Identification with Privacy Protection based on Data Hiding

Taras Holotyak, Svyatoslav Voloshynovskiy, Ivan Prudyus

***Abstract*—In many problems such as biometrics, multimedia search and retrieval, recommendation systems requiring privacy-preserving similarity computations and identification, some binary features are stored in the public domain or outsourced to the third parties that might raise certain privacy concerns about the original data. To avoid this privacy leak, privacy protection is used. In the most cases, the privacy protection is uniformly applied to all binary features resulting in the data degradation and corresponding loss of performance. To avoid this undesirable effect we propose a new privacy amplification technique that is based on data hiding principles and benefits from side information about bit reliability a.k.a. *soft fingerprinting*. In this paper, we investigate the identification rate vs. privacy-leak trade-off. The analysis is performed for the case of perfect match between the side information shared between the encoder and decoder as well as for the case of partial side information.**

***Index Terms*—identification rate, privacy leakage, privacy preserving.**

I. Introduction

Content identification systems are widely used in various emerging applications ranging from identification of physical objects and humans to multimedia management (content filtering, content tagging) and security (copyright protection, broadcast monitoring, etc.). Most identification techniques are based on binary digital fingerprinting. A digital fingerprint represents a short, robust and distinctive content description allowing fast and privacy-preserving operations. In this case, all operations are performed on the fingerprint instead of on the original large and privacy-sensitive data, thus allowing introducing crypto-based security into the analog or noisy digital world [1]. These new techniques are able to overcome the fundamental sensitivity issue of classical cryptographic encryption and one-way functions to small noise in input data by trading-off the security and robustness to noise.

This paper is an extension of our previous works [2]–[4]. We have previously considered the rate-privacy-complexity trade-off for identification applications [2]. This approach is based on global privacy amplification, where all bits of stored fingerprints are randomized with the same probability disregarding their reliabilities. This approach is similar in spirit to compression-based approach [5]. However, contrary to the previous approach a concept of bit reliability was introduced to reduce the identification complexity based on a bounded distance decoder (BDD) [6]. Obviously, such a construction does not fully benefit from the fact that the information about the reliable bits can be present at the encoder and decoder that can be used not only for the efficient decoding but also for the enhanced privacy amplification.

Therefore, we introduced an information-theoretic framework for the analysis of private content identification based on finite length fingerprinting with bit reliability side information [3]. In this paper, contrary to previous works in content authentication based on *helper data* [1], [5], [7], [8], we propose and extend a privacy amplification mechanism, which is adaptive to the bit reliability, and demonstrate its advantages over the state-of-the-art privacy amplification in the identification problem. We present and analyze a privacy-preserving technique, which asymptotically achieves the theoretical identification performance limits in terms of identification rate. The analysis is performed for the case of a perfect match between the side information shared between the encoder and decoder as well as for the case of partial side information.

II. Identification problem formulation

We will assume that the *data owner* has M entries in the database indexed by an index m, i.e., $\mathbf{x}(m) \in \mathbb{R}^N$, $1 \leq m \leq M$, where $M = 2^{LR}$ with R to be the identification rate of (M, L)-fingerprinting code and L stands for the fingerprint length. The index m is associated with all identification information (ownership, time of creation, distribution channel, etc.) and the data $\mathbf{x}(m)$ is some privacy sensitive part of the database represented by image, video, audio, biometric, physical unclonable functions (PUFs), etc. The *data user* has a query data $\mathbf{y} \in \mathbb{R}^N$ that can be in some relationship with $\mathbf{x}(m)$ via a probabilistic model $p(\mathbf{y}|\mathbf{x})$ or can represent some irrelevant input $\mathbf{x}'$. The data user wishes to retrieve the identification information of $\mathbf{x}(m)$ that is the closest to the query $\mathbf{y}$ or reject the query, if no relevant database entry is found. For complexity and privacy reasons, the above identification is performed in the domain of digital fingerprints $\mathbf{x}_S \in \{-1, +1\}^L$ and $\mathbf{y}_S \in \{-1, +1\}^L$ that are short length, secure and robust counterparts of $\mathbf{x}$ and $\mathbf{y}$, respectively. Moreover, to ensure adequate privacy protection of digital fingerprints, the data owner applies privacy amplification (PA) to produce a protected version $\mathbf{u}(m)$ of $\mathbf{x}_S(m)$. The resulting fingerprints can be shared with third parties for various security and management services. In particular, the storage of the resulting codebook/database of protected fingerprints $\mathbf{u}(m)$, $1 \leq m \leq M$, and the content identification can be performed on a remote server that can be honest in terms of claimed functionalities but curious in terms of

T. Holotyak and S. Voloshynovskiy are with the Department of Computer Sciences, University of Geneva, Switzerland. E-mails: {svolos, Taras.Holotyak}@unige.ch

I. Prudyus is with the Institute of Telecommunications, Radioelectronics and Electronic Engineering, Lviv Polytechnic National University, Ukraine. E-mail: iprudyus@lp.edu.ua

observing, analyzing or leaking the stored data. The result of identification should be an estimate of index $\hat{m}$ of the corresponding closest entry or the erasure, i.e., null hypothesis. If the query is properly identified, the corresponding encrypted content $\mathbf{x}(m)$ or associated identification information is delivered to the data user using the predefined data exchange protocol. At the same time, the attacker can observe the entire database and analyze query [9].

III. Analysis of privacy preserving strategies

In this paper, identification methods, where information about $\mathbf{u}$ is reduced to the binary fingerprints, will be considered. This class of methods is very important for practical applications since it reduces complexity and memory storage requirements.

Storage of compressed or randomized (CR) [5]. Each codeword $\mathbf{u}(m)$, $1 \leq m \leq M$ of the database is a fingerprint that is randomized or compressed with the factor λ. This is equivalent to the passing the entire version of $\mathbf{x}_S$ database through a binary symmetric channel (BSC) with cross-over probability λ. Applying decoding technique that uses side information about $Y_M \in \mathbb{R}^L$ of extracted fingerprint at the verification stage, the identification rate and privacy leak defined as:

$$\begin{cases} R_{id|y_M}^{(X_S,CR)} = 1 - \mathrm{E}_{f(y_M)}\left[H(P_{b|y_M} * \lambda)\right], \\ L_p^{(X_S,CR)} = 1 - H(\lambda). \end{cases} \quad (1)$$

where $P_{b|y_M} = \int_{\mathcal{X}_M} Q\left(\frac{x_M}{\sigma_Z}\right) f\left(x_M|y_M\right) dx_M$ and $f\left(x_M|y_M\right)$ is a conditional pdf.

Privacy protection based on helper data (HD). This identification scheme is based on hashing and is parity checking bits storage characterized by the follow parameters:

$$\begin{cases} R_{id}^{(X_S,HD)} = 1 - H(P_b), \\ L_p^{(X_S,HD)} = H(P_b). \end{cases} \quad (2)$$

Privacy preserving based on data hiding (DH) [2], [4]. This group of recently proposed methods can be considered as the extension of [5], where the side information is exploited during both enrollment and verification stages. This approach allows to obtain secure separation of each vector $\mathbf{u}(m)$ into sets of "strong" and "weak" bits. Applying different processing to these sets at the enrollment stage, the set of "strong" bits provides required identification rate, while "weak" bits satisfies corresponding level of privacy.

$$\begin{cases} R_{id|y_M}^{(X_S,DH)} = \frac{L_Y}{N}\left(1 - \mathrm{E}_{f(y_M)}\left[H(P_{b|y_M}^S)\right]\right), \\ L_p^{(X_S,DH)} = 1 - H(P_d^{DH}), \end{cases} \quad (3)$$

where $P_{b|y_M}^S$ is representing probability of bit error in strong channel in methods with the available side information Y_M; the average probability of bit disclosure P_d^{DH} is defined as $P_d^{DH} = \frac{L_X}{N} P_d^S + \frac{N-L_X}{N} P_d^W$, L_X determines the number of components in the strong (disclosed) channel, P_d^S ($P_d^S = 1$) and P_d^W ($P_d^W = \frac{1}{2}$) defines probability of sign information disclosure in strong and weak channels correspondingly.

The main properties of the considered methods are compared in terms of $R_{id} - L_p$ characteristics (Fig. 1). The obtained results show the advantage of the proposed identification method based on data hiding over CR method. In the high SNR regime, the privacy preserving method based on the HD shows best performance over the rest methods and can asymptotically ($SNR \to \infty$) reach the zero-privacy leakage property. However, at the low SNR its performance over the DH method diminishes.

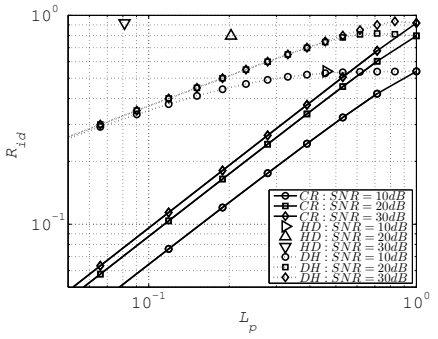

Fig. 1. $R_{id} - L_p$ diagram of identification methods.

IV. Conclusions

In this paper, we extended application of side information in privacy preserving identification. Several techniques were analyzed for the case of soft information available on different stages of identification. In particular, we established that one can achieve considerable privacy amplification using even imperfect side information without the identification rate loss.

References

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

[2] S. Voloshynovskiy, O. Koval, F. Beekhof, F. Farhadzadeh, and T. Holotyak, "Information-theoretical analysis of private content identification," in *IEEE Information Theory Workshop, ITW2010*, Dublin, Ireland, Aug.30-Sep.3 2010.

[3] S. Voloshynovskiy, O. Koval, T. Holotyak, F. Beekhof, and F. Farhadzadeh, "Privacy amplification of content identification based on fingerprint bit reliability," in *Proceedings of IEEE International Workshop on Information Forensics and Security*, Seattle, The USA, December 12–15 2010.

[4] Sviatoslav Voloshynovskiy, Taras Holotyak, Oleksiy Koval, Fokko Beekhof, and Farzad Farhadzadeh, "Private content identification based on soft fingerprinting," in *Proceedings of SPIE Photonics West, Electronic Imaging, Media Forensics and Security XIII*, San Francisco, USA, January, 2326 2011.

[5] T. Ignatenko and F.M.H. Willems, "Privacy leakage in biometric secrecy systems," in *46th Annual Allerton Conference on Communication, Control, and Computing*, Urbana, USA, 23-26 Sept. 2008, pp. 850–857.

[6] F. Beekhof, S. Voloshynovskiy, O. Koval, and T. Holotyak, "Fast identification algorithms for forensic applications," in *Proceedings of IEEE International Workshop on Information Forensics and Security*, December 6–9 2009.

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

[8] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: Theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, pp. 503–512, 2007.

[9] S. Voloshynovskiy, F. Beekhof, O. Koval, and T. Holotyak, "On privacy preserving search in large scale distributed systems: a signal processing view on searchable encryption," in *Proceedings of the International Workshop on Signal Processing in the EncryptEd Domain*, Lausanne, Switzerland, 2009.