Low-frequency Data Embedding for DFT-based Image Steganography

Petar Branislav Jelušić[1], Ante Poljičak[2], Davor Donevski[1], Tomislav Cigula[1]

[1]*Faculty of Graphic Arts, University of Zagreb, Croatia*
[2]*RIT Croatia, Zagreb, Croatia*
petar.branislav.jelusic@grf.unizg.hr, axp11cad@rit.edu, davor.donevski@grf.unizg.hr, tomislav.cigula@grf.unizg.hr

Keywords: DFT, image steganography, low-frequency data embedding, Gray Component Replacement

Abstract

The research in this paper is centered around examining the possibility of using low-frequency ranges in the frequency domain for data embedding in images. Specifically, different frequency ranges will be tested to determine how they affect image quality and detection at the decoder. The goal is to determine the optimal frequency range for data embedding. Finding that optimal frequency range will lead to higher detection rates while keeping image quality stable, or, contrary, provide higher image quality while maintaining the same detection rates. The proposed steganography method is suited for printing, but in this research, tests are conducted in the digital domain exclusively. The results show that the method is able to maintain consistent image quality regardless of the frequency range. Detection rates suggest that only the lowest frequency ranges should be avoided, while other frequency ranges can be used with similar success.

Introduction

This paper aims to determine the optimal frequency range for data embedding. Tests with various frequency ranges will be conducted to do so. Conclusions from these tests will help develop a more efficient digital image steganography method. The steganography method proposed in this paper is derived from the watermarking method proposed in [1]. The said watermarking method uses the Discrete Fourier Transform (DFT) to embed the watermark in the frequency domain of the cover image. The method is suited for printing, so it has to sustain aggressive attacks such as the print-scan process. Thus, stronger implementation is needed, resulting in highly visible embedding artifacts. The method uses Gray Component Replacement (GCR) to mask these artifacts. The capacity of the steganography method is achieved by using a block-based approach. The combination of DFT-based data embedding and GCR masking is proven to be a successful approach, as it produces a robust method while maintaining high imperceptibility levels [2], [3].

Approach

The DFT-based watermarking method used to develop the proposed steganography method uses medium-frequency bands for watermark embedding. Similarly, most frequency-based watermarking and steganography methods use medium frequency bands for embedding [4]–[6]. The reasoning behind it is simple; embedding in low-frequency bands results in high robustness but produces highly visible artifacts. On the other hand, high-frequency band embedding does not produce as many visible artifacts but provides less robustness. Medium-frequency bands provide a balance of those two extremes and are thus most often used. Keeping in mind that the proposed steganography method is suited for printing, robustness is of the highest priority. With the aforementioned effects of using different frequency bands for embedding in mind, it would be beneficial for this method to try and use low-frequency bands for embedding. The main downside of using these bands is the occurrence of visible artifacts. However, previous tests have shown that the GCR algorithm can mask most artifacts effectively. Best to the authors' knowledge, state-of-the-art research does not include DFT-based techniques that use low-frequency data embedding, so any conclusions and insights should be considered novel.

Data Embedding and Decoding

As stated earlier, the proposed steganography method uses the DFT to transform the image from the spatial domain to the frequency domain. Then, the image is divided into image blocks to achieve its final capacity. The embedding is done in each image block separately. A circular-shaped vector is used at the encoder to additively modify coefficients of the image's magnitude. A seed is used for creating a pseudo-random sequence of values. This is needed for vector generation, as the decoder will later use the same pseudo-random sequence for detecting the said

vector. By adjusting the radius of the vector, different frequency ranges are modified (Fig. 2). The decoder has to have a priori knowledge of both the radius used for embedding and the seed used for vector generation, to try and detect the modified coefficients. The correlation between the generated vector and the vector detected at the decoder is measured using the Pearson product-moment correlation coefficient. Finally, the decoder uses the Grubbs' outlier test to *decide* whether the embedded data is present in the image block. Using Grubbs' test for detecting outliers is a well-established technique in recent literature [7]–[9].

Masking

Masking methods are used to hide visible artifacts introduced by data embedding. In this research, the masking method is based on gray component replacement (GCR). In four-color printing, colors resulting from combinations of all three chromatic inks (C-cyan, M-magenta, and Y-yellow) can be reproduced by different combinations of all four inks. That is, gray component in the mix of three chromatic inks can be replaced with black ink (K). The device (or colorant) space is referred to as CMYK space. Note that four-color channels make it four-dimensional. For each point in CMYK space, there is a corresponding point in the three-dimensional CIE L*a*b* color space. While CMYK space is device-dependent, i.e., same CMYK values result in a different color appearance on different devices, CIE L*a*b* space is device independent, i.e., describes color as perceived by humans. This research is conducted on CMYK digital images intended for printing. Data is embedded in the K channel only, which introduces visible artifacts if other channels (C, M, and Y) are left intact. Masking is performed using GCR. The C, M, and Y channels are adjusted such that in the masked image, the visual appearance (CIE L*a*b* values) of the original image is preserved while the data is stored in the K channel. The color transformation model used to perform GCR is detailed in [10]. The visual representation of the method is given in Fig. 1.

Figure 1. Original image (left), the K channel of the image with embedded data (middle), and the CMYK image with embedded data (right)

Experimental

All tests are done in the digital domain exclusively. A dataset of 1000 CMYK images was used. For each experiment, five different frequency ranges are used for embedding: *H (r = 0.3), MH (r = 0.25), M (r = 0.20), LM (r = 0.15),* and *L (r = 0.10)*. For purposes of this research, the implementation strength γ is kept at a fixed

value of $\gamma = 20$ for all tests. In Fig. 2., the frequency domain of an image is shown with all five radii used in the tests to illustrate how modifying the radius impacts different frequency ranges.

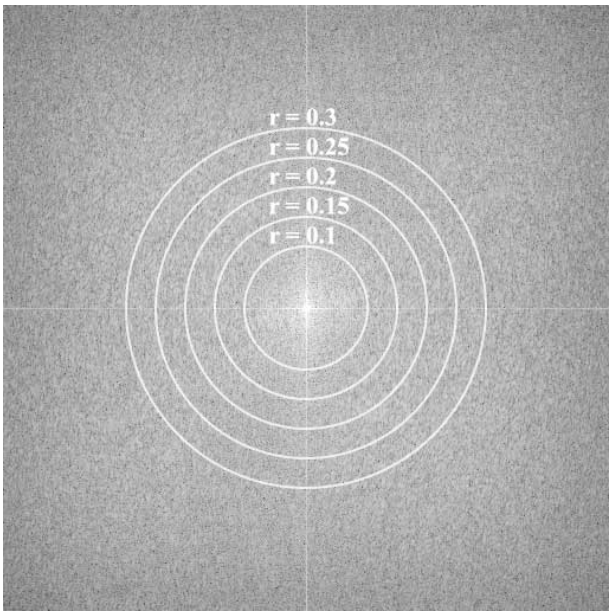

Figure 2. Frequency ranges used in tests, represented as different radii within the frequency domain

Images are 1024x1024 pixels in dimension, and each image is divided into four square blocks of 512x512 pixels in dimension. A stego message is embedded in each block separately. The stego message consists of three total bits of data, while *image block 4* is intentionally left without embedded data. The experimental part is organized as follows. Tests are conducted to determine the robustness, using detection rate *Dr* as the metric of choice. In Fig. 3. and Fig. 4., image quality tests are presented, with Structural Similarity Index Measure (SSIM) and Peak Signal to Noise Ratio (PSNR) metrics used. Mathematical definitions of both metrics can be found in [11].

Results

Detection rates results are displayed in Table 1. The results show that all tested frequency ranges produce high detection rates. *M* and *LM* frequency ranges produce the most consistent detection rates, regardless of image block. It can be concluded that all frequency ranges can be used successfully, with the exception of *L*.

	H	MH	M	LM	L
Image Block 1	**99.3**	94.7	98.6	95.9	91.3
Image Block 2	91.4	91.9	97.4	**98.4**	92.3
Image Block 3	**99.9**	99.2	99.8	99.4	97.4
Image Block 4	**97.4**	96	95.9	97.0	89.5

Table 1. Detection rates for each image block and each frequency range

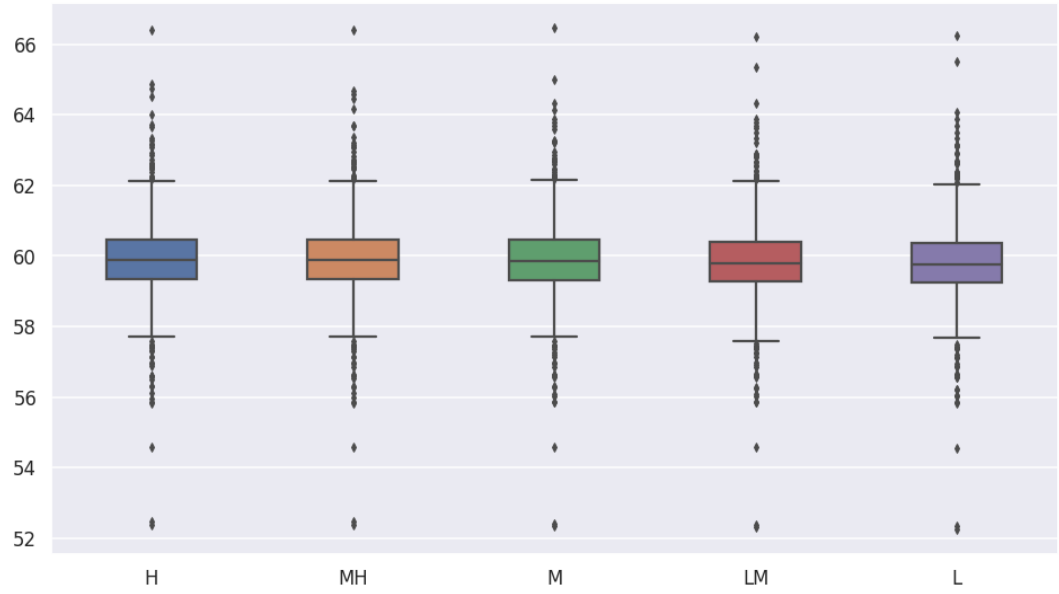

Figure 3. PSNR values (ordinate) when comparing original images and images with embedded data. Different frequency ranges are represented on the abscissa.

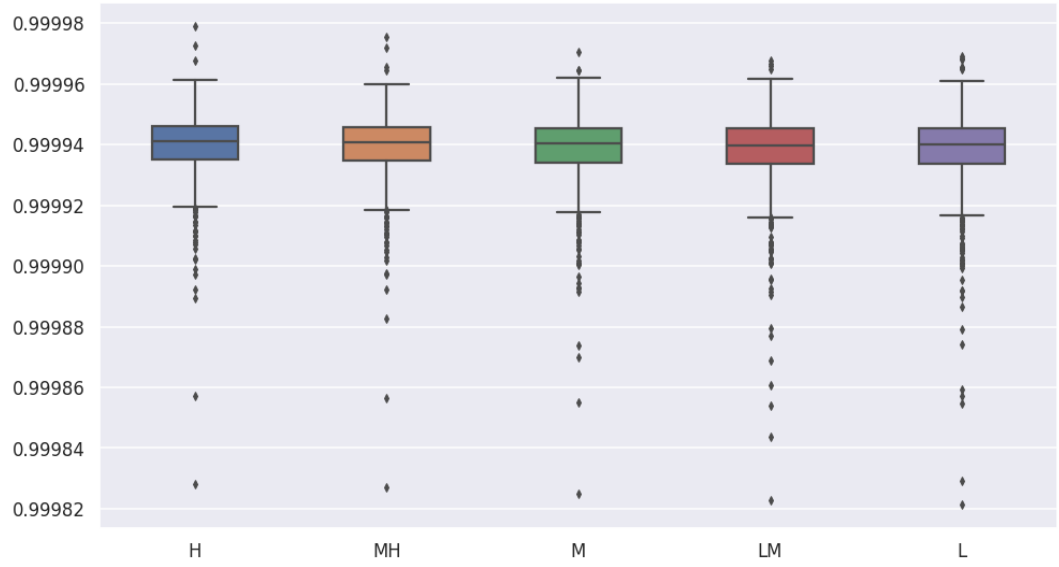

Figure 4. SSIM (ordinate) values when comparing original images and images with embedded data. Different frequency ranges are represented on the abscissa.

Fig. 3 and Fig 4. display results in regard to image quality. Both PSNR and SSIM values clearly show that the method is able to maintain consistent image quality, regardless of the frequency range. This is in line with results from previous tests [11], and a direct result of using GCR for masking. Ideally, GCR preserves both the color appearance in terms of CIE L*a*b* values and the data embedded in CMYK image's K channel. However, high impact factors can lead to large changes in K, such that it gets too small or too large to have a C, M and Y solution for a given CIE L*a*b* color. For example, forcing large K (black ink) value for some light CIE L*a*b* color will have no solution because even if C, M, and Y were removed completely, K alone would result in a color darker than the aimed color. In such cases, the masking method in this research finds CMYK solution to aimed CIE L*a*b* color with K value closest to that imposed by the data embedding. That is, where necessary, implementation strength is sacrificed in favor of colorimetric accuracy. This explains why image quality is preserved regardless of the frequency range.

Conclusion and future research

The results gathered in the presented research provide proof that low-frequency ranges can indeed be used for data embedding within the proposed steganography method. As the method is suited for printing and will be used in the print domain, any improvement of the method's robustness is welcome. Adjusting the frequency ranges towards lower bands will provide just that. Future research will be based on more precise vector lengths and radii adjustments. By fine-tuning these parameters, it is possible the method will yield even better results.

Acknowledgment

This research is a part of the projects DOK-2018-09-7543 and UIP-2017-05-4081, Development of the model for production efficiency increase and functionality of packaging, supported by Croatian Science Foundation.

References

[1] A. Poljicak, D. Donevski, P. B. Jelusic, T. Tomasegovic, and T. Cigula, "Analysis of the GCR communication channel for image steganography," *Proc. Elmar - Int. Symp. Electron. Mar.*, vol. 2019-Septe, no. September, pp. 65–68, 2019, doi: 10.1109/ELMAR.2019.8918869.

[2] D. Donevski, A. Poljicak, and M. S. Kurecic, "Colorimetrically accurate gray component replacement using the additive model," *J. Vis. Commun. Image Represent.*, vol. 44, pp. 40–49, 2017, doi: 10.1016/j.jvcir.2017.01.018.

[3] A. Poljicak, D. Donevski, and L. Mandic, "Applicability of the GCR masking in an image watermarking method," *Proc. Elmar - Int. Symp. Electron. Mar.*, vol. 2017-Septe, no. September, pp. 215–218, 2017, doi: 10.23919/ELMAR.2017.8124471.

[4] W. Y. Chen, "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation," *Appl. Math. Comput.*, vol. 185, no. 1, pp. 432–448, 2007, doi: 10.1016/j.amc.2006.07.041.

[5] S. Pereira and T. Pun, "Fast robust template matching for affine resistant image watermarks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1768, no. 6, pp. 199–210, 2000, doi: 10.1007/10719724_15.

[6] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "Robust watermarking method in DFT domain for effective management of medical imaging," *Signal, Image Video Process.*, vol. 9, no. 5, pp. 1163–1178, 2015, doi: 10.1007/s11760-013-0555-x.

[7] C. Wang, J. Caja, and E. Gómez, "Comparison of methods for outlier identification in surface characterization," *Meas. J. Int. Meas. Confed.*, vol. 117, no. November 2017, pp. 312–325, 2018, doi: 10.1016/j.measurement.2017.12.015.

[8] M. Urvoy, D. Goudia, and F. Autrusseau, "Perceptual DFT Watermarking With Improved Detection and Robustness to Geometrical Distortions," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 7, pp. 1108–1119, Jul. 2014, doi: 10.1109/TIFS.2014.2322497.

[9] M. Urvoy and F. Autrusseau, "Application of grubbs' test for outliers to the detection of watermarks," *IH MMSec 2014 - Proc. 2014 ACM Inf. Hiding Multimed. Secur. Work.*, no. 1000, pp. 49–60, 2014, doi: 10.1145/2600918.2600931.

[10] D. Donevski, A. Poljicak, M. Prsa, and T. Hudika, "Adjustable color transformation model," *Proc. Elmar - Int. Symp. Electron. Mar.*, vol. 2019-Septe, no. September, pp. 69–72, 2019, doi: 10.1109/ELMAR.2019.8918906.

[11] P. B. Jelusic, A. Poljicak, D. Donevski, and T. Cigula, “Analysis of the DFT-based Watermarking Method for Image Steganography,” pp. 1–6, 2020.

Author biography

Petar Branislav Jelušić studied at the Faculty of Graphic Arts in Zagreb, where he obtained his Master’s degree in 2017. After a few years of working as a freelance web and graphic designer, he joined the Faculty of Graphic Arts once again, this time as a Research Assistant and PhD student. His interests include image processing, data visualization, and neural networks.