2}|k), \end{cases} \tag{1}$$

where H_0 corresponds to the decision 0 and H_1 to 1.

Various tests can be performed such as the Bayessian, minimax or Neyman-Pearson tests; however, we will use the optimal Neyman-Pearson test due to the particularities of the authentication problem, which are discussed below. Disregarding the chosen testing strategy, two types of errors are possible: a type I error or false alarm (F) occurs, if an authentic document is decided to be a fake, and a type II error or miss (M) occurs, if a counterfeited document is considered to be authentic.

According to the Neyman-Pearson test, the goal of the authentication system is to keep

the probability P_F of false alarm fixed and to minimize the probability P_M of missing a counterfeited document. Contrarily, the objective of the counterfeiter is to modify the document keeping the modifications in the specified ranges of allowable distortions in such a way that P_M is maximized. These conflicting requirements can be formulated as a game between the system designer and the attacker:

$$\min_{\Phi,\Upsilon} \max_{p_{V_1^{N_1},V_2^{N_2}|Y_1^{N_1},Y_2^{N_2}}(.|.)} P_M(\Phi,\Upsilon,p_{V_1^{N_1},V_2^{N_2}|Y_1^{N_1},Y_2^{N_2}}(.|.)), \tag{2}$$

which depends on the particular encoder/decoder pair Φ,Υ, and the attacking channel $p_{V_1^{N_1},V_2^{N_2}|Y_1^{N_1},Y_2^{N_2}}(.|.)$.

The Neyman-Pearson test states that for a given maximal tolerable probability P_F, P_M can be minimized by declaring hypothesis H_0 if, and only if, the log-likelihood ratio $\ell(v_1^{N_1},v_2^{N_2}|k)$, defined as:

$$\ell(v_1^{N_1},v_2^{N_2}|k) \triangleq \log_2 \frac{p^0_{V_1^{N_1},V_2^{N_2}|K}(v_1^{N_1},v_2^{N_2}|k)}{p^1_{V_1^{N_1},V_2^{N_2}|K}(v_1^{N_1},v_2^{N_2}|k)}, \tag{3}$$

satisfies:

$$\ell(v_1^{N_1},v_2^{N_2}|k) \geq T, \tag{4}$$

for some threshold T.

We define the corresponding probabilities of false alarm and miss for a given key k as:

$$P_M(k) \triangleq \Pr[\ell(v_1^{N_1},v_2^{N_2}|k) \geq T|H_1], \tag{5}$$

$$P_F(k) \triangleq \Pr[\ell(v_1^{N_1},v_2^{N_2}|k) < T|H_0]. \tag{6}$$

The conditional relative entropy or discrimination $D(p^0_{V_1^{N_1},V_2^{N_2}|K}||p^1_{V_1^{N_1},V_2^{N_2}|K})$, defined as the expected value of the log-likelihood function in (3) with respect to $p^0(v_1^{N_1},v_2^{N_2},k)$, measures the level of distinguishability between the two involved distributions:

$$D(p^0_{V_1^{N_1},V_2^{N_2}|K}||p^1_{V_1^{N_1},V_2^{N_2}|K}) = \sum_{\substack{k\in\mathcal{K} \\ (v_1^{N_1},v_2^{N_2})\in\mathcal{V}_1^{N_1}\times\mathcal{V}_2^{N_2}}} p_K(k)p^0(v_1^{N_1},v_2^{N_2}|k)\log_2\frac{p^0(v_1^{N_1},v_2^{N_2}|k)}{p^1(v_1^{N_1},v_2^{N_2}|k)}, \tag{7}$$

where $p_K(k)$ is the distribution of K on $\mathcal{K}$ that can be assumed to be uniform, i.e. $p_K(k) = 1/|\mathcal{K}|$.

In this case, the average error probabilities $P_F = \sum_{k\in\mathcal{K}} p_K(k)P_F(k)$ and $P_M = \sum_{k\in\mathcal{K}} p_K(k)P_M(k)$ satisfy [20]:

$$P_M \log_2 \frac{P_M}{1-P_F} + (1-P_M)\log_2 \frac{1-P_M}{P_F} \leq D(p^0_{V_1^{N_1},V_2^{N_2}|K} || p^1_{V_1^{N_1},V_2^{N_2}|K}). \tag{8}$$

Fixing $P_M = 0$, one can obtain a lower bound on the probability of false alarm:

$$P_F \geq 2^{-D(p^0_{V_1^{N_1},V_2^{N_2}|K} || p^1_{V_1^{N_1},V_2^{N_2}|K})}. \tag{9}$$

The above authentication system can be considered in the scope of a *hashing and data-hiding problem*. There are several possible system designs based on *separation* or *joint* principles as an analogy to Shannon's source-channel communication problem. Here, one faces the same problems of performance optimality, complexity as well as the issue of security. Since the optimal system structure still remains an open theoretical problem, we will focus on the separation approach in this paper, leaving the solutions to the above issues subject of future research.

B. Authentication Using Cross-Storage of Hashes

In this section, we consider in detail all the elements of an authentication system based on the separation of robust perceptual hashing and data-hiding. The considered identification document uses self cross-storage of hashes as described in Section III B.

Let us again assume $i = 1, 2$. Referring to Figures 5 and 6, the encoder has access to the host data $X_i^{N_i}$ and to the uniquely assigned secret keys K_H^i and K_{DH}^i, which are uniformly distributed over the sets $\mathcal{K}_H^i = \{1, 2, \ldots, |\mathcal{K}_H^i|\}$ and $\mathcal{K}_{DH}^i = \{1, 2, \ldots, |\mathcal{K}_{DH}^i|\}$ for hashing and data hiding, respectively. We assume that $X_i^{N_i} \sim p_{X_i^{N_i}}(\cdot)$. The secret key K_H^i and the host data $X_i^{N_i}$ are used to generate a hash message M_{3-i} that is encoded into the watermark $W_i^{N_i}$ based on $X_i^{N_i}$ and the secret key K_{DH}^i. The watermark $W_i^{N_i}$ is embedded into the host data $X_i^{N_i}$, resulting in the watermarked data $Y_i^{N_i}$. The watermarked data $Y_i^{N_i}$ is communicated through the channel $p(v_i^{N_i}|y_i^{N_i})$, which introduces some legitimate or illegitimate distortions. For authenticating the document, the decoder outputs $\hat{M}_i$, an estimate of M_i, based on the distorted data $V_i^{N_i}$ and K_{DH}^i. Additionally, the hash $\hat{M}_i'$ is computed from $V_i^{N_i}$ and K_H^i. Finally, the decision about the authenticity of $(V_1^{N_1}, V_2^{N_2})$ is made based on the comparison of $(\hat{M}_1, \hat{M}_2)$ with $(\hat{M}_1', \hat{M}_2')$. We assume that the hash message $M_i \in \mathcal{M}_i$ and the hash

$M_i' \in \mathcal{M}_i'$ are uniformly distributed over $\mathcal{M}_i = \{1, 2, \ldots, |\mathcal{M}_i|\}$ and $\mathcal{M}_i' = \{1, 2, \ldots, |\mathcal{M}_i'|\}$, respectively. We also assume that $|\mathcal{M}_i| = 2^{N_i R_{DH}^i}$ and $|\mathcal{M}_i'| = 2^{N_{3-i} R_H^{3-i}}$, where R_{DH}^i is the data-hiding rate, R_H^{3-i} is the hashing rate, and N_i is the length of all the involved vectors $X_i^{N_i}$, $W_i^{N_i}$, $Y_i^{N_i}$ and $V_i^{N_i}$.

The distortion function is defined as $d(x^N, y^N) = \frac{1}{N}\sum_{i=1}^{N} d(x_i, y_i)$, where $d(x_i, y_i) : \mathcal{X} \times \mathcal{Y} \to \mathcal{R}^+$ denotes an element-wise distortion metric between x_i and y_i.

Definition 1: A *discrete memoryless data-hiding channel* (see Figure 7) consists of four alphabets $\mathcal{X}_i$, $\mathcal{W}_i$, $\mathcal{Y}_i$, $\mathcal{V}_i$, a probability transition matrix $p(v_i^{N_i}|w_i^{N_i}, x_i^{N_i})$ that corresponds to the covert communication of the watermark $W_i^{N_i}$ through the host image $X_i^{N_i}$ (channel $p(y_i^{N_i}|w_i^{N_i}, x_i^{N_i})$), and the attacking channel $p(v_i^{N_i}|y_i^{N_i})$ such that:

$$p(v_i^{N_i}|w_i^{N_i}, x_i^{N_i}) = \sum_{y_i^{N_i} \in \mathcal{Y}_i^N} p(y_i^{N_i}|w_i^{N_i}, x_i^{N_i}) p(v_i^{N_i}|y_i^{N_i}). \tag{10}$$

The attacking channel is subject to the distortion constraint D^{A_i}:

$$\sum_{y_i^{N_i} \in \mathcal{Y}_i^N} \sum_{v_i^{N_i} \in \mathcal{V}_i^N} d(y_i^{N_i}, v_i^{N_i}) p(v_i^{N_i}|y_i^{N_i}) p(y_i^{N_i}) \leq D^{A_i}, \tag{11}$$

where:

$$p(v_i^{N_i}|y_i^{N_i}) = \prod_{j=1}^{N_i} p_{V_i|Y_i}(v_{ij}|y_{ij}). \tag{12}$$

Definition 2: A $(2^{N_i R_{DH}^i}, N_i)$ code for the data-hiding channel consists of a *message set* $\mathcal{M}_i = \{1, 2, ..., 2^{N_i R_{DH}^i}\}$, an *encoding function*:

$$f_i^{N_i} : \mathcal{M}_i \times \mathcal{X}_i^{N_i} \times \mathcal{K}_{DH}^i \to \mathcal{W}_i^{N_i}, \tag{13}$$

an *embedding function*:

$$\psi_i^{N_i} : \mathcal{W}_i^{N_i} \times \mathcal{X}_i^{N_i} \to \mathcal{Y}_i^{N_i}, \tag{14}$$

subject to the embedding distortion constraint D^{E_i}:

$$\frac{1}{|\mathcal{K}_{DH}^i||\mathcal{M}_i|} \sum_{k_{DH}^i \in \mathcal{K}_{DH}^i} \sum_{m_i \in \mathcal{M}_i} \sum_{x_i^{N_i} \in \mathcal{X}_i^{N_i}} d(x_i^{N_i}, \psi_i^{N_i}(f_i^{N_i}(m_i, x_i^{N_i}, k_{DH}^i), x_i^{N_i})) p_{X_i^{N_i}}(x_i^{N_i}) \leq D^{E_i}, \tag{15}$$

and a *decoding function*:

$$g_i : \mathcal{V}_i^{N_i} \times \mathcal{K}_{DH}^i \to \mathcal{M}_i. \tag{16}$$

We define the *average probability of error* for a $(2^{N_i R^i_{DH}}, N_i)$ code as:

$$P_e^{(N_i)} = \frac{1}{|\mathcal{K}^i_{DH}||\mathcal{M}_i|} \sum_{k^i_{DH} \in \mathcal{K}^i_{DH}} \sum_{m_i \in \mathcal{M}_i} \Pr\left\{ g(V_i^{N_i}, K^i_{DH}) \neq m_i | K^i_{DH} = k^i_{DH}, M_i = m_i \right\}. \quad (17)$$

Definition 3: A rate $R^i_{DH} = \frac{1}{N_i} \log_2 |\mathcal{M}_i|$ is achievable for distortions (D^{E_i}, D^{A_i}), if there exists a sequence of $(2^{N_i R^i_{DH}}, N_i)$ codes with $P_e^{(N_i)} \to 0$ as $N_i \to \infty$.

Definition 4: The capacity of the data-hiding channel is the supremum of all achievable rates for distortions (D^{E_i}, D^{A_i}).

Theorem 1 (data-hiding capacity for a fixed channel) [21]: A rate R^i_{DH} is achievable for the distortion D^{E_i} and the fixed attacking channel $p(v_i|y_i)$ with bounded distortion D^{A_i}, iff $R^i_{DH} < C_i$, where:

$$C_i = \max_{p(u_i, w_i|x_i)} \left[I(U_i; V_i) - I(U_i; X_i) \right], \quad (18)$$

and U_i is an auxiliary random variable distributed over the set $\mathcal{U}_i$, with $|\mathcal{U}_i| \leq |\mathcal{X}_i||\mathcal{W}_i| + 1$.

Definition 5: A hash code consists of a *hash set* $\mathcal{M}'_{3-i} = \{1, 2, ..., 2^{N_i R^i_H}\}$ and a *hash function*:

$$\xi_i : \mathcal{X}_i^{N_i} \times \mathcal{K}^i_H \to \mathcal{M}'_{3-i}. \quad (19)$$

The construction of a hash should satisfy several conflicting requirements. The hash function produces the secure hash index $M'_{3-i} \in \mathcal{M}'_{3-i}$, i.e. a hash value, given K^i_H and $X_i^{N_i}$. Contrarily to classical hashing [18], where two vectors that differ in only a single bit have independent hash values, we require that two vectors $X_i^{N_i}$ and $X_i'^{N_i}$ that are perceived (respectively, understood) by the observer (respectively, by the reader) to be similar in a perceptual sense have the same hash value. In practice, it also means that if a vector $X_i'^{N_i}$ is obtained via a mapping $p(x'^{N_i}_i | x_i^{N_i})$ of $X_i^{N_i}$, where $E[d(X_i^{N_i}, X_i'^{N_i})] \leq D^{A_i}$, i.e., the distance between the two vectors is not greater than a maximum distortion value D^{A_i}, one should expect $\xi(K_H, X_i^{N_i}) = \xi(K_H, X'^{N_i}_i)$. Additionally, the hash should be secure in the sense that having the host data $X_i^{N_i}$, the attacker cannot generate a hash without the knowledge of the secure key K^i_H.

Definition 6: An authenticator is defined as a binary decision $\{0, 1\}$ based on the mapping:

$$\eta : (\mathcal{M}_1 \times \mathcal{M}_2) \times (\mathcal{M}'_1 \times \mathcal{M}'_2) \to \{0, 1\}. \quad (20)$$

The authentication amounts to select one of the two hypothesis $\{H_0, H_1\}$ based on the binary representations of the hashes computed from the observed data $(V_1^{N_1}, V_2^{N_2})$, namely

$(\hat{M}_1', \hat{M}_2') \equiv (\hat{\mathbf{B}}_1', \hat{\mathbf{B}}_2')$, and those from the decoded messages $(\hat{M}_1, \hat{M}_2) \equiv (\hat{\mathbf{B}}_1, \hat{\mathbf{B}}_2)$, where $\mathbf{B}$ stands for the binary representation of M. The binary decision $\{0, 1\}$ is taken by comparison of the number of different bits between $[\hat{\mathbf{B}}_1 \hat{\mathbf{B}}_2]$ and $[\hat{\mathbf{B}}_1' \hat{\mathbf{B}}_2']$ with respect to a predefined threshold $T(P_F)$.

It is straight-forward to show [22] that if $X_1^{N_1}$ and $X_2^{N_2}$ are finite alphabet stochastic processes that satisfy the asymptotic equipartition property (AEP) [23], then there are hashing and data-hiding codes with specified average probability of false alarm P_F and vanishing average probability of miss P_M as $N_1 \to \infty$ and $N_2 \to \infty$, if the rates of the hashing and data-hiding codes R_H^1, R_H^2, R_{DH}^1 and R_{DH}^2 satisfy $R_H^1 \leq R_{DH}^2 \leq C_2$ and $R_H^2 \leq R_{DH}^1 \leq C_1$.

In the following Section, we detail practical constructions of data-hiding and robust perceptual hashing schemes that can be used as building blocks for the proposed authentication system.

V. PRACTICAL SETUP FOR DOCUMENT AUTHENTICATION

A. Information Storage with Digital Data-Hiding

In the past decade, a number of data-hiding schemes were proposed in the literature. However, the majority of them deals only with digital image, audio or video documents [24]. Nonetheless, printed or electronic text documents are still the most common and unavoidable form of information communication among humans. For example, on identification documents the personal data are reproduced in text form.

One possible explanation of this situation is that text documents have a relatively small number of features that can be exploited in order to hide (or embed) information in comparison to other media documents. Indeed, a text document can be seen as a highly structured image which is precisely the kind of image to which the human visual system (HVS) is more sensitive. For the same reason, the data embedding rate in text documents is comparatively much smaller than that in images, audio or video.

Four major groups of methods for data-hiding in text documents have appeared in literature: *syntactic methods* [25, 26], where the diction or structure of sentences is transformed without significantly altering their meaning; *semantic methods* [25, 26], where words are

replaced by their synonyms and/or sentences are transformed via suppression or inclusion of noun phrase coreferences; *open space methods* [25, 27], where either inter-line or inter-word or inter-character spaces are modulated; and *character feature methods* [27–29], where features such as shape, size or position are manipulated.

However, syntactic and semantic methods are not suitable for all types of documents, including identification documents, and usually need human supervision. Open space methods can be automated, are robust against printing and scanning, but have low information embedding rates. On the other hand, existing character feature methods have higher information embedding rates but are less or not robust against printing and scanning. Since automation is very important for identification document authentication we will not consider syntactic or semantic methods.

Thus, the character feature methods seem to be the most promising for document identification assuming that their robustness can be improved. Recent studies [30–33] attempt to create a unified approach for text data-hiding based on the Gel'fand-Pinsker framework [21] of communications with side information for channels with random parameters. This resulted in the development of the so-called *color index modulation* (CIM) method, where the color or grayscale character features are used for data-hiding of documents stored in electronic or printed form. In this method, the gray shades are mapped to their halftone representation during document printing. This technique is fully automatable, has high information embedding rate, shows good resistance to printing and scanning, and can be applied to both digital and printed text documents. However, the main drawback of CIM techniques applied to protect analog documents is the low robustness to blurring and resolution reduction, which is of high importance for document identification using mobile phones where these distortions are highly likely to occur due to the limited quality of the optic equipment therein.

Notably, the Gel'fand-Pinsker framework is also the theoretical basis for the state-of-the-art practical image data-hiding techniques such as *quantization index modulation* (QIM) [34] and the *scalar Costa scheme* (SCS) [35].

According to the Gel'fand-Pinsker problem formulation [21], each component of the cover data $\{X_i\}$, $i = 1, 2, \cdots, N$, represents either an image element (pixel) or a text character. In the case of an image, X_i is either the gray shade or color of i^{th} pixel. In the case of a text, a character is defined as an element from a given alphabet $\mathcal{X}$ of alpha-numeric symbols. More

precisely, X_i should be considered as a data structure consisting of multiple quantifiable component fields (features): *shape, location, orientation, size, color,* etc. One must use the features that show the best resistance to the typical distortions of mobile phone imaging devices. In our previous research we have studied *color index modulation* that can be used for copy detection but is very sensitive to color manipulations [33]. One good candidate feature is *location* and the corresponding data-hiding technique is called *location index modulation* (LIM) shown in Figures 8 and 9 for the scalar and vector cases, respectively. In LIM, $x = \mathsf{A} = (x^h, x^v)$ is considered as the location of the involved character and $Q_m(x)$ as a location quantizer defining the character's new location.

B. Robust Perceptual Hashing

According to the system architecture shown in Figure 3c, the protection of the identification document is based on the cross-storage of biometrics and personal data. Since biometrics represent a relatively large amount of information stored in the form of images, the storage of this information inside the personal data is a great challenge due to the low embedding rate of text data-hiding techniques. Therefore, one can either compress the data and then encrypt it using proper cryptographic techniques, thus satisfying the security requirements with a resulting rate matching with the text data-hiding rate; or apply adequate cryptographic hashing. Both approaches share a common drawback: a high sensitivity to any change in the sense that any stream modification, even of a single pixel, causes a different result. The same is true for the personal data that should be stored inside the biometric data. Indeed, since the document authentication is performed using mobile imaging devices, which produce low quality images, the image data-hiding rate is also limited and a similar problem exists. That is why there is a great need for tolerant *visual* hash functions that are robust to legitimate changes. The idea of robust visual hashing is to generate a key-dependent secure digest, which continuously changes with the input and differs by at most a small number of bits for two distinct but perceptually equivalent inputs.

Robust hashing can be seen as a three-step operation: *feature extraction*, which is resistant/invariant to legitimate transformations; *randomization* of the extracted features, generally key-dependent, in order to achieve security; and *data reduction* (compression), which maps the randomized information to a shorter bit string representing the input data.

Sometimes, randomization is combined with compression or randomization in the form of XOR-ing is applied to the binary compressed data [36].

For the feature extraction from the visual input, we have to define what an "acceptable" alteration is, and which inputs can be considered as "perceptually equivalent". This aspect concerns both the type and the level of distortion we want to allow, and is dependent on the targeted application. The allowable distortions to which the selected features should be invariant could include signal processing changes such as slight lossy compression, signal fading, noise addition, grey-scale conversion, etc., as well as some classes of geometrical distortions.

1. Robust Visual Hashing for Images

Early tolerant visual hashing algorithms for images have been proposed by Schneider and Chang [37], which use features like edges, color/gray-scale histograms, or DCT coefficients; and by Brandt and Lin [38] which are also robust to translation, rotation, and scaling. Xie and Arce [39] extract information from edges using the DWT. Bhattacharjee and Kutter [40] extract perceptually interesting feature points that are not embedded within the image but are stored separately. Later Hel-Or *et al.* [41] proposed geometric hashing based on salient points and a voting algorithm; and Fridrich [42] proposed a function using the low-pass of DCT coefficients, which can be made invariant to translation, scaling and rotation using the Fourier-Mellin transform [43]. Another approach was considered by Monga and Evans [44], which extracts geometry preserving image features in order to generate the hash. Mihcak and Venkatesan [45] proposed an iterative visual hash algorithm based on repeated thresholding and spatial filtering. Lefbvre *et al.* [46] proposed the radon soft hash algorithm (RASH) in order to handle desynchronization and geometric distortions. Finally, Swaminathan *et al.* [47] developed a visual hash algorithm based on Fourier transform features and controlled randomization.

The randomization step, generally based on a key K, is essential, since the generated code should keep the same properties as a classical cryptographic hash function beside their continuous character: codes should be unpredictable for random inputs, and two completely different inputs should result into uncorrelated codes. In the case of keyed hashing, two different keys should also produce totally different codes. Fridrich [42] uses key-dependent

random matrices to randomize low-pass DCT, and Venkatesan *et al.* [48] propose a random tiling of the discrete wavelet transform (DWT) of the input prior to features extraction.

The data reduction step is analogous to lossy data compression, which reduces the length of the encoded features to a compact digest code. Both the randomization and the data reduction steps should preserve the continuous property of the input features. For this purpose these two steps could be done jointly rather than separately.

The verification is then done by counting the percentage of mismatching bits with a threshold representing the amount of allowed distortion.

Our design closely follows the design of Fridrich [49]. Let the image x^N be the realization of a vector random variable X^N. Let h^L be a hash of length L with key k_H, i.e. $h^L = \xi(x^N, k_H)$. Then, any h_b, that is, bit number b of h^L, is computed as follows. A mask α_b^N is generated from a uniform distribution $\mathcal{U}(-0.5, 0.5)$, dependent on k_H. Then for every b, we compute $\lambda_b = \sum_{j=1}^{N} \alpha_{bj} x_j$. Once values of λ_b have been computed for all $b \in \{1, \ldots, L\}$, we determine λ_m as the median of all λ_b. Then each bit b of the hash h^L is determined as:

$$h_b = \begin{cases} 0 & \text{if } \lambda_b < \lambda_m, \\ 1 & \text{otherwise.} \end{cases}$$

2. Robust Visual Hashing for Text

A robust text hashing function ξ takes as input a secret key k_H and an image of a text object x^N to give the hash value $h^L = \xi(k_H, x^N)$. The text object could be either a character, a word, a sentence, a paragraph, a line of text, a text fragment, or even the whole text document. The hash value h^L is required to be invariant under legitimate modifications of the text document such as conversion between electronic formats, data-hiding, and typical handling operations that include printing, scanning, photocopying, faxing, etc.

We will consider the OCR + MAC text hashing technique [33]. One attractive feature of this technique is that it is compatible with character feature text data-hiding methods such as CIM and LIM. This text hashing technique is based on optical character recognition (OCR) and a classical cryptographic message authentication code (MAC). The main idea is (see Figure 10) to apply OCR to the text document in order to obtain its ASCII representation; and then, using the secret key k_H, to compute the MAC of this representation in order to obtain the desired hash value. It was shown in [33] that this technique provides good

robustness against legitimate modifications and excellent detection of tampering if OCR is applied in character-by-character mode.

VI. EXPERIMENTAL RESULTS

In this section, we present the experimental results showing the plausibility of the proposed authentication system. In order to be as close as possible to reality, we take as model the current Swiss driving licence shown in Figure 11. According to this card model, we assume the person's image to be of size 320x400 pixels and the total number of text characters to be at least 200.

The different modules of the proposed system are the following:

1. OCR + MAC as text hashing technique,
2. CIM as text data-hiding technique,
3. Robust image hashing as described in Section V B 1,
4. Image data-hiding as described in [50].

For the implementation of OCR + MAC text hashing we used ABBYY FineReader as OCR tool and HMAC SHA-1 truncated to 64 bits as MAC. Since the used image data-hiding technique can reliably store 64 information bits, this implementation takes into account the rate requirement of the image data-hiding part of the authentication system, namely that $R_H^2 \leq R_{DH}^1$.

CIM was implemented using the parameters described in [32]. In particular, we used Arial font characters of size 10 pt and the quantizer set $Q_0(x) = 0$, $Q_1(x) = 46$. The detection was performed by combining the mean and variance metrics of each character's luminance as described in [51]. In order to ensure error-free decoding we employed an outer shortened BCH code with parameters $(n, k) = (192, 68)$, which was derived from the (255,131) BCH code with generator polynomial $g(D) = 2157133314715101512612502774421420241654 71$.

The used robust image data-hiding algorithm is fully described in [50]. For the considered application, this algorithm reliably stores 64 information bits on an image of size 320×400 at an image PSNR of 30 dB. All of the tested images were printed at the resolution of 300 ppi. These parameters make the watermarked image resistant to all legitimate distortions

including printing on paper using halftoning or on plastic using laser engraving as well as scanning or taking a picture using the digital camera of a mobile device.

The implementation of the robust image hashing algorithm presented in Section V B 1 is straight-forward. The algorithm was tested on images of size 320×400.

These modules were implemented separately and tested for the required conditions of document authentication. At this moment, all modules show very good performance when the identification document is printed using commodity printers and scanners. When using digital cameras of mobile phones consistent results were found for all the modules but the text data-hiding module which suffers from the introduced blurring. As possible countermeasures we propose the use of microlenses, higher quality digital cameras, or the use LIM for text data-hiding.

Most of the experimental results can be found in our previous publications [32, 33, 50] (see also [51] for further results on the CIM method). Therefore, we only report here the obtained results for the robust image hashing module, which are new.

Hashes of different lengths have been computed from 400 images, with 10 photo's each of 40 different subjects [52]. The Hamming distance between each possible pair of hashes of the same length has been computed. Ideally, for a given length L, the Hamming distance between the hashes of unrelated images is half the number of bits in the hash, i.e. $L/2$. Figure 12 shows histograms of Hamming distances between different images for hashes of different lengths. The graph clearly shows that the behavior of the hash function is approaching the ideal case with various rates that depend on the hash length. The hash can thus discriminate between images of different people.

The next step is to verify that the hash of an image can still be computed after a number of legitimate distortions. To verify this property, we have watermarked, printed and scanned 10 images [53], and then compared the output to the images without modifications. Essentially, the unmodified image is then the channel input, the channel output is the scanned image, and the channel is formed by the watermarking procedure, the printing process, and the optic equipment used for scanning. Based on the results shown in Figure 12 and taking into account the text data-hiding part of the authentication system, namely that $R_H^1 \leq R_{DH}^2$, we selected a hash length of 64 bits. The experiments have been repeated 100 times for different values of the key k_H, which, due to the construction of the hash, may lead to a different Hamming distance between the hashes of any two images. A histogram of the Hamming

distances between 64-bit hashes of images with an without legitimate distortions is shown in Figure 13, it is a delta-pulse as all these Hamming distances are zero. The histogram of Hamming distances for different images is shown for reference in the same figure. From this graph, it is clear that it is possible to define a threshold T, for example, $T = 2$, where images are considered equal if the Hamming distance between the hashes is smaller than T. These experiments show that, even with a simple approach to perceptual hashing, the security of identification documents can be enhanced by adding the proposed link between biometric and personal data, and that it is a viable approach due to its robustness.

A more detailed security analysis of the practical scheme is desirable. According to Kerckhoffs' principle, the security of the scheme depends only on the secret key. There are four keys used in our system, one for hashing the text, one for hashing the image, one for embedding into the text and one for embedding into the image. A brute-force attack would then require the attacker, in the possession of at least one valid document, to find four keys such that if both the image and text are hashed and the hashes embedded, then the end result is fully identical to the original document. Let us assume that the attacker can indeed determine whether the end result is correct or not. Looking at only one of the two hash-embed sequences, observe that a correct result can only be obtained if both keys are correct, which implies that the cardinality of the combined key space is the product of the cardinalities of the individual key spaces. The messages to be embedded, which are the hashes, can be at least 64 bits, and if we assume that the key space should not be larger than the message space, this would limit the total key space to no less than 128 bits for each pair.

Since the attacker's search for the secret keys can be facilitated by various kinds of available side information, we are planning to perform in the future a thorough security analysis of the system based on Shannon's equivocation measure [54]. In order to quantify the efforts of the attacker in revealing the secret keys, one can use the concept of unicity distance for the situation when multiple ID documents secured with the same keys are available. This analysis should provide the exact number ID documents that are necessary to reveal the secret keys without a single bit error. This analysis falls outside of the scope of this paper and, therefore, will be part of our future research.

Practical authentication system design is usually subject to a trade-off between robustness and security. Robustness refers to the system's capabilities to withstand a class of legitimate

distortions. It is usually provided by introducing a certain level of redundancy via repetitive information embedding and the use of error control codes. Security can be defined as follows: only an authorized user with knowledge of the secret key is granted the right to authenticate the data. It is guaranteed by the hashing part of the protocol, and, in terms of computational security, is measured by the length of the hash. Thus, by fixing the level of robustness, that simultaneously defines the embedding rate, one obtains the number of hash bits that can be reliably hidden. Oppositely, by fixing the number of hash bits one can deduce the number of block repetitions as well as the rate of the error control codes that equivalently define the class of distortions that the developed protocol is guaranteed to be resilient to.

VII. CONCLUSIONS AND FUTURE WORK

In this paper, we considered the problem of authentication of biometric identification documents via mobile devices such as mobile phones or PDAs. The proposed solution makes use of digital data-hiding in order to cross-store the biometric data inside the personal data and vice versa. Moreover, a theoretical framework was presented which enables the analysis of future authentication systems based on this approach and guides their design. In particular, we advocate the separation approach which uses robust visual hashing techniques in order to match the information rates of biometric and personal data to the rates offered by current image and text data-hiding technologies.

We also described practical schemes for robust visual hashing and digital data-hiding that can be used as building blocks for the proposed authentication system. These schemes share a common requirement, namely resistance to legitimate distortions to which the identification document may be subjected. The obtained experimental results show that the proposed authentication system constitutes a viable and practical solution when the document acquisition is performed using a CCD scanner.

In order to create a fully operational system, capable of working with mobile devices, additional research is required to improve the text data-hiding module. One possible solution can be the use of LIM, which we expect to be less sensitive to the blurring effects present in today's digital cameras of mobile devices. For a very significant part, this optic equipment defines the channel through which the data must pass, and therefor its behaviour should be studied in detail. Last but not least, we plan to analyze the system security against possible

attacks, especially those related to the used technologies.

Acknowledgments

This paper was partially supported by the Swiss National Science Foundation (SNF) professorship grants PP002–68653, 114613 and 200021-111643, the SNF Interactive Multimodal Information Management (IM2) project, and the European Commission through the IST program under contract IST-2002-507932 ECRYPT. The information in this document reflects only the authors' views, is provided as is and no guarantee or warranty is given that the it is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

---

[1] I. Cox, M. L. Miller, and J. A. Bloom, *Digital watermarking*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002.

[2] R. L. van Renesse, "Paper based document security – a review," in *Proceedings of the European Conference on Security and Detection*, April 1997, pp. 75–80.

[3] J. Picard, "Digital authentication with copy-detection patterns," in *Optical Security and Counterfeit Deterrence Techniques V. Edited by van Renesse, Rudolf L. Proceedings of the SPIE*, R. L. van Renesse, Ed., vol. 5310, June 2004, pp. 176–183.

[4] R. A. Steenblik and M. J. Hurt, "Unison micro-optic security film," in *Optical Security and Counterfeit Deterrence Techniques V. Edited by van Renesse, Rudolf L. Proceedings of the SPIE, Volume 5310, pp. 321-327 (2004).*, R. L. van Renesse, Ed., Jun. 2004, pp. 321–327.

[5] J. Kittler, "A framework for classifier fusion: Is it still needed?" in *Proceedings of the Joint IAPR International Workshops on Advances in Pattern Recognition*. London, UK: Springer-Verlag, 2000, pp. 45–56.

[6] A. K. Jain, "Biometric recognition: how do i know who you are?" in *Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference*, April 2004, pp. 3–5.

[7] L. Hong, A. Jain, and S. Pankanti, "Can multibiometrics improve performance?" in *1999 IEEE Workshop on Automatic Identification Advanced Technologies (AutoID´99)*, Summit, NJ, USA, October 1999, pp. 59–64.

[8] A. K. Jain, S. Prabhakar, and S. Chen, "Combining multiple matchers for a high security fingerprint verification system," vol. 20, pp. 1371–1379, 1999.

[9] A. Ross and A. Jain, "Information fusion in biometrics," vol. 24, no. 13, pp. 2115–2125, September 2003.

[10] R. Ricci, G. Chollet, M. Crispino, S. Jassim, J. Koreman, M. O.-D. A. Morris, S. Garcia-Salicetti, and P. Soria-Rodriguez, "The securephone: a mobile phone with biometric authentication and e-signature support for dealing secure transactions on the fly," in *Proceedings of Secrypt 2006, International Conference on Security and Cryptography*, Setúbal, Portugal, 2006, pp. 9–16.

[11] B. Schneier, "Rfid passports," in *International Herald Tribune*, October 4 2004.

[12] "Data privacy," http://en.wikipedia.org/wiki/Data_privacy, 2007.

[13] "Visa Waiver Program," Bureau of Consular Affairs, U.S. Dept. of State, 2004, http://travel.state.gov/visa/tempvisitors_novisa_waiver.html.

[14] A. K. Jain and U. Uludag, "Hiding fingerprint minutiae in images," in *Proceedings of 3rd Workshop on Automatic Identification Advanced Technologies (AutoID 2002)*, Tarrytown, NY, USA, March 14-15 2002, pp. 97–102.

[15] A. K. Jain, U. Uludag, and R. L. Hsu, "Hiding a face in a fingerprint image," in *Proceedings of 16th International Conference on Pattern Recognition (ICPR 2002)*, vol. 3, Quebec City, Quebec, Canada, August 11-15 2002, pp. 756–759.

[16] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," in *Communications of the ACM*, vol. 21, February 1978, pp. 120–126.

[17] N. I. of Standards and T. (NIST), "Digital Signature Standard (DSS)," February 2000, fIPS Publication 186-2.

[18] D. R. Stinson, *Cryptography, Theory and Practice*, 2nd ed. CRC, 2002.

[19] "Network of excellence in cryptology (ecrypt)," 2002-now.

[20] U. Maurer, "A unified and generalized treatment of authentication theory," in *Proc. 13th Symp. on Theoretical Aspects of Computer Science (STACS'96)*, ser. Lecture Notes in Computer Science, vol. 1046. Springer-Verlag, Feb. 1996, pp. 387–398.

[21] S. Gel'fand and M. Pinsker, "Coding for channel with random parameters," *Problems of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.

[22] S. Voloshynovskiy, O. Koval, R. Villán, E. Topak, J. Vila-Forcén, F. Deguillaume, Y. Rytsar, and T. Pun, "Information-Theoretic Analysis of Electronic and Printed Document Authentication," in *Proceedings of SPIE-IS&T Electronic Imaging 2006, Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, USA, January 15–19 2006.

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

[24] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking.* Morgan Kaufmann Publishers, Inc., San Francisco, 2001.

[25] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Systems Journal*, vol. 35, no. Nos 3&4, pp. 313–336, 1996.

[26] M. Topkara, C. Taskiran, and E. J. Delp, "Natural Language Watermarking," in *Proceedings of SPIE-IS&T Electronic Imaging 2005, Security, Steganography, and Watermarking of Multimedia Contents VII*, San Jose, USA, January 17–21 2005.

[27] J. T. Brassil, S. Low, and N. F. Maxemchuk, "Copyright protection for electronic distribution of text documents," *Proceedings of the IEEE (USA)*, vol. 87, no. 7, pp. 1181–1196, 1999.

[28] A. K. Bhattacharjya and H. Ancin, "Data Embedding in Text for a Copier System," in *Proceedings of the ICIP*, vol. 2, 1999, pp. 245–249.

[29] Q. Mei, E. K. Wong, and N. Memon, "Data hiding in binary text documents," in *Proceedings of SPIE, Security and Watermarking of Multimedia Contents III*, vol. 4314, August 2001, pp. 369–375.

[30] F. Deguillaume, Y. Rytsar, S. Voloshynovskiy, and T. Pun, "Data-hiding based text document security and automatic processing," in *IEEE International Conference on Multimedia and Expo (ICME) 2005*, Amsterdam, The Netherlands, July 6-8 2005.

[31] R. Villan, S. Voloshynovskiy, F. Deguillaume, Y. Rytsar, O. Koval, E. Topak, E. Rivera, and T. Pun, "A theoretical framework for data-hiding in digital text documents," in *Proceedings of 9th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security*, vol. 3238, Salzburg, Austria, September 19-21 2005, pp. 29–37.

[32] R. Villán, S. Voloshynovskiy, O. Koval, J. Vila-Forcén, E. Topak, F. Deguillaume, Y. Rytsar, and T. Pun, "Text Data-Hiding for Digital and Printed Documents: Theoretical and Practical Considerations," in *Proceedings of SPIE-IS&T Electronic Imaging 2006, Security, Steganography, and Watermarking of Multimedia Contents VIII*, San Jose, USA, January 15–19 2006.

[33] R. Villán, S. Voloshynovskiy, O. Koval, F. Deguillaume, and T. Pun, "Tamper-proofing of

Electronic and Printed Text Documents via Robust Hashing and Data-Hiding," in *Proceedings of SPIE-IS&T Electronic Imaging 2007, Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, USA, 28 Jan. – 1 Feb. 2007.

[34] B. Chen and G. W. Wornell, "Quantization index modulation: A class of provably good methods for digital watermarking and information embedding," *IEEE Trans. on Information Theory*, vol. 47, pp. 1423–1443, 2001.

[35] J. Eggers, J. Su, and B. Girod, "A blind watermarking scheme based on structured codebooks," in *Secure images and image authentication, IEE Colloquium*, London, UK, April 2000, pp. 4/1–4/6.

[36] *Signal Processing: Image Communication*, vol. 19, pp. 325–339, April 2004.

[37] M. Schneider and S. Chang, "A robust content based digital signature for image authentication," in *Proceedings of the IEEE International Conference on Image Processing*, Lausanne, Switzerland, September 1996, pp. 227–230.

[38] R. D. Brandt and F. Lin, "Representations that uniquely characterize images modulo translation, rotation, and scaling," *Pattern Recognition Letters*, vol. 17, pp. 1001–1015, 1996.

[39] L. Xie and G. R. Arce, "Joint wavelet compression and authentication watermarking," in *IEEE Int. Conference on Image Processing ́98 Proceedings.* Chicago, Illinois, USA: Focus Interactive Technology Inc., October 1998.

[40] S. Bhattacharjee and M. Kutter, "Compression tolerant image authentication," in *IEEE International Conference on Image Processing '98 (ICIP'98) Proceedings*, Chicago, IL, USA, October 1998.

[41] H. Hel-Or, Y. Yitzhaki, and Y. Hel-Or, "Geometric hashing techniques for watermarking," in *ICIP 2001*, 2001.

[42] J. Fridrich, "Visual hash for oblivious watermarking," in *IS&T/SPIE Proceedings*, vol. 3971, San Jose, California, USA, January 2000.

[43] J. J. K. Ó. Ruanaidh and T. Pun, "Rotation, scale and translation invariant digital image watermarking," in *IEEE Int. Conf. on Image Processing ICIP1997*, Santa Barbara, CA, USA, October 1997, pp. 536–539.

[44] V. Monga and B. Evans, "Robust perceptual image hashing using feature points," in *Proc. IEEE Int. Conf. on Image Processing*, Singapore, October 2004.

[45] M. Mihcak and R. Venkatesan, "New iterative geometric methods for robust perceptual image

hashing," in *Proc. ACM Workshop on Security and Privacy in Digital Rights Management*, Philadelphia PA, November 2001.

[46] F. Lefbvre, B. Macq, and J.-D. Legat, "Rash: RAdon Soft Hash algorithm," in *Proc. EUSIPCO*, Toulouse, France, 2002.

[47] A. Swaminathan, Y. Mao, and M. Wu, "Image hashing resilient to geometric and filtering operations," in *Proc. IEEE Workshop on Multimedia Signal Processing*, Siena, Italy, September 2004.

[48] R. Venkatesanan, S. Koon, M. Jacubowski, and P. Moulin, "Robust image hashing," in *ICIP 2000*, Vancouver, BC, Canada, September 2000.

[49] J. Fridrich, "Robust bit extraction from images," in *Proceedings ICMCS'99*, vol. 2, Florence, Italy, June 1999, pp. 536–540.

[50] F. Deguillaume, "Hybrid robust watermarking and tamperproofing of visual media," Ph.D. dissertation, Computer Vision and Multimedia Laboratory, University of Geneva, Geneva, Switzerland, October 2002.

[51] P. V. K. Borges and J. Mayer, "Text luminance modulationn for hardcopy watermarking," *Signal Processing, Elsevier*, vol. 87, no. 7, pp. 1754–1771, July 2007.

[52] F. Samaria and A. Harter, "Parameterisation of a stochastic model for human face identification," in *2nd IEEE Workshop on Applications of Computer Vision*, Sarasota (Florida), December 1994.

[53] [Online]. Available: http://www.nist.gov/srd/nistsd18.htm

[54] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, no. 28, pp. 656–715, 1949.

Figures

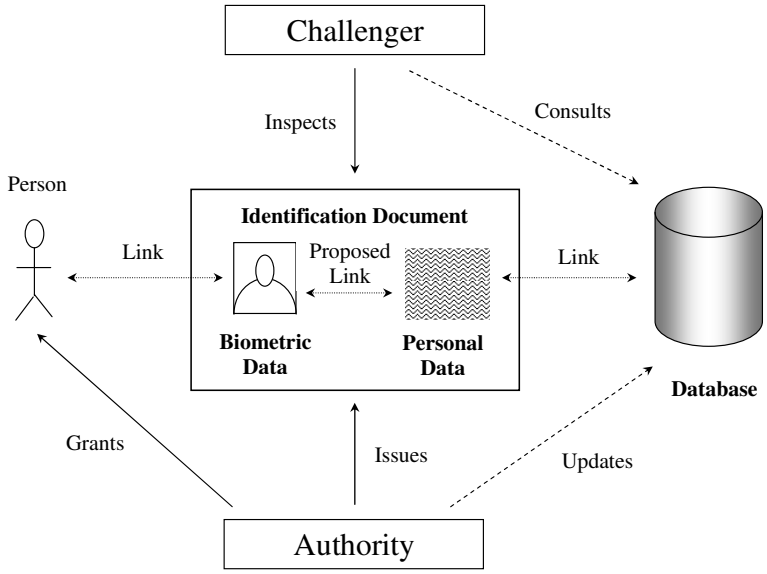

FIG. 1: The relations between an authority, a person, a challenger and an identification document.

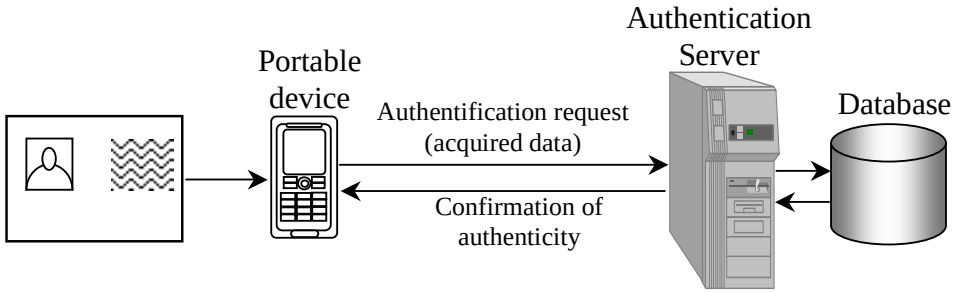

FIG. 2: Proposed system architecture for document authentication.

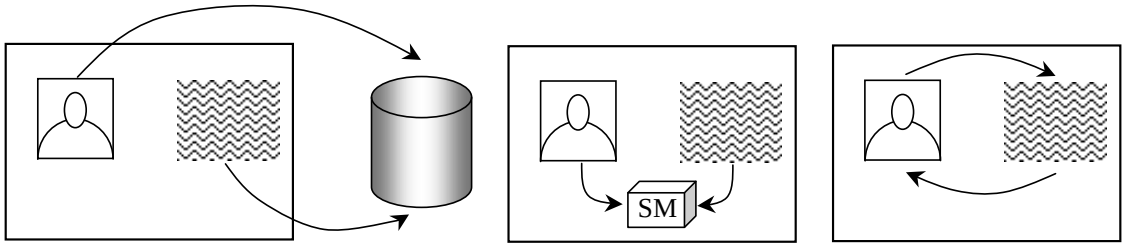

FIG. 3: Document authentication system architectures based on the secure link between biometrics and personal data via: (a) database; (b) on-document storage module; (c) self cross-storage based on digital data-hiding.

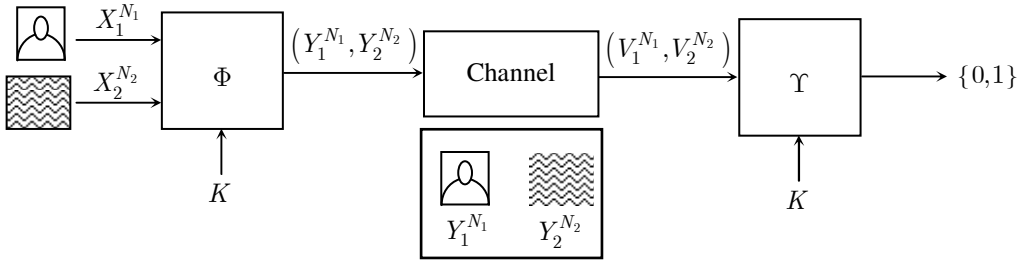

FIG. 4: Block diagram of a generic biometric document authentication system.

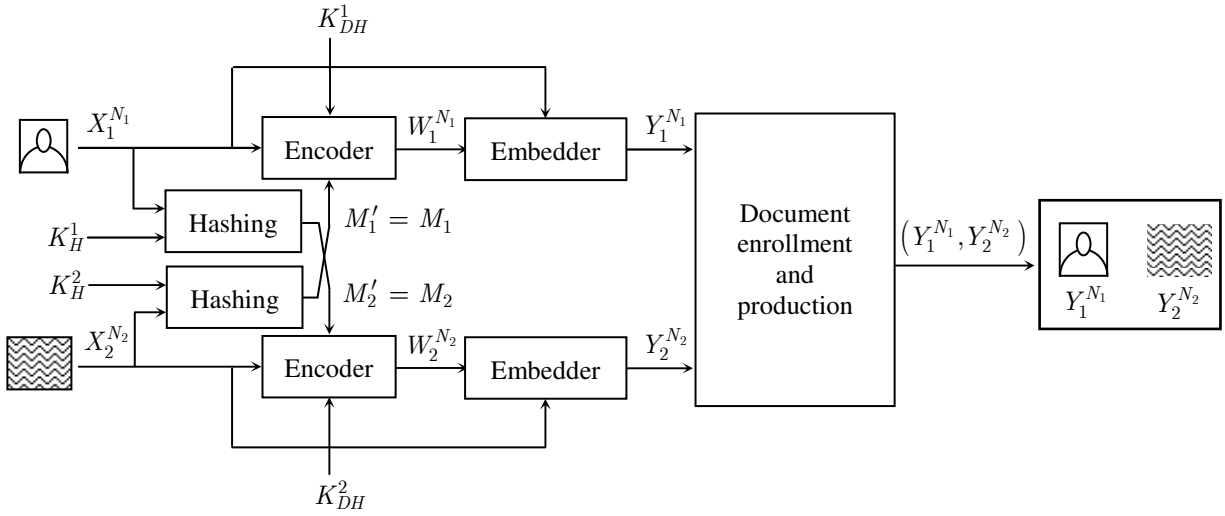

FIG. 5: Proposed enrollment and production of an identification document.

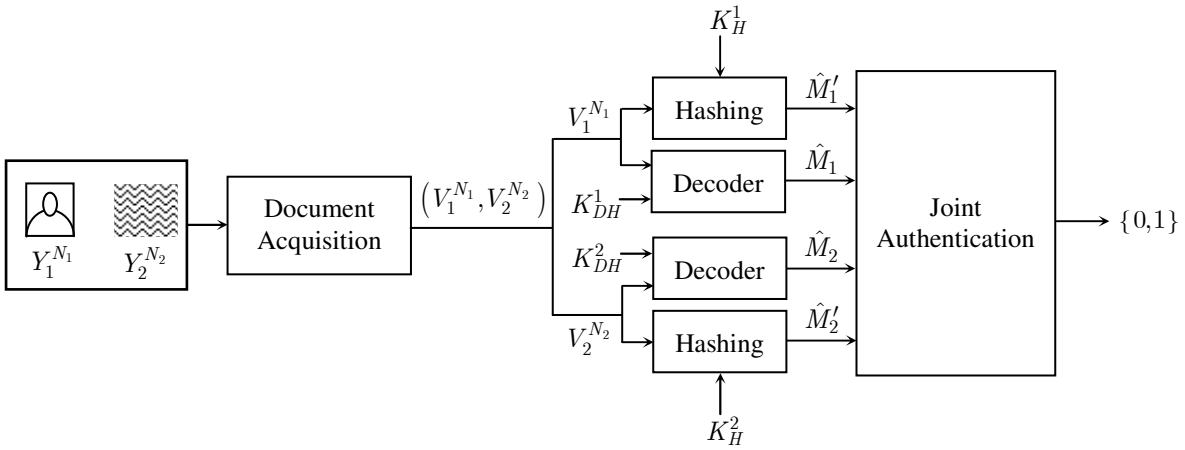

FIG. 6: Proposed authentication of an identification document.

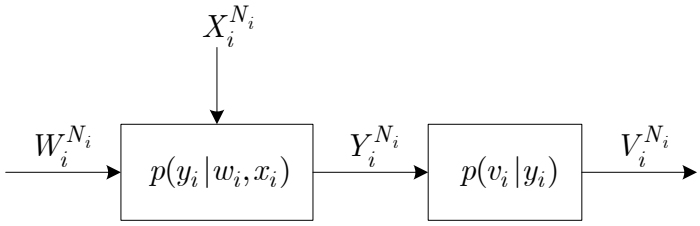

FIG. 7: Discrete memoryless data-hiding channel.

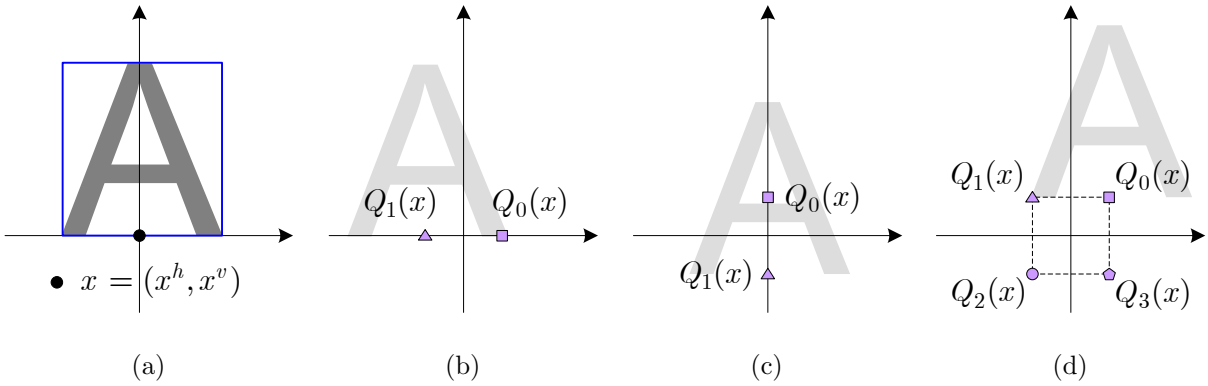

FIG. 8: Location Index Modulation ($N = 1$): (a) original character $x = \mathsf{A} = (x^h, x^v)$; (b) marked character $Q_1(x)$ by horizontal shifting; (c) marked character $Q_1(x)$ by vertical shifting; (d) marked character $Q_0(x)$ by combined horizontal and vertical shifting.

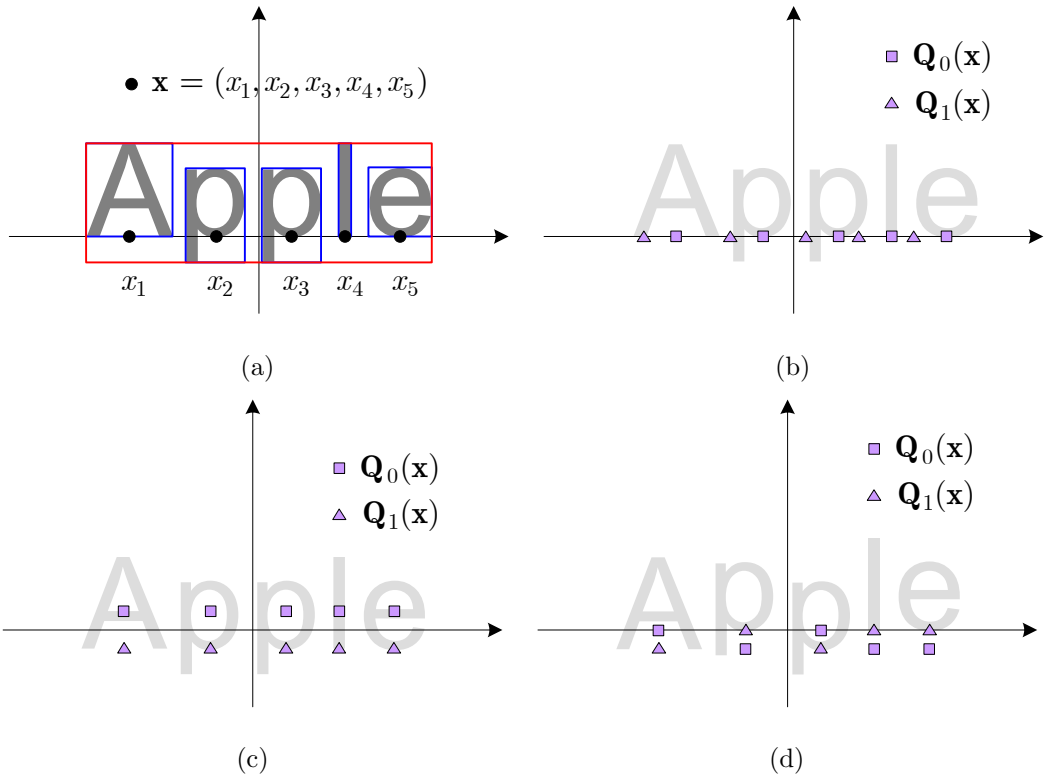

FIG. 9: Location Index Modulation ($N = 5$): (a) original word $x^N = (\mathsf{A}, \mathsf{p}, \mathsf{p}, \mathsf{l}, \mathsf{e}) = (x_1, x_2, x_3, x_4, x_5)$, where each $x_n = (x_n^h, x_n^v)$; (b) marked word $\mathbf{Q}_0(x^N)$ by horizontal shifting (a.k.a. word-shift coding); (c) marked word $\mathbf{Q}_1(x^N)$ by vertical shifting; (d) marked word $\mathbf{Q}_1(x^N)$ by mixed horizontal and vertical character shifting.

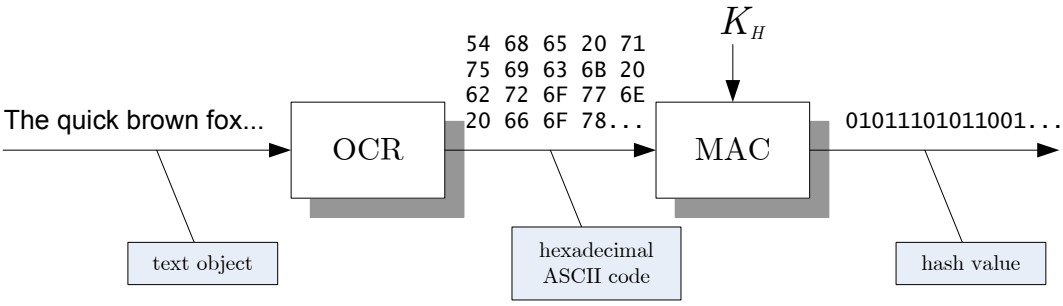

FIG. 10: OCR + MAC text hashing.

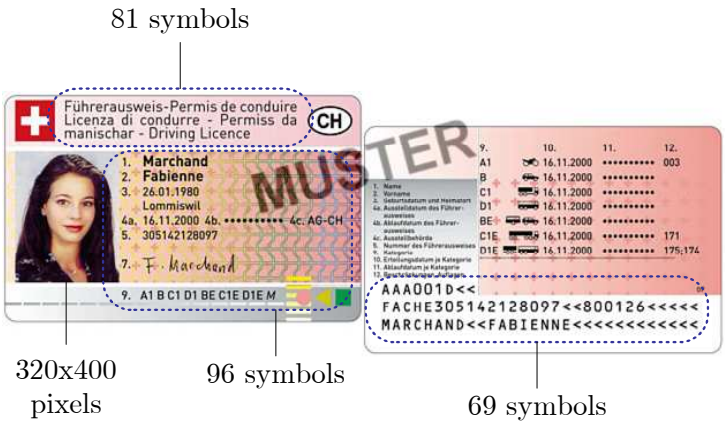

FIG. 11: Identification document sample.

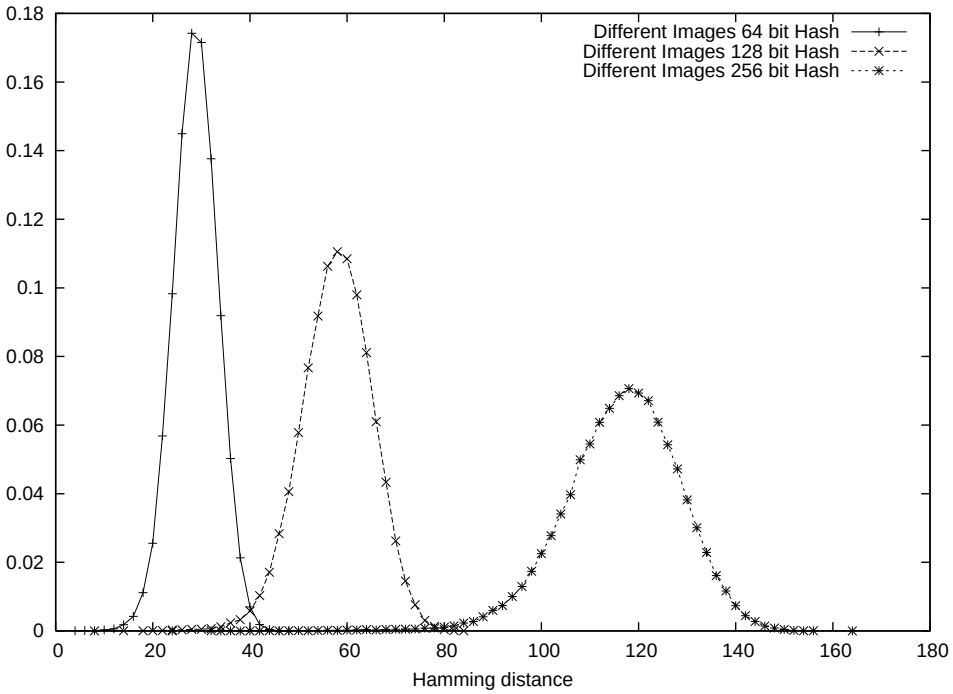

FIG. 12: Hamming distances between different images.

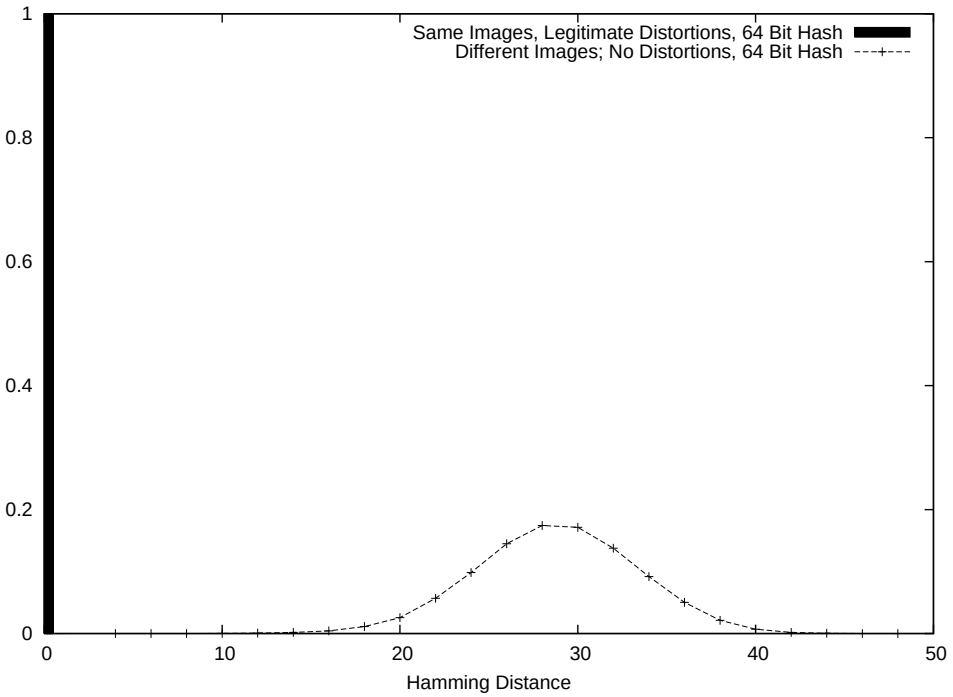

FIG. 13: Hamming distances between 64-bit hashes of images before and after being watermarked, printed and scanned, which are legitimate distortions. The Hamming distances of different images are provided for reference.