<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Optimum Exact Histogram Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authors(s)</strong></td>
<td>Balado, Félix</td>
</tr>
<tr>
<td><strong>Publication date</strong></td>
<td>2018-04-20</td>
</tr>
<tr>
<td><strong>Conference details</strong></td>
<td>2018 IEEE International Conference on Acoustics, Speech and Signal Processing, Calgary, Alberta, Canada (ICASSP-2018), 15-20 April 2018</td>
</tr>
<tr>
<td><strong>Publisher</strong></td>
<td>IEEE</td>
</tr>
<tr>
<td><strong>Link to online version</strong></td>
<td><a href="https://2018.ieeeicassp.org/">https://2018.ieeeicassp.org/</a></td>
</tr>
<tr>
<td><strong>Item record/more information</strong></td>
<td><a href="http://hdl.handle.net/10197/9975">http://hdl.handle.net/10197/9975</a></td>
</tr>
<tr>
<td><strong>Publisher's statement</strong></td>
<td>© 2018 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.</td>
</tr>
<tr>
<td><strong>Publisher's version (DOI)</strong></td>
<td>10.1109/ICASSP.2018.8462242</td>
</tr>
</tbody>
</table>
OPTIMUM EXACT HISTOGRAM SPECIFICATION

Félix Balado

School of Computer Science
University College Dublin, Ireland

ABSTRACT

Exact histogram specification (EHS) is a classic image processing problem which generalises histogram equalisation. Over the years, no optimum solution to the EHS problem has been given with respect to any similarity criterion. An analytic and efficient solution to the optimum EHS problem, according to the mean squared error (MSE) criterion, is presented here. The inverse problem is also examined, and closed-form performance analyses are given in both cases.

Index Terms—Exact histogram specification, histogram matching, histogram equalisation.

1. INTRODUCTION

The exact histogram specification (EHS) problem (less often called direct histogram specification, histogram matching, histogram modification, or histogram modelling) is a classic image processing problem that finds its roots in the generalisation of the concept of histogram equalisation by Zhang [1]. For years, the solution to the EHS problem was known to be unique in the continuous case. In 2006 Coltuc et al. [2] showed that the lack of uniqueness in the discrete case—the most relevant in practical image processing—could be overcome by using strict pixel orderings. This work sparked a peak of activity around the EHS problem [3, 4, 5, 6, 7]. However, the problem remains unsolved in terms of analytical optimality under any similarity criterion. No closed-form performance analyses have been provided either. Here we solve the optimum EHS problem using the minimum Euclidean distance criterion (i.e., the minimum MSE) to gauge optimality. We then analyse the inverse problem, and we put forward a reconstruction strategy which improves on the state of the art. We give closed-form performance analyses for both problems. Our results hinge on the centrality of permutations in EHS.

1.1. Notation

Boldface lowercase Roman letters are column vectors. The i-th element of vector a is a_i. The special symbols 0 and 1 are the all-zeros and the all-ones column vectors, respectively, of length given by the context. Capital Greek letters denote matrices; the entry at row i and column j of A is (A)_{i,j}. (\cdot)^{\top} is the transpose operator. diag(a) is a diagonal matrix with a in its diagonal, whereas diag(A_1, A_2, \ldots, A_m) is a block-diagonal matrix whose blocks are the square matrices A_1, A_2, \ldots, A_m, not necessarily of same dimensions. I is the identity matrix. The 2-norm of a is \|a\| = \sqrt{a^\top a}. Calligraphic letters are sets, and |V| is the cardinality of set V. The indicator function is defined as \mathbb{1}_\emptyset = 1 if logical expression \emptyset is true, and zero otherwise.

We will focus on greyscale images. An image is denoted by an n-vector x = [x_1, x_2, \ldots, x_n]^\top \in \mathcal{V}^n where \mathcal{V} = \{v_1, v_2, \ldots, v_q\} \subset \mathbb{Z}. We assume that x^\top is obtained by concatenating the rows of the matrix of quantised image intensities. Also, v = [v_1, v_2, \ldots, v_q]^\top gives the elements of \mathcal{V} in increasing order, that is, v_1 < v_2 < \cdots < v_q. For intensities represented with b bits, v = [0, 1, \ldots, 2^b - 1]^\top and q = 2^b. The histogram of x is a vector h^x = [h_{q_1}^x, h_{q_2}^x, \ldots, h_{q_q}^x]^\top such that h_{q_k}^x = \sum_{i=1}^n \mathbb{1}_{[v_k, v_{k+1})} for k = 1, 2, \ldots, q.

Let S_n be the symmetric group, namely, the group of all permutations of \{1, 2, \ldots, n\}. A permutation \sigma \in S_n is a vector \sigma = [\sigma_1, \sigma_2, \ldots, \sigma_n]^\top where \sigma_i \in \{1, 2, \ldots, n\} and \sigma_i \neq \sigma_j for all i \neq j. This vector defines a permutation matrix \Pi_\sigma with entries (\Pi_\sigma)_{i,j} = \mathbb{1}_{[\sigma_i - 1]}(j). The reordering of an n-vector x using \sigma is the vector y = \Pi_\sigma x, for which y_i = x_{\sigma_i} for i = 1, 2, \ldots, n. Two or more different permutations may lead to the same reordering of the elements of x. Hence we will follow the convention that a rearrangement of x is a unique reordering of its elements. The number of rearrangements of x is given by the multinomial coefficient \binom{n}{n/q} = n!/(\prod_{i=1}^q h_{q_i}^x)! \cdot S_n \subset S_n denotes any set of permutations leading to all rearrangements of x. The rearrangement of x in nondecreasing order is denoted by x^1, with elements x_1^1 \leq x_2^1 \leq \cdots \leq x_n^1, whereas the rearrangement of x in nonincreasing order is denoted by x^n.

2. EXACT HISTOGRAM SPECIFICATION

The EHS problem is as follows: given an original image \mathbf{x} \in \mathcal{V}^n and a target histogram h^t \in \mathcal{V}^n and such that 1^\top h^t = n, we wish to produce an equalised version \mathbf{y} \in \mathcal{V}^n of \mathbf{x} such that h^y = h^t. A particular case is the classic problem of histogram equalisation, in which the target histogram is flat and then h^t = (n/q) \cdot 1 (assuming that q divides n). This is why EHS can be called "generalised histogram equalisation". If we define x \in \mathcal{V}^n to be an arbitrary vector with the target histogram, for instance,

\[
\mathbf{x} \triangleq \mathbf{x}^t = \left(\begin{array}{cccc}
v_1 & v_2 & \cdots & v_q \\
h_1 & h_2 & \cdots & h_q \\
h_1 & h_2 & \cdots & h_q \\
h_1 & h_2 & \cdots & h_q \\
\end{array} \right),
\]

then the problem description implies that any candidate equalised y must be a rearrangement of x. This is because h^y = h^x requires that \sum_{i=1}^n \mathbb{1}_{[y_k = y_{\sigma_i}]} = \sum_{i=1}^n \mathbb{1}_{[y_k = x_{\sigma_i}]} for all k = 1, 2, \ldots, q, which can only be true if y = \Pi_\sigma x for some permutation \sigma \in S_n. Thus, the pool of candidates for a solution to the problem of EHS is the same as the set of all rearrangements of x. Coltuc et al. [2] also discussed the combinatorics of EHS but considering the reorderings (permutations) of x rather than its rearrangements, consequently stating that there are n! possibilities instead of |S_n| = \binom{n}{n/q}.

An optimality criterion must be adopted in order to select a solution y^\ast among the pool of possibilities. The sensible criterion is the maximisation of the similarity between \mathbf{z} and y^\ast. If \delta: \mathcal{V}^n \times \mathcal{V}^n \rightarrow \mathbb{R} is a similarity measure, then optimum EHS comes down to solving the following combinatorial optimisation problem:

\[
\sigma^\ast = \arg \max_{\sigma \in S_n} \delta(z, \Pi_\sigma x).
\]
In the remainder we will assume \( \delta(z, y) = -\|z - y\| \), which implies the MSE criterion. The shortcomings of the MSE as a quality evaluator in image processing are well known [8], but one should also note that the optimum EHS problem has not yet been solved for any similarity criterion. Furthermore, we will verify that the MSE exhibits desirable properties in the context of histogram equalisation.

Before solving (2) it is interesting to highlight some connections of the optimum EHS problem. The quantization of the optimum EHS problem has not yet been solved for any similarity criterion. Also, optimum EHS solutions of the optimum EHS problem. The quantization of the optimum EHS problem has not yet been solved for any similarity criterion.

The main difference in the counterforensics problem is that \( H^x \) stems from an authentic signal \( x \) (decoy), and thus \( x \) is usually chosen from a representative database.

2.1. Optimum Exact Histogram Specification

The problem of finding a rearrangement of \( x \) closest to \( z \) in the Euclidean distance has a simple solution using the so-called rearrangement parameter in the source coding problem. Also, optimum EHS solutions of the optimum EHS problem. The quantization of the optimum EHS problem has not yet been solved for any similarity criterion. Furthermore, we will verify that the MSE exhibits desirable properties in the context of histogram equalisation.

Before solving (2) it is interesting to highlight some connections of the optimum EHS problem. The quantization of the optimum EHS problem has not yet been solved for any similarity criterion. Also, optimum EHS solutions of the optimum EHS problem. The quantization of the optimum EHS problem has not yet been solved for any similarity criterion.

Thus, the minimum squared Euclidean distance in optimum EHS is

\[
\|z - y^*\|^2 = \|z\|^2 - 2(z^\top)^\ast x^\ast + \|x\|^2.
\]

(4)

We discuss next how to produce an optimum \( y^* \) attaining (4). Since we have that \( x = x^\top \), given any permutation \( \sigma_x \) that sorts \( z \) in nondecreasing order, i.e. \( z^\top = \Pi_{\sigma_x} z \), we can write \( z^\top \Pi_{\sigma_x} x = (z^\top)^\ast x^\ast \). Consequently, a permutation matrix associated to \( \sigma_x \), in (2) is \( \Pi_{\sigma_x} \). Thus, an optimum is \( y^* = \Pi_{\sigma_x} x = \Pi_{\sigma_x} x^\ast \), which amounts to unsorting \( x^\ast \) using the inverse of a permutation that sorts \( x \). An alternative view is that \( y^\ast \) stems from replacing the \( h_k^x \) smallest elements of \( x \) by \( v_k \), the next \( h_k^x \) smallest elements of \( z \) by \( v_k \), etcetera. The complexity of this operation is that of sorting a vector, and the worst-case complexity of the best sorting algorithms is \( O(n \log n) \). We must also note that the optimum solution \( y^\ast \) maximises the average local intensity ratio \( (1/n) \text{diag}(z)^{-1} y \) (assuming \( z > 0 \) for all \( i \), i.e., the average local contrast between \( y \) and \( z \)—a relevant factor in histogram equalisation.

2.2. Nonunique Optimum Solutions

The optimum \( y^* \) is not unique whenever there are sorting ties in \( z^\top \). In order to address this question, define vectors \( x_k^\ast \) of length \( h_k^x \), for \( k = 1, 2, \ldots, q \), such that \( (x_k^\ast)^\top = (x_k^\ast)^\top = \cdots = (x_k^\ast)^\top = x^\ast \). The histograms of these vectors can be obtained using two binary \( n \times q \) matrices defined as follows: \( \Lambda^y \), with entries \( (\Lambda^y_{i,k})_{i,k} = P_i[x^\ast_i = 0] \), and \( \Lambda^y \), with entries \( (\Lambda^y_{i,k})_{i,k} = P_i(x^\ast_i = 1) \). We can now define \( H = \Lambda^y \Lambda^x \), for which it holds that \( H = \{h_k^y, h_k^x, \ldots, h_k^x\} \). This is because \( (H)_{k,i} \) gives the number of elements of \( z^\top \) with value \( v_k \) that correspond to value \( v_i \) in \( x^\ast \). Using these histograms, the number of different optimum solutions is

\[
s = \prod_{k=1}^q \binom{h_k^x}{h_k^y}.
\]

(5)

In order to spell out each of the \( s \) equivalent solutions, let \( \Xi_{\sigma_1 \ldots \sigma_q} = \text{diag}(\Pi_{\sigma_1}, \Pi_{\sigma_2}, \ldots, \Pi_{\sigma_q}) \), with \( \sigma_k \in S_q \). There are \( s \) different \( \Xi \)-matrices because \( |S_q| \) equals the \( k \)-th multinomial in (5); for any of them it holds that \( \Xi_{\sigma_1 \ldots \sigma_q} z^\top = z^\top \). As \( \Xi_{\sigma_1 \ldots \sigma_q} = \Pi_{\sigma_z} z \), we can generate all optimum solutions to the EHS problem as follows:

\[
y_{\sigma_1 \ldots \sigma_q} = \Pi_{\sigma_z} \Xi_{\sigma_1 \ldots \sigma_q} x^\ast.
\]

(6)

For the sake of choosing one of the \( s \) solutions, we will assume in the following that \( \Pi_{\sigma_z} \) corresponds to stable sorting [13], which preserves the original order of the sorting in \( z \), and that \( \Xi_{\sigma_1 \ldots \sigma_q} = I \). However (6) is important for two reasons: 1) it is the basis for accurate distortion bounding strategies in Section 2.3; and 2) it evinces that the optimum solutions to the EHS problem are an instance of partitioned permutation coding [14]. In partitioned permutation coding not all rearrangements of a vector are allowed, but only rearrangements of partitions of the vector. This is what we observe in (6): \( h^x \) induces the partitioning of \( x^\ast \) into \( q \) partitions \( x_1, x_2, \ldots, x_q \), such that only rearrangements of these partitions are permissible in order to produce rearrangements of \( x^\ast \), each of which leads to a unique \( y^\ast \).

This fact will find application in the inverse problem (Section 3).

2.3. Performance Analysis

Next, we produce bounds on the minimum distortion (4) which do not depend on sorting \( z \), and which exploit the geometry of permutations. The two basic geometric facts are: 1) since \( \|y\| = \|x\| \), all rearrangements \( y = \Pi_{\sigma_x} x \) lie on the permutation sphere centred at \( 0 \) with radius \( \|x\| \); and 2) the rearrangements also lie on the permutation plane with equation \( y^\top 1 = x^\top 1 \). Two other fundamental geometric facts are given by the theorem and proposition that follow.

**Theorem 1 (Covering Sphere):** All rearrangements \( y = \Pi_{\sigma_x} x \) contained within a covering sphere with minimum radius \( R = \sqrt{\|x\|^2 - (1/n)\|x\|^2} \) and centre \( c = (1/n)\|x\|^2 \). Equivalently, \( \|y - c\|^2 \leq R^2 \) for any rearrangement \( y \), and the \( (c, R) \) pair specifies the smallest sphere for which this is true. Furthermore all rearrangements actually lie on the surface of the covering sphere, i.e., \( \|y - c\|^2 = R^2 \) for any rearrangement \( y \).

**Proof:** See Appendix A.

**Proposition 1 (Centre of Covering Sphere):** The average of all rearrangements \( y = \Pi_{\sigma_x} x \) is the centre of the covering sphere, i.e., \( y = \left(\sum_{i=1}^n \sum_{\sigma_x \in S_n} \Pi_{\sigma_x} x \right) / (1/n) \).

**Proof:** Firstly, \( \left(\sum_{i=1}^n \sum_{\sigma_x \in S_n} \Pi_{\sigma_x} x \right) / (1/n) \) appears \( \Pi_{\sigma_x} h_i^x \) times in the second summation. With this equality and \( (1/n) \sum_{\sigma_x \in S_n} \Pi_{\sigma_x} = (1/n)11^\top \), we get \( \left(\sum_{i=1}^n \sum_{\sigma_x \in S_n} \Pi_{\sigma_x} x \right) / (1/n) \|x\|^2 = c \). □

Before proceeding, we should mention that the three geometric lower bounds given in [11] also hold in this problem. We would simply like to add that the first two bounds in [11] can alternatively be obtained by first applying Cauchy’s inequality [12] to \( (z - c)^\top (y - c) \) in \( \|z - c - (y - c)\|^2 \) and to \( z^\top y \) in \( \|z - y\|^2 \), respectively, and then using the fundamental geometric facts about...
permutations. Also, a basic upper bound can be obtained by observing that the squared distance from $z$ to $y^*$ must always be smaller or equal than its average squared distance to the ensemble of all rearrangements of $x$, i.e., $\|z - y^*\|^2 \leq \left(\frac{1}{k}\right)^{\alpha - 1} \sum_{\sigma \in S_k} \|z - \Pi_{\sigma} x\|^2$. Using the same result as in the proof of Proposition 1 we see that $\|z - y^*\|^2 \leq \|z\|^2 + \|x\|^2 - (2/n)(z^T 1) (x^T 1)$. This bound can alternatively be found by applying Chebyshev’s sum inequality [12] to $(z_k)^T x_k$ in (4). All of these bounds involve every rearrangement of $x$, and thus are generally loose. For instance, equality in Chebyshev’s sum inequality requires $x = \alpha 1$ or $z = \beta 1$, which means that the upper bound cannot be sharp in real applications. The two lower bounds stemming from Cauchy’s inequality are sharp if there is alignment between $y^*$ and $c$ or $z - c$, or between $y^*$ and $z$, respectively (as collinearity implies equality in Cauchy’s inequality), but either contingency depends on the actual $x$ and $h^s$.

Much better bounds can be found by exploiting the special geometry of the $s$ optimum rearrangements. Since $\|z - y^*\|$ is constant for all optimum rearrangements, then they lie on a sphere with that radius and centre $z$. Thus their average $\overline{y}^*$ is inside the sphere, or precisely on its surface, and thus not further away from $x$ than any of them, i.e., a lower bound is $\|z - \overline{y}^*\| \leq \|z - y^*\|$. In order to obtain $\overline{y}^* = (1/s) \sum_{\sigma \in S_k} y_{\sigma 1} - \sigma$, define vectors $c_k$ of length $h^s_k$ such that $\Pi_{\sigma} y^* = [c_1^1, c_2^1, \ldots, c_0^1]$. Now, using (6) see that

$$c_k = \frac{1}{h^s_k \sigma_k \in S_k} \sum_{\sigma \in S_k} \Pi_{\sigma} x_k = \left(1 \cdot x^k\right)_{h^s_k},$$

where the first equality in (7) is because the summation over $\sigma_k$ appears repeated $s/|S_k|$ times in the average over $\sigma_1, \ldots, \sigma_q$, and the second one is because of Proposition 1 applied to $x_k^1$. Now, $\|z - \overline{y}^*\|^2 = \|z - \Pi_{\sigma} x^1\|^2 = \sum_{k=1}^{\sigma} \|\Pi_{\sigma} x_k - c_k\|^2$, and therefore

$$\|z - \overline{y}^*\|^2 = \sum_{k=1}^{\sigma} h^s_k (v_k - (1 \cdot x^k)_{h^s_k}^2).$$

We show next that the $s$ optimum solutions live in yet another geometric locus. The square of the distance of an optimum solution $y^*$ to the average is $\|y^* - \overline{y}^*\|^2 = \Pi_{\sigma} y^* - \Pi_{\sigma} \overline{y}^*\|^2 = \sum_{k=1}^{\sigma} \|\Pi_{\sigma} x_k - c_k\|^2$. Applying Theorem 1 to each term in this sum (see (7)), and then using $\sum_{k=1}^{\sigma} \|x_k\|^2 = \|x\|^2$ we get

$$\|y^* - \overline{y}^*\|^2 = \|x\|^2 - \frac{1}{h^s_k} (1 \cdot x^k)_2^2.$$ (9)

Since (9) is independent of $y^*$, then all $s$ optimum solutions are on the surface of a fourth sphere, this time with centre $\overline{y}^*$ and radius $\|y^* - \overline{y}^*\|$. Hence, using the triangle inequality we obtain the following upper bound on the optimum distortion:

$$\|z - y^*\| \leq \|z - \overline{y}^*\| + \|y^* - \overline{y}^*\|.$$ (10)

3. INVERSE PROBLEM

The inverse EHS problem, first proposed in [15], is as follows: given $y^*$ and $h^s$, produce the best approximation to $z$. According to [7], this can be a means to gauge an EHS algorithm. In our opinion, however, an EHS method should solely be judged from its maximisation of a similarity measure and from its complexity (see Section 2). Still, the inverse EHS problem is interesting and distinct in and of itself, for reasons discussed below. Since $y^*$ is at minimum distance from $z$, then the optimum inverse must also be at minimum distance from $y^*$. So, at first sight, the inverse problem is like the EHS problem with original image $y^*$ and target histogram $h^s$, where the equalised solution can now be called the reconstruction $\tilde{z}$ of $z$.

This observation takes us to the same element pairings in the inner product $(z^T)^T x^T$, but viewed the other way round. Therefore we now create $z'$ using $h^s$ as in (1), we then sort $y^*$ to get $x^1 = \Pi_{\sigma} y^*$, and finally obtain $\tilde{z} = \Pi_{\sigma} z^1$.

3.1. Nonunique Reconstructions

As in Section 2.2, $\tilde{z}$ is not unique whenever there are sorting ties in $x^1$. Nevertheless, this fact becomes the key difference with respect to the direct EHS problem: whereas all reconstructions are at equal minimum distance from $y^*$, i.e., $\|y^* - \tilde{z}\| = \|z - y^*\|$, not all them are at equal distance from $z$. The reconstruction distortion $\|z - \tilde{z}\|^2$ is what matters in the inverse problem. The number of possible reconstructions is determined by the histograms of vectors $z^1_k$ of length $h^s_k$, for $k = 1, 2, \ldots, q$, such that $z^1_k = [z_1^1, z_2^1, \ldots, z_q^1]^T$. These histograms are again given by matrix H in Section 2.2, but using its columns rather than its rows, i.e., $H = [h^s_1, h^s_2, \ldots, h^s_q]$. Therefore the number of different reconstructions is $s' = \prod_{k=1}^{q} h^s_k$.

In general, $s' \neq s$. Each reconstruction can be put as $\tilde{z} = \Pi_{\sigma} z^1 \Xi z^1$ for some $\Xi' = \text{diag}(\Pi_{\sigma}^T, \Pi_{\sigma}^T, \ldots, \Pi_{\sigma}^T)$ with $\sigma_k \in S_k^1$. Exact reconstruction requires that $\tilde{z} = \Pi_{\sigma} z^1 \Xi z^1 = z$; thus, assuming without loss of generality that $\Pi_{\sigma} z^1$ corresponds to stable sorting of $y^*$, the main question is how to choose $\Xi'$ (because $\Pi_{\sigma}$ is unknown). The analysis that follows will give us relevant clues.

3.2. Performance Analysis and Reconstruction Approaches

Our main goal is to bound or estimate $\|z - \tilde{z}\|^2$. An optimum of the EHS problem can be written in two different ways: $y^* = \Pi_{\sigma} z^1 \Xi z^1$ and $y^* = \Pi_{\sigma} z^1 \Xi z^1$, and then $x^1 = \Pi_{\sigma} \Pi_{\sigma} \Xi z^1$. This implies that

$$\Pi_{\sigma} \Pi_{\sigma} \Xi z^1 = \text{diag}(\Pi_{\sigma}^T, \Pi_{\sigma}^T, \ldots, \Pi_{\sigma}^T),$$

where $\Pi_{\sigma}^T = h^s_k \times h^s_k$ permutation matrix for $k = 1, 2, \ldots, q$. We can exploit the structure of (11) to decompose the reconstruction distortion as follows: $\|z - \tilde{z}\|^2 = \|\Pi_{\sigma} z^1 - \Pi_{\sigma} \Xi z^1\|^2 = \|z^1 - \Pi_{\sigma} \Pi_{\sigma} \Xi z^1\|^2 = \sum_{k=1}^{\sigma} \|z_k^1 - \Pi_{\sigma} z_k^1\|^2$. Applying now the left-hand side inequality in (3) to each term in this sum, we obtain

$$\|z - \tilde{z}\|^2 \leq 2 \left(\|z^1\|^2 - \sum_{k=1}^{\sigma} \|z_k^1\|^2 \right).$$ (12)

This bound, and other results, can also be given by exploiting the exact analogy between the inverse EHS problem and perfect steganography of memoryless signals [14]. In the latter problem, $z^1_k$ would be called a host signal, $z_1^1, z_2^1, \ldots, z_q^1$ would be partitions of $z^1_k$, and $\Pi_{\sigma} z_k^1$, for $k = 1, 2, \ldots, q$, the partition rearrangements used to encode one message out of $s'$. The vector $\Pi_{\sigma} \Pi_{\sigma} \Xi z^1$ would be a watermarked signal carrying the message. Finally, the reconstruction distortion is analogous to the watermark power. Because of this analogy, if ties are broken uniformly at random when sorting $y^*$ (i.e., if $\Xi$ is chosen uniformly at random among the $s'$ possibilities), then
all the results from [14] apply unaltered, and we can accurately predict the reconstruction performance. This reconstruction procedure will be called the random approach. We refer the reader to [14] for proofs of the two results that we will simply state next. By the weak convergence (in probability, and as \( n \to \infty \)) to

\[
\|z - \bar{z}\|^2 = 2 \left(\|u\|^2 - \sum_{k=1}^{n} \frac{1}{h_k} (1|z_k|^2)\right)^2.
\]  

(13)

The reconstruction error rate \( \nu \) is (1/n) \( \sum_{i=1}^{n} \frac{1}{h_k} (1|z_k|^2) \), (cf. the degree of host change in [14]) is mentioned in [2] as an additional performance measure. In the random approach, \( \nu \) converges to \( \frac{1}{n} \sum_{i=1}^{n} h_k |z_k|^2 \) (cf. [14]). Although (13) is, in general, quite better than (12), exact reconstruction requires that \( \sum_{i=1}^{n} h_k |z_k|^2 \) be called the random approach. We refer the reader to [14] for details of the reconstruction performance. This reconstruction procedure can be obtained by choosing \( \Xi = \text{diag}(J_1, J_2, \ldots, J_n) \), where \( J_k \) is the \( h_k^\times h_k^\times \) exchange matrix. 

4. RESULTS

We assume \( h^\times = (n/q)1 \) (i.e., classic histogram equalisation) and we use each of the 24 images in [7, Figure 2] as \( z \). The peak signal-to-noise ratio (PSNR) is denoted as \( \xi = 10 \log_{10}(n(2^n - 1)/\|z - y\|^2) \) (dB). As our EHS results are provably optimum in terms of PSNR, we just verify, in the first three columns of both tables in Fig. 1, the accuracy of the tight lower and upper bounds \( \xi \) and \( \xi_u \) (which correspond to (10) and (8)) respectively with respect to the maximum \( \xi^* \) (which corresponds to the empirical \( \nu^* \)). All remaining results in Figure 1 are for the inverse EHS problem, where we reconstruct \( z \) from \( y^\times \) and all PSNRs correspond to \( \|z - \bar{z}\|^2 \) (rather than \( \|z - y\|^2 \)). Since we are not claiming optimality in the inverse problem, we compare our figures with the state-of-the-art results by Nikolova and Steidl [7] (marked as \( \xi^{(7)} \)), who found their algorithms superior to [2] and [3] (i.e., the relevant prior art). Our empirical results for the random and stable methods in Section 3 show that \( \xi \) and \( \nu^* \) in the \( \xi \) and \( \nu^* \), respectively. \( \xi^\prime \) is the lower bound corresponding to (12) and \( \nu^* \) corresponds to (13). The theoretical values accurately match their corresponding empirical, i.e., \( \xi^\prime \) and \( \nu^* \). We stress that \( \xi \) and \( \nu^* \) are not averages, but "one-shot" results. The random approach works better than (or as well as) [7] in 14/24 cases. The stable approach works better than [7] in 21/24 cases. Two remarkable cases are "raffiti" and "stream", for which the best previous results (i.e., \( \xi^{(7)} \)) are just above the worst-case \( \xi^\prime \), but for which the

stable approach achieves near-perfect reconstruction. To conclude, we have given an optimum and practical solution to EHS, supported by an accurate analysis. We have also shown the connections of EHS and inverse EHS with other seemingly unrelated research topics.

A. PROOF OF THE COVERING SPHERE THEOREM

The minimax problem to solve is \( R^2 = \min_{\mu} \max_{\mu} |y - c|^2 \). Assume initially that \( c = c^\times \). Given \( c \), the least squared radius required for covering all rearrangements is \( \max_{\mu} |y - c|^2 \). As \( |y - c|^2 = |y| - 2y^\times + |c|^2 \) and \( |y| = |x| \), we only have to minimise \( y^\times \). Since \( c = c^\times \), the inequality on the left-hand side of (3) implies that a minimising rearrangement is \( y = x^\times \). Next, we have to find \( R^2 = \min_{\mu} |x^\times - c|^2 \). The optimum \( \mu \) must be on the permutation plane since all the rearrangements are on that plane, and so \( c^1 = x^1 \). Using this equality and the inequalities \( c_{1} \leq c_{2}, c_{2} \leq c_{3}, \ldots, c_{n-1} \leq c_{n} \), we pose the following constrained optimisation problem for \( f(c) = 2c^\times - \|c\|^2 \). The optimum \( \mu \) must be on the plane and where the last equality in (17) is because the equality in vector \( \sum_{i=1}^{n} h_k |z_k|^2 \) corresponds to (12) and \( \nu^* \) corresponds to (13). The theoretical values accurately match their corresponding empirical, i.e., \( \xi^\prime \) and \( \nu^* \). We stress that \( \xi \) and \( \nu^* \) are not averages, but "one-shot" results. The random approach works better than (or as well as) [7] in 14/24 cases. The stable approach works better than [7] in 21/24 cases. Two remarkable cases are "raffiti" and "stream", for which the best previous results (i.e., \( \xi^{(7)} \)) are just above the worst-case \( \xi^\prime \), but for which the

Fig. 1. The first three columns in each table show results for optimum EHS (Section 2); the remaining columns show results for the inverse problem (Section 3). Theoretical results are shaded in grey. \( \xi^* \) are PSNRs in decibels, and \( \nu^* \) values are reconstruction error rates.
B. REFERENCES


