How to (Possibly) Foil Multimedia Security?

Félix Balado
School of Computer Science and Informatics
University College Dublin
Belfield Campus, Dublin 4, Ireland
Email: felix@ucd.ie

Thierry Fournel
Laboratoire Hubert Curien, UMR CNRS 5516
Saint-Étienne University
Carnot Campus, 42000 Saint-Étienne, France
Email: fournel@univ-st-etienne.fr

***Abstract*—Multimedia security can be foiled thanks to Slepian's permutation modulation. Originally proposed in 1965 for standard problems of channel and source coding in communications, permutation codes can also provide optimum solutions in two relevant fields: steganography (foiling hidden information detection tests) and counterforensics (foiling forensic detection tests). In the first scenario, permutation codes have been shown to implement optimum perfect universal steganography (that is to say, steganography with maximum information embedding rate, undetectable and only relying on the empirical distribution of the host) for histogram-based hidden information detectors. In the second scenario, permutation codes have been shown to implement minimum-distortion perfect counterforensics (that is to say, forgeries which are undetectable and as close as possible to a target forgery) for histogram-based forensic detectors. Interestingly, both of these developments have revealed connections with compression through theoretical bounds from the mathematical theory of information. In steganography, the long-acknowledged duality between perfect steganography and lossless compression has been made explicit by permutation coding. On the other hand, a connection between counterforensics, lossy compression and histogram specification is also shown.**

I. Introduction

Multimedia security is a field that concerns different security aspects of digital multimedia signals, such as for instance digital images. In this tutorial paper we will review recent findings which show how to obtain optimum solutions to two apparently separate multimedia security questions: 1) how to modify a *host* signal to conceal information within it in a way that will be completely undetectable by a third party?; and 2) how to create a forged version of an original signal which can be passed as authentic with absolute certainty?

The first question led to the birth (or rather, rebirth) of the field of *steganography* back in the 1990s. The second question has become the subject of intense activity halfway through the last decade with the advent of the field of digital forensics, and it has been labeled *counterforensics*. Only recently [1], [2], [3] it has been realized that the very same codes which were originally proposed by Slepian in 1965 for the scenario of communication through a noisy channel, are in fact the theoretical and practical optimum solution to canonical problems both in steganography and counterforensics.

II. Foundations of Information Security

In this section we will discuss the general reasons why permutation coding is a fundamental tool in information security.

A. Optimum Hypothesis Testing

Optimum hypothesis testing plays a fundamental role both in steganography and in forensics. This is because in both fields an adversary exists who can perform a binary hypothesis test in order to detect some property of a signal:

- In digital steganography the adversary is a *warden* who intercepts a signal sent between two communicating parties and tries to ascertain whether it carries hidden information or not[1]. This operation is usually called steganalysis.
- In digital forensics the adversary is a *forensic examiner* who tries to determine whether a given signal has been tampered with or not, that is to say, he tries to determine its authenticity.

The best detection tool available to the warden and to the forensic examiner is optimum binary hypothesis testing, which is implementable through Neyman-Pearson's lemma [4]. This lemma proves the uniformly most powerful hypothesis test, which is a likelihood ratio relying on probability distributions that model the two hypotheses (null hypothesis, indicating a negative result of the test, versus alternative hypothesis).

B. First-Order Detection Avoidance

Both the *steganographer* (person who hides information in a host signal) and the *forger* (person who creates a forgery) wish to evade a detection test. If they are able to evade the aforementioned optimum binary hypothesis test then they will be able to evade *any* test. Consequently it is best to assume that the warden or forensic detector perform optimum detection, which maximizes security from their viewpoint.

Let us next denote by $\mathbf{x} = [x_1, \cdots, x_n]^t \in \mathbb{Z}^n$ either the host signal available to the steganographer or the original signal available to the forger, and by $\mathbf{y} \in \mathbb{Z}^n$ an information-carrying signal produced by the steganographer or a forgery produced by the forger, respectively. If one assumes initially that the optimum detection test only uses first-order statistics, then one can see that the null hypothesis is completely characterized by a probability distribution $p_X(x)$ which models any sample in vector $\mathbf{x}$. If this distribution is known, then the steganographer and the forger can always foil optimum detection provided that they only produce signals $\mathbf{y}$ whose samples are outcomes of $p_X(x)$, because these signals will always be classed under the null hypothesis.

[1] It must be made clear that the related field of watermarking only requires imperceptibility of the hidden information, but not undetectability.

But what should they do when $p_X(x)$ is not known? This situation is common: consider, for instance, the case in which vector $\mathbf{x}$ represents a natural image in the spatial domain. In this situation the steganographer and forger may resort to Occam's razor, in the form of the so-called *universal* approach to statistical modeling: the use of empirical distributions as proxies of theoretical distributions. If we only consider first-order statistics, empirical distributions are essentially histograms, which are defined as follows: if vector $\mathbf{v} \in \mathbb{Z}^q$ contains the $q \leq n$ unique values in $\mathbf{x}$, then the histogram of $\mathbf{x}$ with support in $\mathbf{v}$ is just a vector $\mathbf{h}_\mathbf{x} = [(h_\mathbf{x})_1, \cdots, (h_\mathbf{x})_q]^t$ such that $(h_\mathbf{x})_k$ is the number of times that v_k appears in $\mathbf{x}$. The universal model of the true distribution $\mathbf{p} \triangleq [p_X(X = v_1), \cdots, p_X(X = v_q)]^t$ is the empirical probability distribution obtained by normalising the histogram, that is, the empirical estimate of $\mathbf{p}$ is $\hat{\mathbf{p}} \triangleq (1/n)\mathbf{h}_\mathbf{x}$.

Last but not least, note that first-order statistics can only completely characterize signals whose samples are mutually independent. This condition does not include many signals of interest, such as multimedia signals. However, it can always be approximated by means of decorrelation techniques.

C. The Fundamental Role of Permutation Codes

We thus arrive at a juncture in which it is clear that both the steganographer and the forger wish to produce signals $\mathbf{y}$ with the same empirical first-order statistics as $\mathbf{x}$, i.e., the same histogram, since doing so will foil optimum detection tests with complete certainty, importantly, even if the distribution $p_X(x)$ is unknown. It is now that we can see why permutation codes are fundamental in information security: the only vectors $\mathbf{y} \in \mathbb{Z}^n$ for which $\mathbf{h}_\mathbf{y} = \mathbf{h}_\mathbf{x}$ (for the same support $\mathbf{v}$) must be permutations of $\mathbf{x}$, that is to say, $\mathbf{y} = \Pi\mathbf{x}$ for some $n \times n$ permutation matrix Π. Therefore, the fundamental codes both in steganography and counterforensics are the Variant I permutation codes originally proposed by Slepian [5] for communication through a noisy channel. In this scenario the encoder sends $\mathbf{y} = \Pi\mathbf{x}$, and the decoder determines the most likely sent signal from $\mathbf{z} = \mathbf{y} + \mathbf{n}$, where $\mathbf{n}$ is channel noise.

The choice of $\mathbf{x}$ in information security scenarios bears important differences with respect to its choice in communications. In the latter scenario the encoder has complete freedom to choose $\mathbf{x}$, typically in order to minimize the probability of decoding error; the base vector $\mathbf{x}$ has to be transmitted thereafter to the decoder, prior to the start of communications. However, in steganography the steganographer has no freedom to choose $\mathbf{x}$, since this signal is a given host within which he wishes to hide information, and moreover $\mathbf{x}$ cannot be communicated to the decoder (*blind* data hiding). On the other hand, in counterforensics the forger can only choose $\mathbf{x}$ from among the class of authentic (natural) signals.

III. Fundamentals of Permutation Coding in Steganography and Counterforensics

In this section we will sketch the main practical issues and connections found in the application of permutation coding to steganography and counterforensics. We will also see that the so-called *rearrangement inequalities* [6] play a role in each of these two fields. These inequalities apply to the inner product of any two real vectors $\mathbf{u}$ and $\mathbf{v}$, and they can be written as

$$\overrightarrow{\mathbf{u}}^t \overleftarrow{\mathbf{v}} \leq \mathbf{u}^t\mathbf{v} \leq \overrightarrow{\mathbf{u}}^t \overrightarrow{\mathbf{v}}, \tag{1}$$

where $\overrightarrow{\cdot}$ indicates sorting in nondecreasing order and $\overleftarrow{\cdot}$ indicates sorting in nonincreasing order.

A. Steganography

In the steganography problem the steganographer embeds messages in a host $\mathbf{x}$ by producing signals $\mathbf{y}$ with the same empirical distribution as $\mathbf{x}$. The warden will be unable to determine that this signal carries information just by observing its histogram, as we discussed in Section II. The steganographer can only produce $r = \binom{n}{\mathbf{h}_\mathbf{x}} = n!/((h_\mathbf{x})_1! \cdots (h_\mathbf{x})_q!)$ such signals. If he wishes to send message $m \in \{0, 1, \cdots, r-1\}$ he must find a permutation matrix Π_m associated to this message, and then produce $\mathbf{y} = \Pi_m\mathbf{x}$. The decoder receives $\mathbf{y}$, and must retrieve m without access to $\mathbf{x}$. The main difficulty found is that r is generally an exceedingly large number. For example, in the conservative case in which $\mathbf{x}$ contains $n = 100$ different values r is of the order of 10^{360}. Therefore, encoding or decoding by means of a lookup table in which messages index rearrangements of $\mathbf{x}$ is virtually impossible, due to the exponentially growing requirements.

The key to overcoming this complexity issue lies in a closer look at the *embedding rate*, which measures how many bits of information per signal sample can be encoded. This rate is simply $\rho = (1/n)\log_2 r$ bits/host element. Now, assuming that all factorials in this expression are large, we may apply Stirling's approximation $\log x! \approx x \log x - x$ to see that $\rho \approx H(X)$, where X is a random variable with distribution $\hat{\mathbf{p}}$ (*type* of $\mathbf{x}$) and $H(\cdot)$ is the entropy of X, i.e. $\rho \approx -\sum_{k=1}^{q} \hat{p}_k \log_2 \hat{p}_k$. Therefore, the entropy of the host is approximately the maximum embedding rate if one wishes to implement perfect (undetectable) steganography.

It should be now recalled that $H(X)$ is also the optimum lossless compression rate of a signal with distribution $\hat{\mathbf{p}}$, which means that *all* possible n-vectors having this empirical entropy can be represented using $nH(X)$ bits. The way to do so in practice is through arithmetic coding (entropy coding) [7]. This implies that arithmetic coding can also be used to implement permutation coding, thus crucially circumventing the aforementioned complexity issue: any possible message m can be specified with $\log_2 r \approx nH(X)$ bits; decompressing this bitstream using arithmetic decoding and the statistics of the host will yield a vector $\mathbf{y}$ with the desired empirical distribution $\hat{\mathbf{p}}$, that is to say, a permutation of the host[2]. Retrieving the message m at the decoder just requires compressing $\mathbf{y}$ using arithmetic coding. This connection between permutation coding and arithmetic coding embodies the duality between steganography and lossless compression that was postulated from the start of the field in the 1990s.

To conclude this section, we should briefly mention that, like in other data hiding problems, an imperceptibility constraint must be typically imposed in steganography. Equivalently, the so-called *embedding distortion* must be bounded in expectation or deterministically, i.e. $\|\mathbf{y} - \mathbf{x}\|_2^2 \leq D$. This can

[2]In practice, *adaptive* arithmetic coding must be used, and the adaptation procedure must be reversed in order to guarantee that a permutation of $\mathbf{x}$ is exactly obtained; this is straightforward, and the details can be found in [1].

be easily achieved by partitioning $\mathbf{x}$ into subvectors containing values within close vicinity of each other, as described in [1]; partitioning will decrease the embedding distortion but also the embedding rate. However, the rate-distortion tradeoff achieved through partitioning is near optimal [2]. In any case, from the lower bound in (1) the embedding distortion is always upper bounded as $\|\mathbf{y}-\mathbf{x}\|_2^2 \leq 2(\|\mathbf{x}\|_2^2 - \overrightarrow{\mathbf{x}}^t\overleftarrow{\mathbf{x}})$.

B. Counterforensics

In the counterforensics problem the forger possesses an imperfect forgery $\mathbf{z}$ (imperfect because he does not know whether it is detectable or not) and an authentic signal $\mathbf{x}$. His task is finding a signal $\mathbf{y} = \Pi\mathbf{x}$ that minimizes $\|\mathbf{z}-\mathbf{y}\|_2^2$, since this will render a signal as similar as possible to the imperfect forgery $\mathbf{z}$ but which will always be classed as authentic by a first-order forensic detector, because it has the histogram of an authentic signal, as we discussed in Section II.

Finding this minimum might seem very difficult, since we have seen that the number r of different permutations grows exponentially on n. Nevertheless we will see next that, like in the steganographic problem, the solution is computationally feasible. Minimizing $\|\mathbf{z}-\Pi\mathbf{x}\|_2^2$ on Π is equivalent to maximising the bilinear form $\mathbf{z}^t\Pi\mathbf{x}$ on Π. We know from the upper bound in (1) that $\mathbf{z}^t\Pi\mathbf{x} \leq \overrightarrow{\mathbf{z}}^t\overrightarrow{\mathbf{x}}$. Therefore, if $\overrightarrow{\mathbf{z}} = \Pi_z\mathbf{z}$ and $\overrightarrow{\mathbf{x}} = \Pi_x\mathbf{x}$, an optimum permutation matrix is $\Pi_z^t\Pi_x$. In practice the forger simply has to sort $\mathbf{z}$ and $\mathbf{x}$, which is a low complexity operation, and then obtain $\mathbf{y}$ by replacing the largest element of $\mathbf{z}$ by the largest of $\mathbf{x}$, the second largest element of $\mathbf{z}$ by the second largest of $\mathbf{x}$, and so on.

It is worth noting that the optimum minimum-distortion solution that we have given above has been independently discovered and rediscovered through the years by researchers in various fields following different approaches. This is because optimum counterforensics is formally identical to —at least— two seemingly unrelated fields:

- Lossy source coding using permutation codes [8]: the first step to encode $\mathbf{z}$ using a permutation code with base codeword $\mathbf{x}$ requires quantizing it to the closest codeword, which is essentially what we have done above. The optimum procedure above was already found by Slepian using mathematical induction (see [5]).
- Exact histogram specification [9]: what we have actually done above is finding the closest version of $\mathbf{z}$ with exactly the same histogram as $\mathbf{x}$. Many works in this field have arrived at the same solution as we have through different rationales, but, to the best of our knowledge, without proving its optimality in the Euclidean distance sense.

IV. Geometric View of Information Security

The properties of permutation codes also allow a geometric interpretation of steganography and counterforensics. Clearly, all permutation codewords lie in a plane with equation $\sum_k y_k = \sum_k x_k$. Furthermore any p-norm is preserved for all permutation codewords, that is to say, $\|\mathbf{y}\|_p = \|\mathbf{x}\|_p$. In particular, the 2-norm implies that all permutations lie on a sphere of radius $\|\mathbf{x}\|_2$. These basic facts are depicted in Figure 1. Apart from the intuitive insights that can be gathered from this interpretation, its main practical consequence is the establishment of bounds on the maximum distortion in steganography and on the minimum distortion in counterforensics. Although we have already seen that the tightest distortion bounds are given by the rearrangement inequalities (1), geometric distortion bounds are much more easily amenable to analysis, since they do not involve sorting operations. Further information about these can be found in [2] and [3].

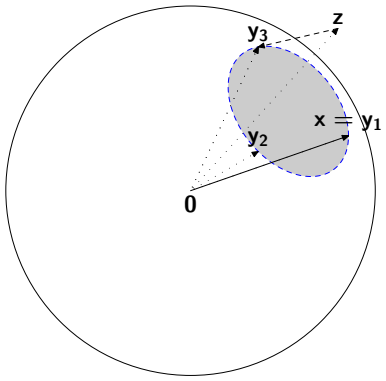

Fig. 1. Geometric interpretation. In this toy example $\mathbf{x} = [3, 7, 3]^t$ and thus $r = 3$. In steganography $\mathbf{x}$ is the host, and only three different messages can be sent. In counterforensics $\mathbf{x}$ is an authentic signal and the permutation closest to the imperfect forgery $\mathbf{z}$ must be found.

V. Conclusions

This tutorial has reviewed the central role played in multimedia security by permutation coding, as the optimum universal approach to foiling first-order statistics detection.

Acknowledgment

F. Balado would like to thank the University of Saint-Étienne for having supported this work through an invited professorship. This research is also supported by Science Foundation Ireland under grant 09/RFP/CMS2212.

References

[1] F. Balado and D. Haughton, "Permutation codes and steganography," in *38th IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Vancouver, Canada, May 2013, pp. 2954–2958.

[2] ——, "Optimum perfect steganography of memoryless sources as a rate-distortion problem," in *5th IEEE Int. Workshop on Information Forensics and Security (WIFS)*, Guangzhou, China, November 2013.

[3] F. Balado, "The role of permutation coding in minimum-distortion perfect counterforensics," in *39th IEEE Int. Conf. on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, Italy, May 2014.

[4] H. Van Trees, *Detection, Estimation, and Modulation Theory*, ser. Detection, Estimation, and Modulation Theory. Wiley, 2004, no. pt. 1.

[5] D. Slepian, "Permutation modulation," *Procs. of the IEEE*, vol. 53, no. 3, pp. 228–236, 1965.

[6] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*. Cambridge at the University Press, 1934.

[7] R. C. Pasco, "Source coding algorithms for fast data compression," Ph.D. dissertation, Stanford University, May 1976.

[8] T. Berger, F. Jelinek, and J. Wolf, "Permutation codes for sources," *IEEE Trans. on Information Theory*, vol. 18, no. 1, pp. 160 –169, January 1972.

[9] D. Coltuc, P. Bolon, and J. Chassery, "Exact histogram specification," *IEEE Trans. Image Processing*, vol. 15, no. 5, pp. 1143–1152, May 2006.