Fast identification of highly distorted images

Holotyak, Taras; Voloshynovskyy, Svyatoslav; Beekhof, Fokko Pieter; Koval, Oleksiy

How to cite

HOLOTYAK, Taras et al. Fast identification of highly distorted images. In: Proceedings of SPIE / Media Forensics and Security II. San Jose (USA). [s.l.] : SPIE, 2010. (Conference Volume) doi: 10.1117/12.838962

This publication URL: https://archive-ouverte.unige.ch//unige:47642
Publication DOI: 10.1117/12.838962

Fast identification of highly distorted images

Taras Holotyak, Sviatoslav Voloshynovskiy, Fokko Beekhof, and Oleksiy Koval
Department of Computer Science, University of Geneva,
7 route de Drize, CH 1227, Geneva, Switzerland

ABSTRACT

In this paper, we consider a low complexity identification system for highly distorted images. The performance of the proposed identification system is analyzed based on the average probability of error. An expected improvement of the performance is obtained combining random projection transform and concept of bit reliability. Simulations based on synthetic and real data confirm the efficiency of the proposed approach.

Keywords: identification, reliability, complexity, random projections.

1. INTRODUCTION

The identification problem recently attracts a lot of attention in various applications that include but are not limited to copy detection, content management, biometrics, forensics of physical objects, and retrieval in large databases. This task is complicated by various intentional or non-malicious distortions or modifications that are introduced into the original content in security - related or multimedia applications, respectively [1-3] impacting the performance of identification systems.

Historically, solutions proposed to cope with the identification problem were based on assigning a specific index to every object or item by modifying its look like via a printed barcode [4], invisible digital watermark embedding [5], overprinted sparse set of dots (usually yellow) [6] or specially designed storage device such as magnetic stripe, electronic smart cards or RFID [7]. Evidently, such approaches have several drawbacks since allow uncontrolled read-out and duplication of the stored information and its improper use that is unacceptable for security and privacy preserving applications. Moreover, in certain circumstances, the abovementioned modifications are not allowed at all due to various application related constraints including cost or back tracking compatibility.

The mentioned drawbacks can be overcome by using inherit forensic features possessed by real world objects similarly to humans. Physical unclonable functions that are analogous to human biometrics are proven to uniquely represent such objects and can be successfully exploited for their identification. Recently, the first attempt of such system design was performed for identification of consumer electronics and real world objects [1, 2].

The system in the latter case was based on the object surface microstructure image acquired by a particular imaging device. It was demonstrated [1] that the performance of the identification crucially depends on the quality of the extracted forensic features.

The second challenge that was tackled in the mentioned reference was identification complexity issue that was suboptimally resolved using the Reference List Decoding.

In this paper we consider the problem of image identification and seek for jointly highly accurate in terms of performance and computationally efficient solution for large databases. For this purpose we propose to involve into the identification the information about the identification channel output bit reliability as a probabilistic measure of the error presence in its particular bit. We demonstrate that this information has a twofold impact on the identification performance. First, it allows to significantly reducing the randomness of the channel output given its input leading to the enhanced probability of error behavior of the proposed system vs. existing analogues. Secondly, it permits significant reduction of the decoding space cardinality lightening the complexity of the method.

The paper has the following structure. Identification problem formulation based on digital communication fundamentals is presented in Section 2. The identification system based on bit reliability concept is proposed in Section 3. Section 4 contains the results of experimental validation of the proposed identification system. Finally, Section 5 concludes this paper.

Notations. We use capital letters to denote scalar random variables X, $\mathbf{X}$ to denote vector random variables, corresponding small letters x and $\mathbf{x}$ to denote the realizations of scalar and vector random variables, respectively. We use $X \sim p_X(x)$ or simply $X \sim p(x)$ to indicate that a random variable X is distributed according to $p_X(x)$.

2. COMMUNICATION PARADIGM OF IDENTIFICATION

General structure of identification problem formulated based on the digital communication fundamentals is presented in Fig. 1. At the enrolment stage a codebook of length-N feature vectors $\mathbf{x}(i)$, $i \in \{1,2,...,M\}$, that represents identifying objects, is generated and shared with the decoder. It is important to underline that oppositely to the classical communication scenario, there is no freedom in selection of the optimal distribution of X, which is considered to be fixed in identification. At the identification stage the decoder having the access to the distorted version $\mathbf{y}$ of the certain entry of the codebook $\mathbf{x}(m)$ modified according to a known and fixed transition probability $p(\mathbf{y}|\mathbf{x})$ and the collection of $\mathbf{x}(i)$, $i \in \{1,2,...,M\}$, is trying to determine the index $\hat{m}$ of the transmitted codeword. In the case it is possible to generate a unique guess, $\hat{m}$ is declared as the identity of the observed object, otherwise, an error is asserted.

As it was mentioned in the Introduction, modern identification systems have to guarantee not only accurate performance (the probability of correct match of the query and a corresponding codeword), but also consistent level of complexity (average amount of computation efforts), secrecy (non-disclosure of information about system secrets/keys) and privacy (non-disclosure of the person/object-related information).

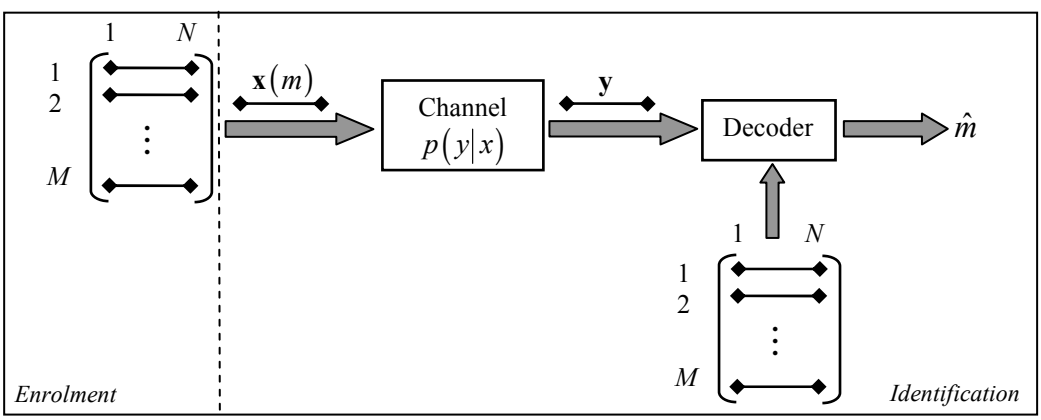


Figure 1. Identification problem.

To cope with the various issues of complexity and the curse of dimensionality many systems perform identification in the lower dimensional space $\mathbb{R}^L$. The obtained features are often additionally quantized to $\{-1,+1\}^L$ to further simplify the search for large databases and enable the usage of cryptographic tools for security and privacy reasons. The basic diagram of such identification system is shown in Fig. 2.

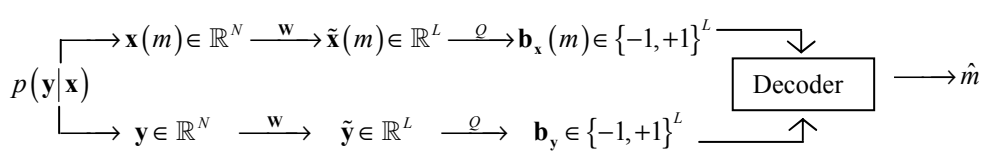


Figure 2. Structure of the typical identification system.

The input data $\mathbf{x}(m) \in \mathbb{R}^N$ is first mapped into $\tilde{\mathbf{x}}(m) \in \mathbb{R}^L$ using the projection operator $\mathbf{W} \in \mathbb{R}^{L \times N}$, which consists of a set of basis vectors $\mathbf{w}_i$, $1 \le i \le L$, $\mathbf{W} = (\mathbf{w}_1, \ldots, \mathbf{w}_L)^T$ with $L \le N$ and then binarized using the quantizer Q resulting in the binary vector $\mathbf{b}_\mathbf{x} \in \{-1,+1\}^L$. We assume that an observation vector $\mathbf{y} \in \mathbb{R}^N$ is linked with $\mathbf{x}(m)$ by a probabilistic mapping $p(\mathbf{y}|\mathbf{x})$, which is transformed into a binary counterpart $\mathbf{b}_\mathbf{y} \in \{-1,+1\}^L$ accordingly. The decoder observes $\mathbf{b}_\mathbf{y}$ and determines the index of the sequence referring to the database of enrolled sequences $\mathbf{b}_\mathbf{x}(m)$, $1 \le m \le M$, where M is the database size. The existing fast identification algorithms assume high correlation between quantized features $\mathbf{b}_\mathbf{x}$, stored in the database, and those extracted from the observation vector $\mathbf{y}$, i.e., $\mathbf{b}_\mathbf{y}$. The expected mismatch between pairs of elements of these binary vectors can be modeled using binary symmetrical channels with certain cross-over probabilities.

Applying dimensionality reduction techniques ($\mathbb{R}^N \to \mathbb{R}^L$), some systems attempt at reducing the complexity to $O(ML)$. However, the considerable dimensionality reduction from N to L is accompanied with high $\bar{P}_b$ and does not allow to perform the reliable identification due to the data processing inequality [8].

3. PROPOSED SOLUTION OF IDENTIFICATION PROBLEM

To resolve the trade-off between the performance and complexity of identification we propose a new approach, based on the random projections and the concept of bit reliability. The main ideas behind the proposed approach consist in:

1) generation of multiple random projections (RP);
2) selection among them only those which correspond to reliable bits;
3) design of a special structure of the decoder to reduce identification complexity.

The schematic diagram of the proposed approach is shown in Fig. 3.

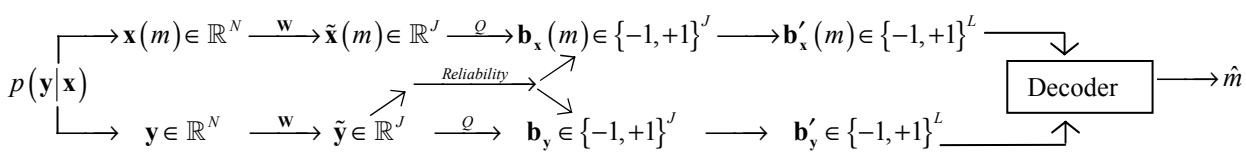


Figure 3. Structure of the proposed identification system.

In order to introduce the concept of bit reliability, one can readily note that not all random projections outputs are leading to the bit error with equal probabilities (Fig. 4). Indeed, those projections that are almost orthogonal with their inputs (Fig. 4,c) are more likely to lead to a bit error than collinear ones (Fig. 4,b). As it was pointed out [8] for the Gaussian case, this error happens with probability equal to $Q(\tilde{x}_i/\sigma_Z^2)$, where $Q(\bullet)$ is a Q function and σ_Z^2 is a variance of the AWGN. Thus, selection of proper projection operators might lead to a significant reduction of the error probability. The number of those projections that are required in order to identify $M = 2^L$ objects can be obtained from the examination of the identification capacity [9]

$$2^{JI(B_X;B_Y)} \ge 2^L, \tag{1}$$

leading to

$$J \ge \frac{\log_2 M}{1 - H(B_X|B_Y)}, \tag{2}$$

where $H(B_X|B_Y) = H_2(\bar{P}_b)$ is a binary entropy.

Thus, generalized procedure of generation of the random projections should be modified as follow. First, a set of J projections is generated $(L \le J \le N)$. Than the required amount of reliable ones is selected based on the channel output $\mathbf{y}$.

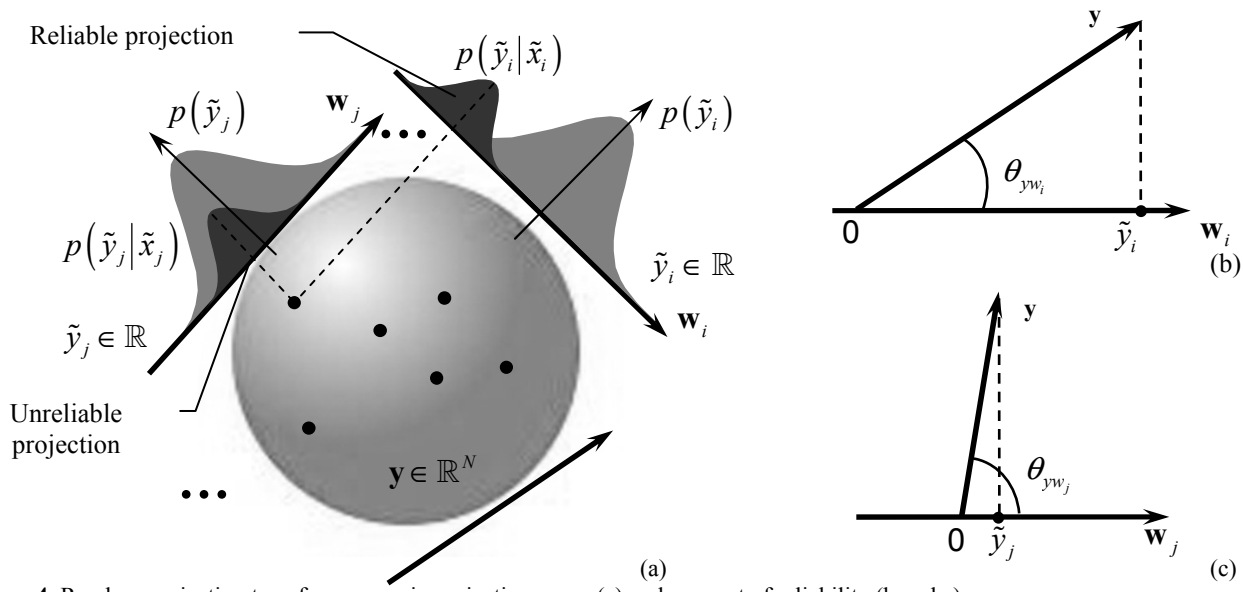


Figure 4. Random projection transform: generic projection space (a) and concept of reliability (b and c).

Under the assumption of an additive communication model $\mathbf{y}$ is generated based on the channel input $\mathbf{x}$ as follows: $\mathbf{y} = \mathbf{x} + \mathbf{z}$, where $\mathbf{z}$ defines channel noise, the special design of projecting matrix $\mathbf{W} \in \mathbb{R}^{J \times N}$, where $\mathbf{W} = (\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_J)^T$ and $W_{i.j} \sim \mathcal{N}(0, 1/N)$, is intended to provide a certain universality of the decoding. In this case projected query can be represented as $\tilde{\mathbf{y}} = \mathbf{W}\mathbf{y} = \mathbf{W}(\mathbf{x} + \mathbf{z}) = \mathbf{W}\mathbf{x} + \mathbf{W}\mathbf{z} = \tilde{\mathbf{x}} + \tilde{\mathbf{z}}$ and regardless of the initial distributions of $\mathbf{x}$ and $\mathbf{z}$ the projection outputs $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{z}}$ will follow the Gaussian distribution. Indeed, for arbitrarily distributed $\mathbf{x}$, the components of $\tilde{\mathbf{x}}$ can be considered as weighted sums of the components of $\mathbf{W}$ implying Gaussian distribution for $\tilde{\mathbf{x}}$ as well. Same arguments can be applied with respect to $\tilde{\mathbf{z}}$.

At the second stage, the reliable bits estimation is performed. This issue becomes important when distorted queries are processed. The reliability of the bit $R_{b_{yi}}$ can be defined as the probability of making correct decision on the output based on the given bit that was passed through a communication channel. Keeping in mind that a posterior probability of error $P_{b|y_i}$ complements the probability of correct decision, one can conclude the following: $P_{b|y_i} \downarrow \Rightarrow R_{y_i} \uparrow$. Due to the impact of the channel $p(\mathbf{y}|\mathbf{x})$, bits in $\mathbf{b}_\mathbf{y}$ are flipped with respect to $\mathbf{b}_\mathbf{x}$ according to the above discussed mechanism (Fig. 4). It is easy to see, that $R_{b_{yi}} \sim |\tilde{y}_i|$. With some freedom in the projection choice it is possible to select ones with negligibly small chances of the bit flipping in the binary data representation (reliable bits), while redundant projections (non-reliable bits) can be simply revoked from the consideration.

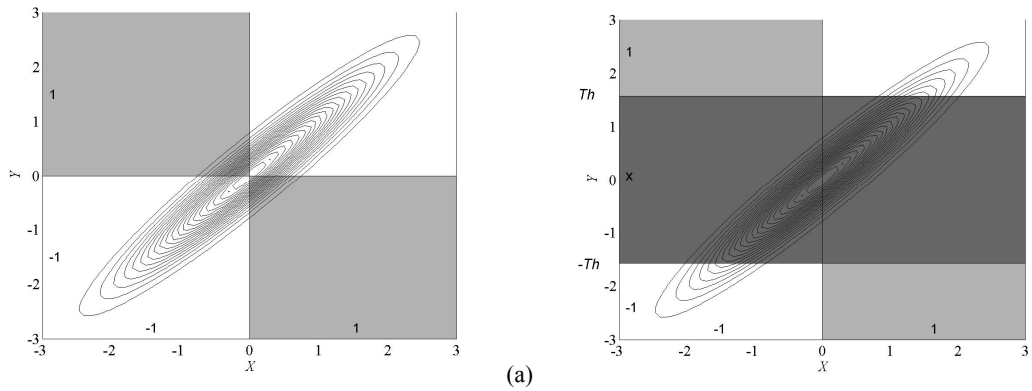
The analysis of the average probability of bit error $\overline{P}_b$ for the Gaussian data and observation distortions is explained in Fig. 4, where different bit constellation patterns are investigated to evaluate the probability of bit flipping. Errors appear in the areas marked by light gray. Non-reliable bits that are excluded from consideration correspond to the dark area, while white zones are related to the correct bit transmission. The average bit error probability can be found as:

$$\begin{aligned}\overline{P}_b = \Pr\left[B_Y = +1 \middle| B_X = -1\right]\Pr\left[B_X = -1\right] + \Pr\left[B_Y = -1 \middle| B_X = +1\right]\Pr\left[B_X = +1\right] = \\ \Pr\left[\tilde{Y} \geq 0 \middle| \tilde{X} < 0\right]\Pr\left[\tilde{X} < 0\right] + \Pr\left[\tilde{Y} < 0 \middle| \tilde{X} \geq 0\right]\Pr\left[\tilde{X} \geq 0\right]\end{aligned} \tag{3}$$

and it can be known that [8]

$$\overline{P}_b = 1/\pi \arccos\left(\rho_{\tilde{X}\tilde{Y}}\right), \tag{4}$$

where $\rho_{\tilde{X}\tilde{Y}} = \sigma_{\tilde{X}} \Big/ \sqrt{\sigma_{\tilde{X}}^2 + \sigma_{\tilde{Z}}^2}$, $\sigma_{\tilde{X}}^2$ and $\sigma_{\tilde{Z}}^2$ are variances of codebook and channel noise in random projection space.



(a) (b)

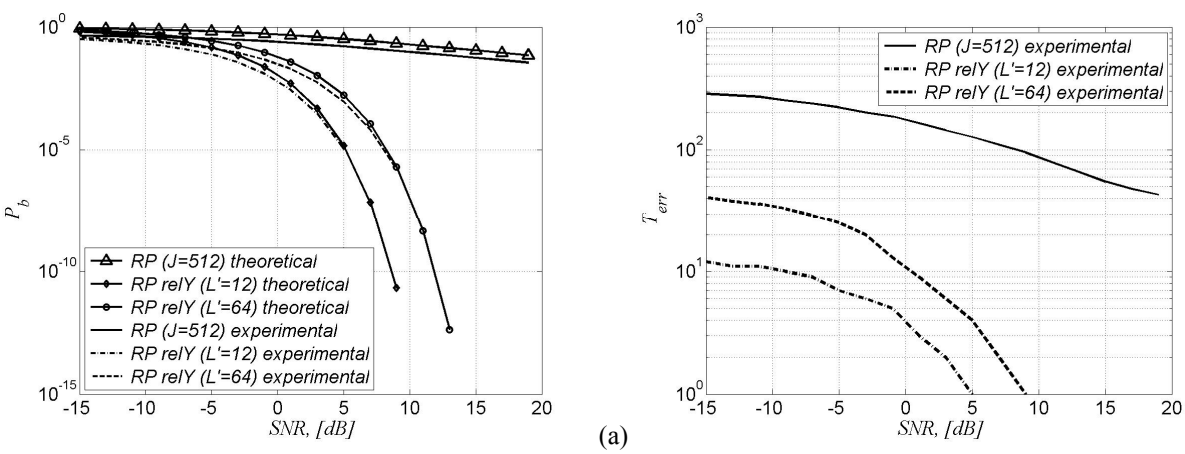
Figure 5. Bit constellation for different identification channels: (a) existing solution, (b) proposed approach based on reliable components.

The closed form solution for $\overline{P}_b$ in the proposed scheme does not exist

$$\overline{P}_b = \Pr\left[B_X = +1 \middle| B_Y = -1\right]\Pr\left[B_Y = -1\right] + \Pr\left[B_X = -1 \middle| B_Y = +1\right]\Pr\left[B_Y = +1\right] = \Pr\left[\tilde{X} \geq 0 \middle| \tilde{Y} < -Th\right]\Pr\left[\tilde{Y} < -Th\right] + \Pr\left[\tilde{X} < 0 \middle| \tilde{Y} \geq Th\right]\Pr\left[\tilde{Y} \geq Th\right], \quad (5)$$

where the threshold Th is defined as $Th = \sqrt{\sigma_X^2 + \sigma_Z^2}\, Q^{-1}\left(1 - L'/(2J)\right)$.

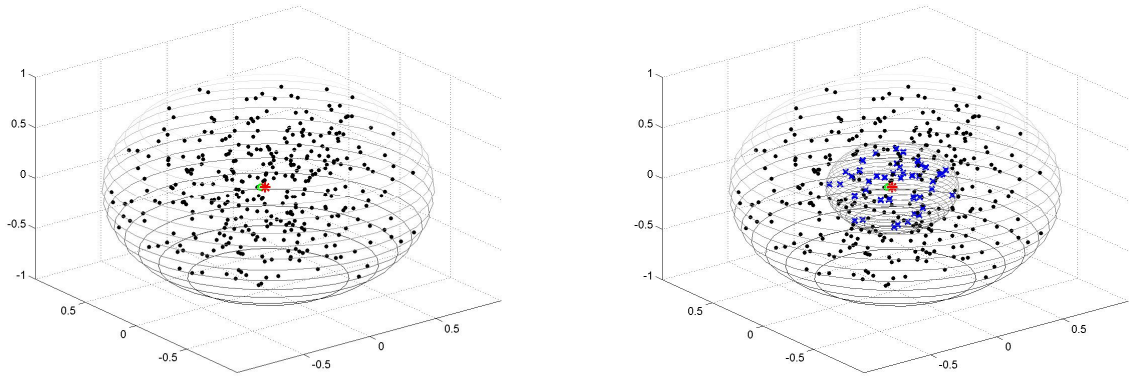
Performance analysis of the classical (Fig. 2) and proposed bit reliability-based (Fig. 3) identification systems in terms of probability of bit error is presented in Fig 6, a. Results for $\overline{P}_b$ were also validated by the experimental simulation for the same setups, where probability of bit error was averaged over more that 10^9 bits. It is possible to conclude that decreasing the size of the block by keeping only most reliable bits the average probability of bit error can be drastically reduced. Similarly, analysis of the average number of errors per block as a function of SNR for different block lengths is presented in Fig.6, b. The obtained dependences reveal that the blocks composed of the most reliable bits only can be identified without errors for rather low SNRs, e.g., for the block with 12 most reliable bits it is possible for SNR >5dB.



(a) (b)

Figure 6. Existing and proposed identification problem solutions comparison: (a) average probability of bit error, (b) average number of error bits.

The possibility to identify at least part of the bits in a codeword without error makes it possible to drastically reduce the complexity of identification algorithm. The graphical interpretation of the complexity reduced identification is depicted in Fig. 7.



(a) (b)

Figure 7. Graphical interpretation of existing (a) and proposed (b) identification methods: (o is a query, * is the sought codeword, x are neighbors of the sought codeword, and • are the rest of codewords).

For the given codebook, in order to find a match with a channel output the existing identification methods perform exhaustive search over the entire codebook. Usually this approach is implemented by a maximum likelihood (ML) decoder

$$\hat{m} = \arg\max_{1 \le m \le M} p\left(\mathbf{y} \middle| \mathbf{x}(m)\right). \tag{6}$$

This solution is optimal in terms of performance, but characterized by complexity $O(MN)$.

Contrarily, such a codeword matching will be performed only in a subset of the codewords in the proposed approach. Since such an extraction is performed based on the most reliable bits, one can conjecture about the presence of the sought codeword in the subset with high probability.

The structure of proposed decoder is shown in Fig. 8. First, the given query is decomposed onto magnitude and sign parts. The sign part, which is equivalent to the bit representation, is preserved for the further matching, while magnitude components are used to evaluate bits reliability. Then, based on the L' most reliable bits of query the sets of codewords indexes with exact matching of corresponding bits are composed. At the end, the final list of the sought codeword and its neighbors can be obtained by the exclusive combination of the mentioned above sets. Subsequently the ML decoding in the neighbor subspace finalizes the identification procedure.

The following section contains the results of the existing and proposed identification systems comparison.

4. EXPERIMENTAL VALIDATION

The first experiment was dedicated to the analysis of complexity reduction of the proposed solution vs. classical identification. For this purpose complexity of the proposed identification method, which utilizes a subspace extraction based on the $L' = 12$ most reliable bits, was compared with the complexity of the ML decoder. The complexity was evaluated as a time to process the query by each identification method. Under the assumption of the AWGN distortions the synthetic Gaussian codebooks ($\sigma_X^2 = 1$) with sizes $M = 2^{10} \div 2^{20}$ and codeword length $N = 2048$ were generated and randomly projected into J-dimensional ($J = 512$) space. The results of comparison are summarized in Fig. 9, a. Both the ML decoder and proposed method have shown exponential dependence of the complexity of the size M of the codebook. However, being almost similar for small M s, for $M = 2^{20}$ the proposed identification method is significantly outperforming the existing one (about 150 times). Also, only about 0.60s is required by the proposed identification method to identify a query in a 1Mo database.

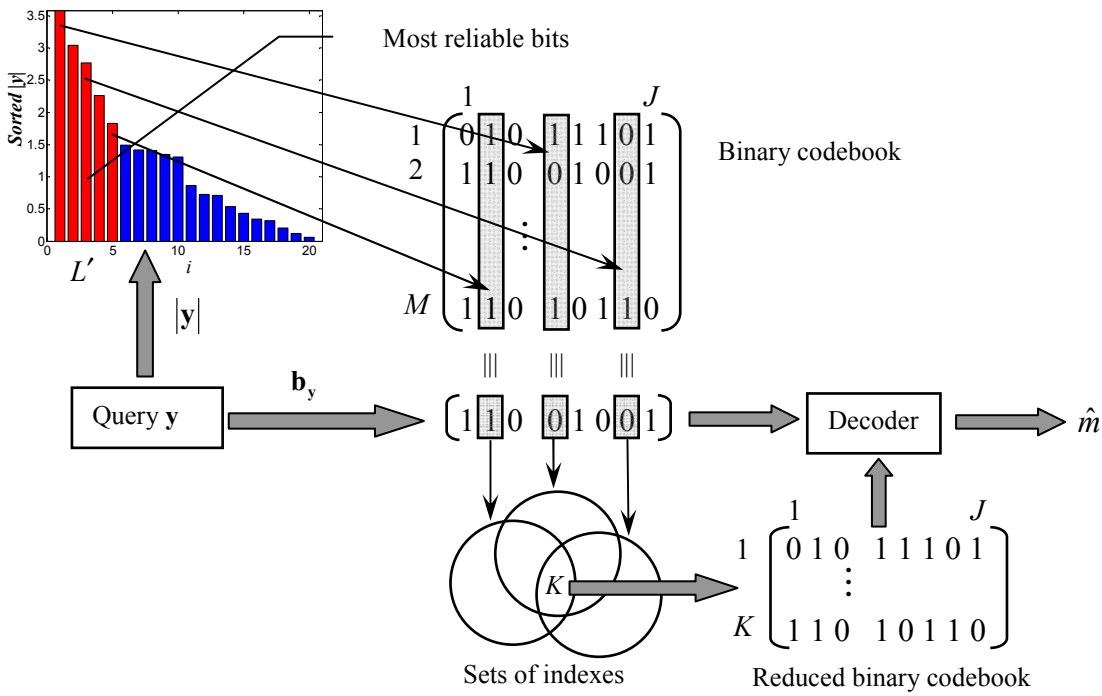
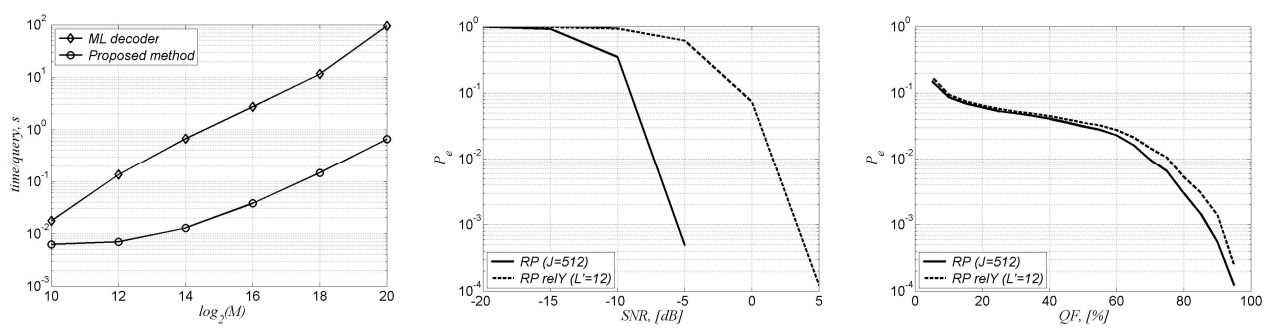


Figure 8. Proposed identification decoder.

The second part of simulations addresses to the impact of complexity reduction on the identification system performance in terms of the average probability of error. The results of simulation are shown in Fig. 9, b and c for both synthetic and real data. For the fixed size database ($M = 2^{14}$, $N = 4096$) degradation of the average probability of error of the proposed method was compared with performance of the ML decoder. While a gap in performance of the proposed identification vs. the exhaustive search was observed (~10 dB), it is important to note that the working SNR range of the proposed technique was moved to lower SNRs with respect to existing identification technique. Furthermore, for SNR>5dB, the proposed method demonstrates errorless performance.

Finally, a set of experiments was done with real images. The assumed distortion model was the degradations introduced due to the JPEG lossy compression. The obtained results allow to conclude about similar performance of the ML decoder and proposed identification method for highly distorted images (JPEG QF<60%). The same behavior (with small degradation of proposed method performance) is observed for higher QF.



(a) (b) (c)

Figure 9. Experimental validation results: (a) complexity of identification; (b) average probability of error for synthetic data under AWGN distortions; (c) average probability of error for real data under compression distortions.

5. CONCLUSIONS

In this paper we considered the problem of the accurate and computationally efficient image identification based on the bit reliability concept. The identification framework is developed for the Gaussian formulation of the identification problem. The framework applicability to real images is justified by the proper design of the random projection operator that maps arbitrary statistics to the Gaussian. It is demonstrated that the bit reliability information can significantly enhance the system performance by reducing probability of bit error vs. existing identification systems and improve computational complexity by reducing the cardinality of the decoder search. While a significant performance gap between the proposed system and the ML decoder-based one still exists, it is possible to admit the enlargement of the operating SNR range towards low SNRs. Finally, a set of computer simulations was performed that confirmed our theoretical findings.

ACKNOWLEDGMENTS

This work is supported by SNF projects 111643 and 1119770.

REFERENCES

1. S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun, "Unclonable identification and authentication based on reference list decoding," *In Proceedings of the conference on Secure Component and System Identification*, Berlin, Germany, March 17-18, 2008.
2. F. Beekhof, S. Voloshynovskiy, O. Koval, and R. Villan, "Secure Surface Identification Codes," *In Proceedings of SPIE Photonics West, Electronic Imaging / Media Forensics and Security* X, San Jose, USA, 2008.
3. E. Valle, M. Cord, and S. Philipp-Foliguet. "CBIR in Cultural Databases for Identification of Images: A Local-Descriptors Approach," 2008, http://www.scientificcommons.org/43597051
4. C. K. Harmon. *Lines of Communication: Bar Code and Data Collection Technologies for the 90S*. Helmers Pub, 1994.
5. I. J. Cox, M. L. Miller, and J. A. Bloom. *Digital Watermarking. Morgan Kaufmann Publishers*, Inc., San Francisco, 2001
6. Z. F. Keith, T. Knox, and E. J. Schneider. Method and apparatus for detecting photocopier tracking signatures. US Patent 6515764, Issued on February 4, 2003, filed February 1998
7. J. Koniecek and K. Little. *Security, ID Systems and Locks: The Book on Electronic Access Control*. Elsevier Computers/Computer Security, 1997
8. S. Voloshynovskiy, O. Koval, F. Beekhof, and T. Pun. "Conception and limits of robust perceptual hashing: toward side information assisted hash functions," *In Proceedings of SPIE Photonics West, Electronic Imaging / Media Forensics and Security* XI, San Jose, USA, 2009
9. F.Willems, T. Kalker, J. Goseling, and J-P. Linnartz. On the capacity of a biometrical identification system. *In: Proc. of the 2003 IEEE Int. Symp. on Inf. Theory*, pages 8–2, 2003.