Visualisation of Benchmarking Results in Digital Watermarking and Steganography

Christian Krätzer

Research Group Multimedia and Security,
Department of Computer Science,
Otto-von-Guericke-University of Magdeburg, Germany

Abstract. The goal of this paper is to facilitate the discussion about fitting representation approaches for fair benchmarking and the selection and use of techniques by non-experts. To meet this goal a brief review on digital watermarking (DWM) and steganography features commonly encountered in algorithm evaluation and benchmarking is given. Then selected techniques derived from the field of information visualisation are introduced and considered for application in the visualisation of research and benchmarking results in DWM and steganography.

1 Introduction

In 1998 J. Fridrich gave an extensive overview over the state of the art on data hiding in digital imagery [1], including a definition of the data hiding term, as well as a close review on two of the most common digital data hiding techniques: digital watermarking (DWM) and steganography. In the eight years since 1998 the development of digital watermarking techniques and steganography has made large progress. In the field of digital watermarking new properties like the invertability of watermarks have to be considered as well as the shifted importance of features, which is very well illustrated by the example of complexity. This feature gained a stronger relevance with the growing importance of mobile devices and the definition of application scenarios which require real time capable watermarking algorithms. In the field of steganography of course new types of covers were considered moving from largely storage channel based approaches to more sophisticated time channel based techniques or hybrid techniques. Also here the shifting of the relevance of features shows, e.g. with the robustness of steganographic techniques which are nowadays also considering algorithms compliant with faulty communication channels [2].

Besides the actual research on DWM and steganography algorithms the comparison of benchmarking results has gained importance in scientific publications on these topics. To address this fact selected visualisation techniques are presented for discussion within the watermarking community. Some of these techniques have not been used before in DWM benchmarking and the evaluation of steganography but might prove useful in further research.

The paper is structured into the following sections: Basics on information visualisation including a notation which is used to describe the visualisation problem encountered are described in section 2. In section 3 main features of DWM and steganography algorithms are reviewed since the characteristics of these data have a strong influence on the visualisation decision. Relevance of DWM and steganography benchmarking and analysis, and therefore the appropriate visualisation of these results is emphasised in section 4. Section 5 introduces visualisation techniques, sorted by the dimensionality of the entity to be visualised. Section 6 concludes the paper.

2 Visualisation in scientific work

Robert Spence divides in [5] visualisation techniques applied in scientific work into scientific visualisation (primary related to, and representing visually, something "physical", like the flow of water in a pipe, temperature distribution in materials, etc) and information visualisation (dealing with abstract quantities e.g. baseball scores, fluctuating exchange rates between currencies, etc). Based on the nature of algorithm evaluation and benchmarking, the main focus of this document is placed therefore in what he identifies as the area of information visualisation, but we also consider selected results from scientific visualisation (like a notation for describing the visualisation task) since as a science it exceeds information visualisation in age and the maturity of theoretical research.

It is common to present data, structures and relations graphically to enable efficient analysis and communication. This presentation requires the transformation of data of different kinds into geometric information (B.H. Mc Cormick et. al [7]). The two main goals in visualisation are to present (research) results and to facilitate the analysis of the data. In [6] the importance of finding a fitting presentation for a given data set is indicated by H. Schumann and W. Müller. The application of a inappropriate presentation might easily lead to incorrect interpretations in an analysis. Therefore it is fundamental to define and describe the characteristics of a set of data (the subject of visualisation) and consider these characteristics very early in the visualisation process. Here for a description of the visualisation tasks considered a notation introduced by K.W. Brodlie et. al [8] for scientific visualisation is used and applied to information visualisation.
This notation describes the abstraction of data from a so called "underlying field" to an "entity for visualisation" E. Thereby is E an entity specified on a domain (defined by number and type of the independent variables) and yielding a range (characterised by class and dimensionality) of results. Applied to general data presentation the notation uses E_n^F for describing an entity of class F ($F \in \{S, P, V_k, T_o\}$; scalar, set of points, vector with k components or tensor field of o-th order) with an domain of order n. Also the characteristics of the domain can be described in this notation. A continuous domain is denoted with n. If the entity is defined over regions of a continuous domain the notation uses $[n]$. If the entity is defined over an enumerated set $\{n\}$ is used. It is also possible with this notation to describe the fact that multiple results are intended to be visualised

over the same domain (e.g. two scalar fields like pressure and temperature within a volume in 3D; E_3^{2S}) or to describe composite representations.
H. Schumann and W. Müller [6] and Brodlie et. al [8] introduce examples to help with the understanding of this notation. Some of these are repeated in section 5. This notation introduced for scientific visualisation now has to be applied to our needs which are mainly to be found in information visualisation. This is done by considering only what Schumann and Müller call in [6] the "abstract dimensionality" of the observed space. This includes only the data which does not contain any positional or temporal information and binding.

3 Features of steganographic applications and digital watermarking algorithms

In section 2 the importance of characteristics of the sets of data to be visualised is highlighted. Therefore the main features of steganographic applications and DWM algorithms are reviewed here to provide knowledge necessary for the application of visualisation techniques. The description of features given is based on the work of J. Fridrich introduced in 1998 in [1] for data hiding techniques in the image domain. There the most important properties of data hiding schemes were identified as robustness, undetectability, invisibility, security, complexity, and capacity. Based on the definitions given there and using the knowledge that some of the above properties (namely robustness, capacity and undetectability/transparency) are mutually competitive, clear requirements for the construction of watermarking and steganographic algorithms can be derived. In the following the features of steganographic systems and DWM approaches are reviewed briefly for their requirements in presentation techniques.

Capacity: Basically the capacity definitions in steganography and DWM are the same. The question is how much data can be embedded within one byte or one second of cover. Sometimes constrains like a predefined transparency threshold have an impact on the maximum embedding strength applicable. In steganography generally more capacity is better, in DWM the required capacity strongly depends on the chosen application scenario. For example annotation watermarking might require a large capacity at relatively small proportions of the marked object. Necesary information regarding the co-domain of functions computing the capacity is that it is commonly a non-negative, continuous value, which in most cases does not exceed the capacity of the cover.

Robustness: [1] states that the embedded information is said to be robust if its presence can be reliably detected after the image has been modified but not destroyed beyond recognition. In this definition robustness means the resistance to blind, non-targeted modifications or image operations. This image domain based description of the term robustness has been outdated by the emergence of watermarking evaluation tools like Stirmark Benchmark ([9], [10]) or Stirmark Benchmark for Audio (SMBA; e.g. [11]). Lang et. al measure the robustness of a watermarking algorithm for their SMBA in terms of robustness against a pre-

defined set of attacks (signal modifications).
This approach, which tests DWM algorithms against blind, targeted modifications, can be transferred to steganography (see [13], [2]) but here in addition to the integrity of the message the impact of the embedding on the cover(-protocol) has to be considered. If results for this approach used by Lang et. al have to be visualised, the co-domain concerned is a discrete value in the range between zero and the maximum number of attacks. Since the attacks can be grouped into classes depending on the domain they work in or the type of modification they perform, there a need to use a vector might arise to adequately describe the robustness results for the different classes identified.

Transparency (Perceptual transparency and statistical undetectability): [1] distinguishes between the two terms Undetectability (an image with an embedded message is consistent with a model of the source from which images are drawn) and Invisibility (an average human being is not capable to distinguish between carriers that do contain hidden information and those that do not). Instead of this approach to describe the transparency of a message embedding in two terms we would like to refer to a more recent and more formal approach given in [3]. There both terms used in [1] (Undetectability and Invisibility) are joined to form a more appropriate measure labelled transparency. In [3] the differences between transparency considerations in the fields of steganography and digital watermarking are considered in detail, highlighting amongst others the importance of transparency as the main feature in steganography and the strong dependance on the selected application scenario for the transparency requirements in DWM.
In the presentation of transparency results for selected algorithms scalar values or vectors containing the results from an analysis with different measurements are the most common output. Ranges differ depending on the measurement applied (e.g. ODG as defined in [12]).

Security: [1] states that an embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector (except the secret key), and the knowledge of at least one carrier with a hidden message. Since 1998 many publications have addressed the security of steganography and DWM algorithms respectively with attacks on their security. Examples in the field of watermarking are [14] and [15]. Steganalytic approaches (which can be considered as security attacks at this point) have been classified into groups in [16].
One important question to address is: how can security in steganography and DWM be measured? One possibility which might be applicable is the transfer of the classification paradigm from cryptographic security (a discrete scale ranging from “unconditionally secure” to “secure enough”). In this case no normalised representation can be applied for this discrete classification in an useful manner.

Invertability: The feature of invertability is a new DWM paradigm which has been developed after [1] was published. So far no application of invertability in steganography is known to the author. Nevertheless it might be useful to research the possibility of constructing invertible steganographic protocols and algorithms and their impact on deniability (or non-repudiation) of the communication. The representation of this feature is usually a 1-Bit value (binary decision). Therefore for invertability as well as for security a representation has to be found which takes the non-continuous nature of this feature into account.

Additional features: Additional features might be identified as being necessary for a complete description of the performance of an algorithm. As a good example the complexity of the embedding and detection processes shall be mentioned which might be a necessary criterium for the decision whether an algorithm could be used on mobile devices (which normally possess limited computational capabilities). In the visualisation of the results for features not described in detail in this paper the same rule identified in section 2 applies as for the ones described here: the characteristics of a set of data (the subject of visualisation) have to be analysed and have to control the visualisation process.

Relation between characteristics: In her publication [1] J. Fridrich points out that some (namely capacity, robustness and transparency) of the characteristics mentioned above are mutually competitive when considered as requirements for information hiding techniques. Unfortunately no universal linear or functional relationship between the characteristics can be identified for the domain of information hiding techniques which would allow for a dimensional reduction in the visualisation problem.

4 Evaluation of steganography and digital watermarking approaches

What divides steganography and DWM is in most cases only the intention for which a technique is used. If steganography is seen as a means for a hidden end-to-end communication it has more in common with cryptography, which also provides privacy mechanisms for communications, than with digital watermarking. Therefore its evaluation (called steganalysis) is in many cases very similar to cryptanalysis. Benchmarking approaches for steganography algorithms or applications are uncommon (for the same reason as there is no standardisation organisation for steganography), instead steganalysis tools are benchmarked at a large scale. For obvious reasons the scientific community is more interested in creating the perfect universal, blind steganalyser than in finding the perfect steganography approach. Nevertheless the development of an advanced steganalysis tool does require the existence of advanced steganography applications. And these advanced steganography applications have to fulfill certain requirements regarding the characteristics identified in section 3. Most important is that they have to be very transparent. As an additional feature a high capacity would be significant. The robustness is neglected in most discussions about the performance of steganography algorithms, but depending on the application scenario it might be useful to sacrifice some capacity to gain robustness against format conversions [13] or the influence of a faulty communications channel.

In contrast to steganography, where only one well-defined application scenario exists, digital watermarking has a large spectrum of possible means for application (annotation watermarking, watermarking for forensic tracking purposes, etc). Therefore in DWM the approach of benchmarking algorithms is more common than in steganography and is used to characterise selected watermarking algorithms and their fitness for one of the application scenarios. For examples on these benchmarking activities see publications concerning the WET [18] and Audio WET [17] suites. The different application scenarios have of course an impact on the relevance of certain features of the algorithm and the visualisation for research results in this area. If a problem can be considered from different angles or perspectives (application scenarios) then a graphical representation has to be as generic as possible, to cover all these angles, but at the same time it should be as intuitive as possible since it already represents a very complex problem.

As an additional factor influencing the visualisation of results for steganography and DWM algorithms many features (like capacity, transparency and robustness) might be context sensitive for selected algorithms. Therefore when testing these features on a large test-set the results of a binary or discrete decision might become "blurred" or continuous. This might result in the necessity to introduce decision thresholds, quantisation steps or the expression using probabilities, error rates or ϵ-environments in the visualisation problem.

5 Realisation in Visualisation

R. Spence implies in [5] that since we are living in a three-dimensional (3D) world one would imagine that a 3D display of data would be regarded as "natural". In practice this is limited by the capabilities of today's presentation equipment. Due to these capabilities the most commonly used forms are the textual or a two-dimensional (2D) representation of information of n-dimensional $(1 \leq n \leq \infty)$ origin (also known as hypervariate or multivariate data [5]). Common techniques employed in the graphical representation are the projection of the n-dimensional space onto all pairs of axes or the usage of perspective presentations with a distorted 3rd axis (sometimes also called $2\frac{1}{2}$-D representations) for the presentation of 3D data. General problems are encountered which apply to any visualisation technique independent of the dimensionality. A good example is the question: *Which kind of scale (linear, logarithmic, etc) should be applied?*

In the following realisations for the description of (research) results in the contexts of steganography and DWM research are presented. The range of techniques introduced includes general visualisation methods applied in this field and more specific presentations taken from recent publications. First the non-graphical representation is reviewed and then visualisations are given, sorted by increasing dimensionality of the domain of the entity for visualisation using the notation of Brodlie et. al [8].

5.1 Non-graphical representation

The first form of description and comparison of (test-)results to be mentioned is one that can not be placed in Brodlies notation. Nevertheless the presentation in text form is one of the techniques most commonly used in scientific publication. A special form of the presentation in text form is the presentation in tables, allowing for a more structured presentation with possibilities for faster comparison. The following example was taken from [3] and describes, first in text form and then in table 1, the results of a transparency measurement (as the absolute value of the average ODG over a test-set of 389 files) on four selected steganography algorithms (denoted A_S with different parameterisations): *From these results it can be seen that all four A_S used with all parameters tested have a very similar embedding transparency (which in all cases is about* 0.02 *and therefore has to be considered very transparent). Differences can be foun on detail level, when considering the detection process and the context dependency of the algorithm.*

A_S	**Param.**	**avg. embed. t.** $[\|ODG\|]$
Publimark (v. 0.1.2)		0.0180
Steghide (v. 0.4.3)	Enc./ECC ON/OFF	[0.0255 .. 0.0275]
Steghide (v. 0.5.1)	Enc. std./OFF, ...	[0.0232 .. 0.0265]
LSB (v. Heutl051208)		0.01797

Table 1: Computed average $|ODG|$ values for all A_S and their parameters (taken from [3]).

5.2 Using entities for visualisation of dimensionality $n = 1$

The one-dimensional domain leads to (apparently) simple results in presentation. Despite most of the visualisation forms located in this domain are well known, examples are presented here for two reasons: first to facilitate the application of the notation used and second to derive knowledge for the higher dimensional representations from this class of visualisations.

1D scatter plot (E_1^P): The one-dimensional scatter plot is a simple technique projecting test results onto a single axis. Relationships between the different results are expressed in their distance. Additionaly an order is indicated. An example for a 1D scatter plot is given in figure 1 where test results from table 1 are visualised. A problem encountered in this example is the fact that some of the values given in table 1 are representing ranges (results computed using different parameterisations). The solution chosen here depicts only the minimum and maximum value of these ranges.

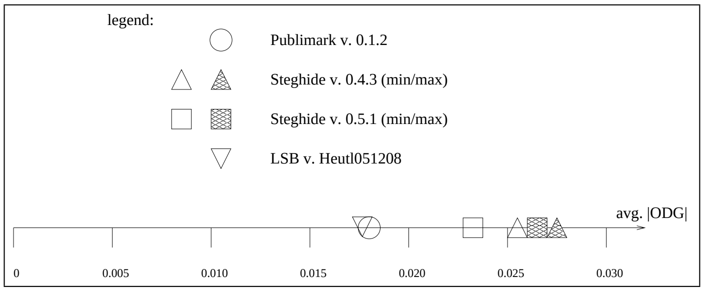


Fig. 1: Transparency results from table 1 as 1D scatter plot (ranges are given with min. and max. values).

Line graph, multiple line graphs (E_1^S, E_1^{mS}): In the line graph of a function the entity is defined pointwise over an interval of the continuous real line (input). An example for superimposed line graphs is given in figure 2. This example, taken from [21], shows the development of the standard deviation of transparency results on a DWM algorithm and different classes of audio material with a varied parameter. The functions are interpolated from a discrete set of measurements. Problems introduced by this interpolation are discussed in detail in [8].

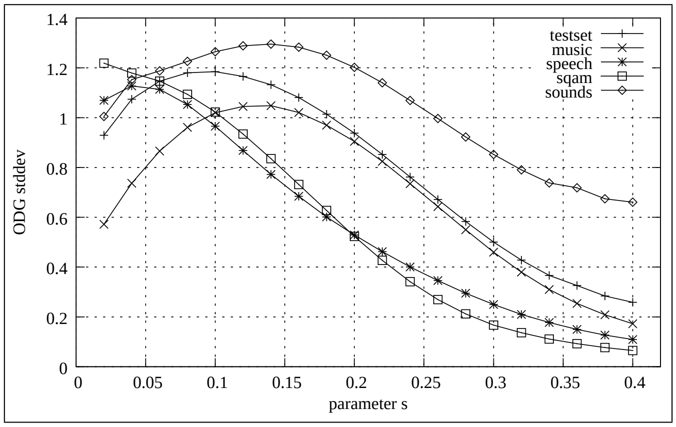


Fig. 2: Interpolated development of the standard deviation of transparency results on a DWM algorithm and different classes of audio material (taken from [21]).

Histogram and Bar chart ($E_{[1]}^S$ and $E_{\{1\}}^S$): In a histogram the entity is defined over regions of the real input. The data is aggregated into bins. The number of elements in each bin is shown in the histogram. The histogram in figure 3 (a) was taken from [19]. It shows the distribution of lengths of delays in a WLAN with and without steganography.

A bar chart depicts the values of items in an enumerated set. If the values can be seen as fractions of a whole then the results could be expressed also as a pie chart. Figure 3 (b) shows a classic example for a bar chart taken from [3].

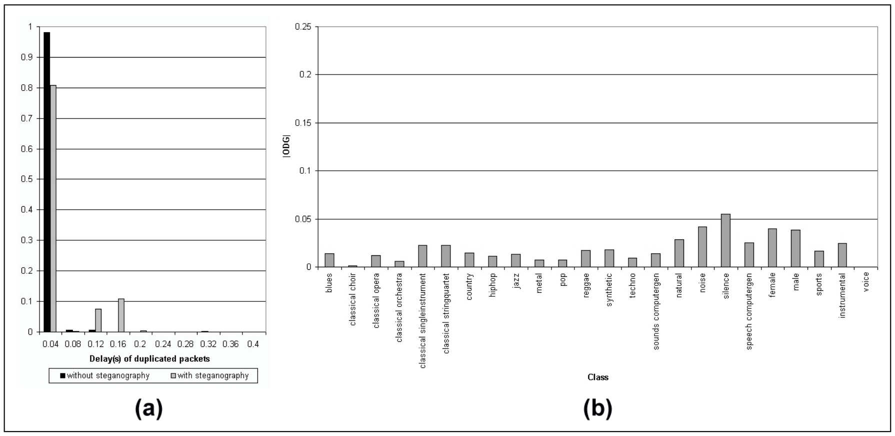


Fig. 3: (a) Results for the delays between WLAN packets with set "Retry" field and the corresponding original packets with and without WLAN steganography (taken from [19]); (b) Transparency results for a steganography algorithm on a test-set grouped into 24 classes of audio material (taken from [3]).

Pixel-based techniques (E_1^S or $E_1^{[S]}$): A technique very similar to the classical histogram is introduced in [6]. This pixel-based technique can be used to visualise results for large sets by representing each element in the set with a marker object (usually a line) with a width of one pixel and a fixed length. To encode the results for each marker object usually colour-coding is applied. In the example given in figure 4 the results from transparency benchmarks on three (two steganography and one watermarking) algorithms are represented. In this case the results were grouped into three classes (regions) and encoded with the colouring of the marker lines in white, grey and black.

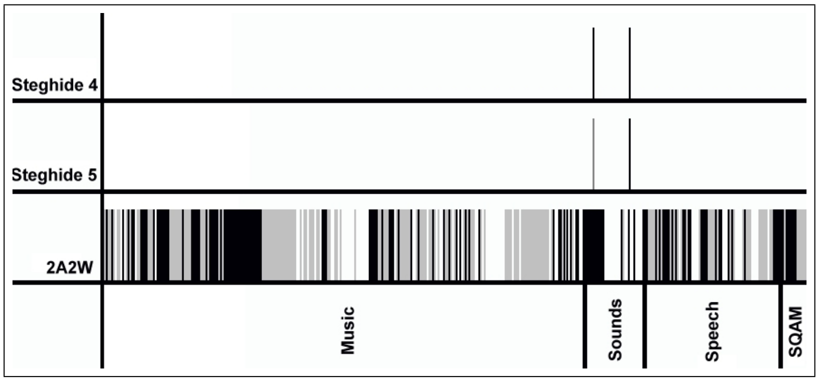


Fig. 4: Results from the transparency benchmarking for two steganography and one watermarking algorithm over a test set of 389 files. The computed $|ODG|$ value is colour-coded in three classes: below 0.2 (white), between 0.2 and 1 (grey) and above 1 (black). (Values taken from [3])

The problem encountered in this visualisation form is the fact that colour-coding always has to follow certain rules reducing the maximum number of marker objects. These rules are based on the limited capabilities of the HPS (Human Perceptual System) like the limited number of colours distinguishable and possible limitations regarding individuals (e.g. colour vision deficiencies [4], [6]) or the limitations of the chosen presentation media (e.g. black-and-white print media). The consequences of these rules for the example shown above can be found in the constriction to three defined classes (regions) for the results, which results in a very low resolution for the transparency values. Nevertheless this example shows very impressively the difference between steganography and watermarking algorithms with regards to embedding transparency.

5.3 Using entities for visualisation of dimensionality $n = 2$

The natural dimensionality of print media as well as common computer displays is 2D. Therefore it would be intuitive to choose two-dimensional entities for representation in scientific work, which is most commonly communicated in print or electronic documents mimicking their printed counterparts in appearance. The fact that entities of this dimensionality are not the most common objects chosen is justified by the point that in scientific work the representation of higher dimensionality is more interesting. Nevertheless with the 2D scatter plot one example is introduced here which can be found quite often in scientific publications.

2D scatter plot (E_2^P): In this traditional scatter plot pairs of values are represented as points in the plane. The example shown in figure 5 was already used as the basis for generating figure 2 by interpolating the functions.

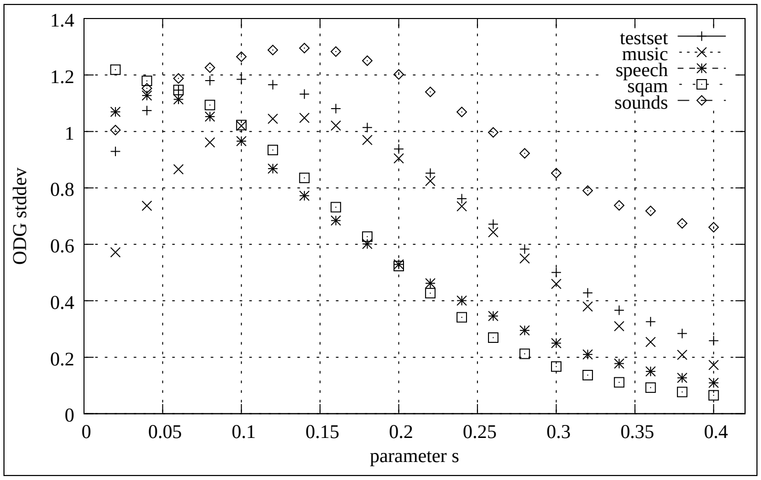
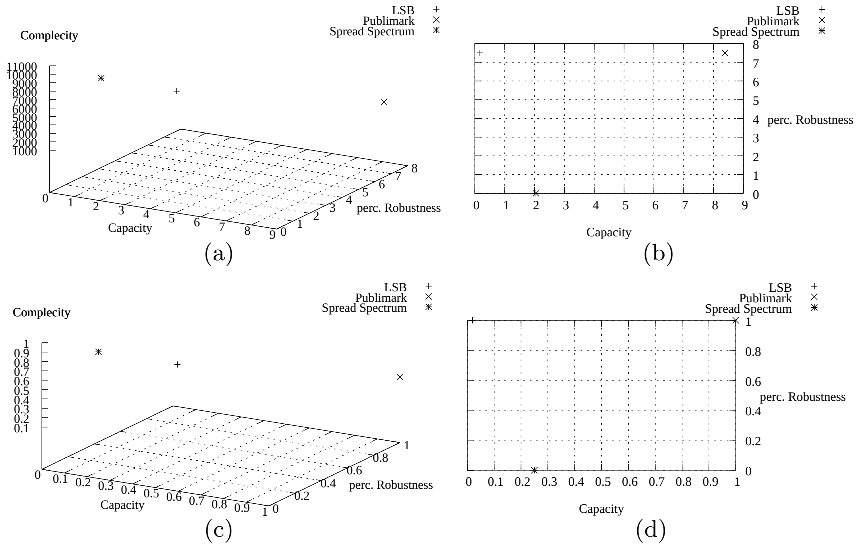


Fig. 5: Standard deviation of transparency results on a watermarking algorithm and different classes of audio material (taken from [21]).

5.4 Using entities for visualisation of dimensionality $n = 3$

The three-dimensional domain is, what Spence considers in [5] to be the "natural" domain of perception for a human audience. Therefore 3D data should be the ones most commonly chosen in presentation. The problem with this approach is that the possibilities of presentation on paper and normal computer displays are a priori limited to 2D information. Three dimensional data can be visualised naturally with appropriate hardware or by projecting them on a 2D plane. In many cases this leads to the question: Which axis should be the one which has to be scaled? Since it has to be assumed that this axis is not as precise readable as the other two, here the main characteristic with the least impact should be chosen. The information hiding paradigm concerned might decide which characteristic should be mapped on this axis (for steganography it might be robustness, while in a DWM scenario the transparency might be chosen).

3D scatter plot (E_3^P): For the 3D case of the scatter plot the result is very often projected on 2D presentation material. In this step the information presented by the 3rd dimensional component is either neglected or distorted. To prevent this techniques like colour-coding or the usage of the size of the marker glyph to indicate the value of the third component can be used.



(a) (b)

(c) (d)

Fig. 6: Visualisation of the embedding Complexity (in seconds), Capacity (in Byte per second) and Robustness (in percent) for three algorithms in 3D scatter plots and 2D projections.

Figures 6 (a) and (c) show 3D scatter plots (non-normalised and in an unit cube) based on figures taken from [17]. Figures 6 (b) and (d) use the technique of axial projection to generate better readable results from the 3D model. If this approach of using axial projections is applied consequently the result is called in [6] a scatter plot matrix.

Triangular representation taken from [20] (E_3^S): Exploiting the metaphor of the triangle (of Transparency, Capacity and Robustness) presented in section [1] for representation the of benchmarking results (like in [20]) leads to a complex, non-orthogonal representation of three different features in 2D. The proposed representation is shown in figure 7.

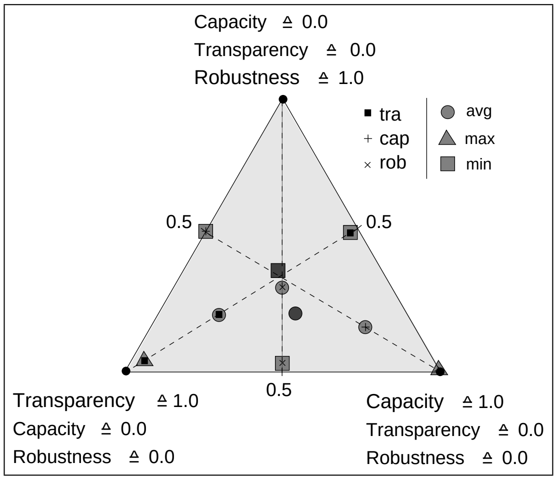


Fig. 7: Benchmarking results of the Complexity, Transparency and Robustness for different watermarking algorithms in a triangular representation (taken from [20]).

Due to the nature of this representation (three non-linear dependent values are mapped in 2D) a specific location within the triangle is not the unique representation of a single (normalised) value set for the three characteristics (if considering the distance to the corner-points as weights in the representation, a point in the centre would equally represent the sets $\{1, 1, 1\}$, $\{0.3, 0.3, 0.3\}$ and $\{0, 0, 0\}$). Other approaches advancing the idea of representation within the triangle, like exploiting area sizes or colour-coding, do not overcome the basic flaw in this representation: in many practical DWM-algorithms the three main characteristics might be dependant but not in a linear way, which means graphically that the result of placing them in a triangle will not result in a point.
Nevertheless the metaphor of the triangle is still a good approach to symbolise the fact that the three main features are dependent on each other.

5.5 Using entities for visualisation of dimensionality $n \geq 3$

Generally the number of linear independent vectors (required for an injective representation) is limited by the dimensionality of the representation system.

In 2D exist exactly two linear independent vectors, in 3D exactly three. Therefore the only way to adequately represent values of an n-dimensional functional nature it would require an n-dimensional space and an equally n-dimensional display method. If instead of functional correlations only states have to be visualised then for most n-dimensional data an adequate representation in 2D or 3D can be found. The problem here is to identify such "adequate" visualisation techniques for a well defined problem. For example the Hyperbox introduced by R. Spence in [5] gives a graphical example of a representation of 6D data in 2D. This representation form, which might be considered a very intuitive way of presentation, is not useful in the focus of this document since the introduced distortion of the data makes a perceptual comparison of results for different algorithms impossible. Another technique for the visualisation of a *n*-dimensional space, which was already introduced in section 5.4, is the scatter plot matrix. This concept of a projection onto all pairs of axes can easily be transferred from the 3D domain to any other dimensionality. Other representations to be introduced for example are the parallel coordinate plots and the Kiviatgraphs ([5], [6]). Both are variable in dimensionality.

Areas under a parallel coordinate plot (E_5^{mS}): The area under the curves in a parallel coordinate plot might be considered in some applications an adequate rating for the quality of an algorithm with regards to *n* characteristics. To use this measure in watermarking and steganography benchmarking is highly questionable since most often non-continuous values are projected and a different order of the features would result in a different area. Figure 8 displays such a parallel coordinate plot with five features for five selected algorithms. The problem in this figure is proposed by the fact that the robustness and capacity are presented by "bigger-is-better" metrics and the transparency and complexity by "lower-is-better" metrics. Nevertheless this presentation provides a good base for algorithm comparison with regards to the features identified.

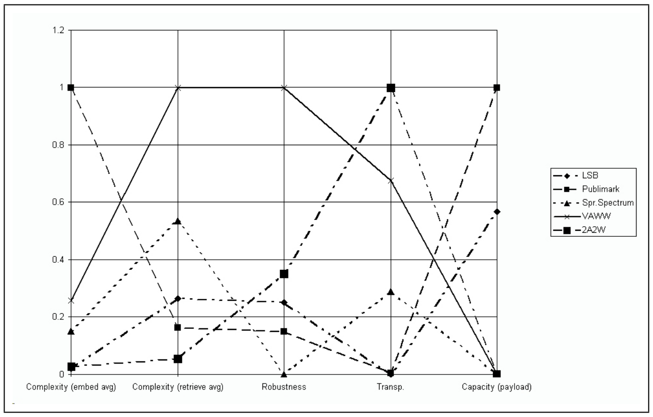


Fig. 8: Parallel coordinate plot displaying normalised benchmarking results of the Complexity (embedding and retrieval), Transparency and Robustness and Capacity for five selected algorithms (values taken from [17]).

Area(s) in a Kiviatgraph (E_5^S and E_5^{mS}): The Kiviatgraph is a presentation form very similar to the parallel coordinate plot. Here the same problems arise when considering the area within the graph as a measure for the performance of an algorithm. A simplified version in a star-shaped form is shown in image 9 (c).

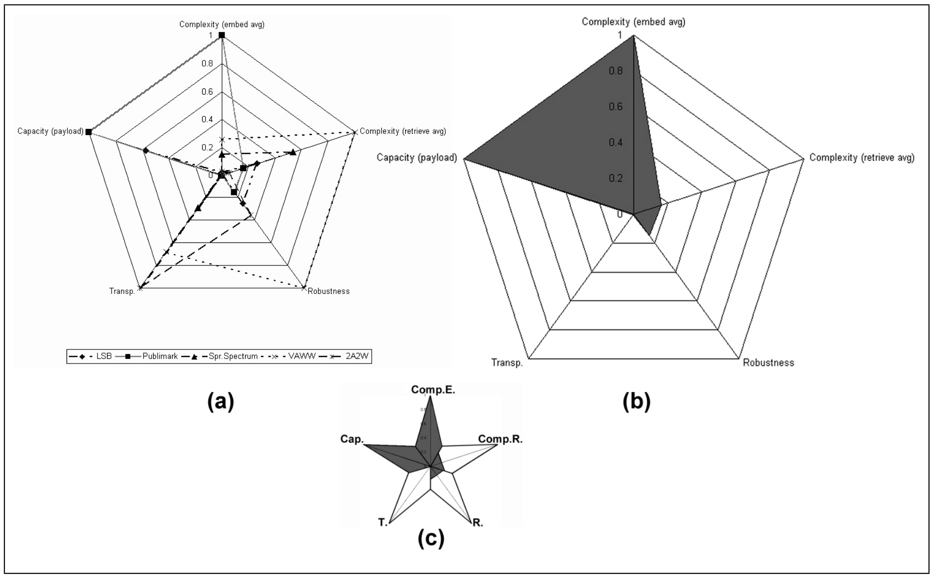


Fig. 9: Kiviat graph displaying normalised benchmarking results of the Complexity (embedding and retrieval), Transparency and Robustness and Capacity for: (a) five selected algorithms, (b) one selected algorithm, (c) simplified version of (b) (values taken from [17])

6 Summary/Conclusion

Apart from primary scientific goals like the development of universal, blind steganalysis tools, commercially exploitable watermarking algorithms or an universally accepted watermarking benchmarking approach, secondary problems like finding the appropriate representation for research results also have to be considered by the research community.

This paper basically contains an overview of features to be benchmarked in DWM and steganography as well as it provides an introduction of a number of visualisation techniques applicable to the results in this field. The goal of this paper was to facilitate the discussion about fitting representation approaches for fair benchmarking and the selection and use of techniques by non-experts. The author does not consider the introduced visualisation techniques as perfect matches for the visualisation problems at hand, but they very well show which problems can be encountered when trying to find fitting representations for complex sets of data.

Acknowledgements

I want to thank Prof. Jana Dittmann for her ideas regarding the visualisation problem discussed in this paper and Andreas Lang for providing material from his research and inspiring new ideas for creating visualisations.
The work about watermarking benchmarking described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT. The information in this document is provided as is, and no guarantee or warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

1. J. Fridrich: *Applications of Data Hiding in Digital Images*, Tutorial for the ISPACS 1998 conference in Melburne, Australia, 1998
2. A. Westfeld: *Steganographie für den Amateurfunk*;, S. 119-130 in Jana Dittmann (Hrsg.): Sicherheit 2006, Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 3. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 20.-22. Februar 2006 in Magdeburg, LNI Vol. P-77, Bonn, 2006
3. Christian Kraetzer, Jana Dittmann and Andreas Lang: *Transparency benchmarking on audio watermarks and steganography*, SPIE conference, at the Security, Steganography, and Watermarking of Multimedia Contents VIII, IS&T/SPIE Symposium on Electronic Imaging, 15-19th January, 2006, San Jose, USA, 2006
4. ICD-10, Chapter VII H53.5, *International Statistical Classification of Diseases and Related Health Problems, 10th Revision*, World Health Organization (WHO), 1999
5. Robert Spence: *Information Visualization*, Addison Wesley, ACM Press, ISBN 0-2001-59626-1, 2001
6. Heidrun Schumann, Wolfgang Müller: *Visualisierung - Grundlagen und allgemeine Methoden*, Springer Verlag, ISBN 3-540-64944-1, 2000
7. B.H. Mc Cormick, T.A. De Fanti, M.D. Brown: *Visualization in Scientific Computing*, Computer Graphics, Vol.21 Nr.6, P. 1-14, Nov. 1987
8. K.W. Brodlie, L.A. Carpenter, R.A. Earnshaw, J.R. Gallop, R.J. Hubbold, A.M. Mumford, C.D. Osland, P. Quarendon: *Scientific Visualization - Techniques and Applications*, Springer Verlag, ISBN 3-540-54565-4, 1992
9. Fabien A. P. Petitcolas, Ross J. Anderson, Markus G. Kuhn: *Attacks on copyright marking systems*, in David Aucsmith (Ed), Information Hiding, Second International Workshop, IH98, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239, 1998
10. Fabien A. P. Petitcolas: *Watermarking schemes evaluation*, I.E.E.E. Signal Processing, vol. 17, no. 5, pp. 58–64, September 2000
11. Andreas Lang, Jana Dittmann, Ryan Spring, Claus Vielhauer: *Audio watermark attacks: from single to profile attacks*, Proceedings of ACM Multimedia and Security Workshop 2005, pp. 39 - 50, ISBN 1-59593-032-9, New York, NY, USA, August 1-2, 2005
12. ITU-R Recomendation BS.1387, *Method for objective measurements of perceived audio quality*, ITU-R, 2001
13. Stefan Katzenbeisser and Fabien A.P. Petticolas: *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Publishers, ISBN 1580530354, 2000

14. Martin Kutter, Sviatoshlav Voloshynovskiy and Alexander Herrigel: *The Watermark Copy Attack*, Electronic Imaging 2000, Security and Watermarking of Multimedia Content II, Volume 3971, 2000
15. J. Dittmann, S. Katzenbeisser, C. Schallhart and H. Veith: *Ensuring Media Integrity on Third-Party Infrastructures*, Proceedings of the SEC2005, Chiba, Japan, May, 2005
16. Neil F. Johnson, Zoran Duric, Sushil Jajodia: *Information Hiding*, Kluwer Academic Publishers, 2001
17. Andreas Lang, Jana Dittmann: *Profiles for Evaluation - the Usage of Audio WET*, SPIE conference, at the Security, Steganography, and Watermarking of Multimedia Contents VIII, IS&T/SPIE Symposium on Electronic Imaging, 15-19th January, 2006, San Jose, USA, 2006
18. Hyung Cook Kim, Eugene T. Lin, Oriol Guitart, Edward J. Delp: *Further progress in watermark evaluation testbed (WET)*, Security, Steganography, and Watermarking of Multimedia Contents 2005: pp. 241-251, 2005
19. Christian Kraetzer, Jana Dittmann, Andreas Lang, Tobias Kuehne: *WLAN Steganography: A First Practical Review*, To appear in: Proceedings of the ACM Workshop on Multimedia and Security, Geneva, Swiss, September 26-17th, 2006
20. Andreas Lang, Jana Dittmann, David, Megías, Jordi Herrera-Joancomartí: *Practical Audio Watermarking Evaluation Tests and its Representation and Visualization in the Triangle of Robustness, Transparency and Capacity*, Submitted to the 2nd WaCha, Geneva, Swiss, 2006
21. Andreas Lang, Jana Dittmann: *Transparency and Complexity Benchmarking of Audio Watermarking Algorithms Issues*, to appear in Proceedings of ACM MM & Sec'06 Workshop, Geneva, Swiss, September 2006