
Proceedings Paper:
Al-Khafaji, H. and Abhayaratne, C. (2017) Graph Spectral Domain Watermarking for Unstructured Data from Sensor Networks. In: Digital Signal Processing (DSP), 2017 22nd International Conference on. Digital Signal Processing (DSP), 2017 22nd International Conference on, 23-25 Aug 2017, London, UK. IEEE. ISSN: 1546-1874.

https://doi.org/10.1109/ICDSP.2017.8096148

Graph Spectral Domain Watermarking for Unstructured Data from Sensor Networks

Hiba Al-khafaji* , Charith Abhayaratne†
Department of Electronic and Electrical Engineering
The University of Sheffield
Sheffield, S1 3JD, United Kingdom
Email: *h.alkhafaji@sheffield.ac.uk, †c.abhayaratne@sheffield.ac.uk

***Abstract*—The modern applications like social networks and sensors networks are increasingly used in the recent years. These applications can be represented as a weighted graph using irregular structure. Unfortunately, we cannot apply the techniques of the traditional signal processing on those graphs. In this paper, graph spread spectrum watermarking is proposed for networked sensor data authentication. Firstly, the graph spectrum is computed based on the eigenvector decomposition of the graph Laplacian. Then, graph Fourier coefficients are obtained by projecting the graph signals onto the basis functions which are the eigenvectors of the graph Laplacian. Finally, the watermark bits are embedded in the graph spectral coefficients using a watermark strength parameter varied according to the eigenvector number. We have considered two scenarios: blind and non-blind watermarking. The experimental results show that the proposed methods are robust, high capacity and result in low distortion in data. The proposed algorithms are robust to many types of attacks: noise, data modification, data deletion, rounding and down-sampling.**

I. Introduction

Recent years have seen a growth of using various sensors to sense and measure various data. As these sensors are located at arbitrary locations, without following a Cartesian grid, the data recorded using a network of sensors can be represented in a graph, with vertices (nodes) representing the locations of sensors. The connectivity between nodes can be defined by considering the relationship among sensors. In this paper we are concerned with protection and authentication of such data captured via a network of sensors. However, there have been limited works on this aspect of addressing irregular graph structures.The most common approaches for protecting graph-type are: adding extra edges between a set of pairs of nodes, which have different colours based on the binary message; Maximal Independent Set (MIS) based on choosing one or more set(s) from the original graph such that the set is independent [1]; inserting new nodes to the original graph and connect them depending on the binary message [2] and hiding a sub-graph which is generated from a watermark [3]. Since these works are based on vertex domain, they are not robust to data processing, noise removal or geometrical attacks, such as, adding new nodes, edges or sub-graphs. In addition, these methods are not secure, if the original graph is available the watermark can be detected by comparing the two graph topologies. Finally, the embedding capacity is very small due to the embedding process is depended on the graph topology, not the correlation of its data.

On the other hand, spread spectrum watermarking has proven to be very successful in image protection, mainly due to advances in signal transforms, such as, the Discrete Cosine Transform (DCT) and the Discrete Wavelet Transform (DWT) [4].

However, such transforms are not applicable for graph data, where the nodes are spread at arbitrary locations, as opposed to uniform sampling grid in images and other signals. In this paper, we propose a new spread spectrum watermarking methodology for graph data by exploiting the spectral decomposition of graph data. In this work, we exploit the recent advances in graph signal processing on graph spectral decomposition of the graph Laplacian matrix, which captures the connectivity of the nodes. [5], [6]. The resulting basis functions are stable and invariant to the geometric changes. Also, the embedding algorithms are dependent on some parameters which can be considered as a secret key, leading to more secured watermarking algorithms. Moreover, the embedding capacity is bigger than the existing methods because most of the graph nodes are used to hide the watermark on the spectral domain. The main contributions of the proposed work are:

1) The first work on graph spread spectrum watermark hiding.
2) Propose novel blind and non-blind watermarking for networked sensor data.
3) Using unfixed (graph connectivity adapted) basis functions for watermark hiding.

The rest of the paper is organized as follows: Section II provides a brief introduction to the related work. Section III presents the proposed method, followed by the results and discussions are presented in section IV. Finally, the conclusions are presented in section V.

II. Related Work

This section includes two parts: watermarking on sensor networks and watermarking on graph domain for mesh data.

A. Watermarking of sensor data

Watermarking is a lightweight approach which is used to provide protection and authentication for sensor data. The first watermarking system in sensor networks was proposed

by Fang et al. [7] for copyright ownership by hiding the authorship signatures in the sensor data during network processing. However, it can be used with limited applications. Similar work was suggested by Koushanfar et al. [8] to hide the watermark during the data acquisition process, it is robust against signature removal and desynchronization. Sion et al. [9] proposed watermarking algorithm based on least significant bits to protect the data stream owners and the authorized users. Similar works were proposed by Kamel et al. [10].

B. Watermarking on graph domain

Most of the watermarking methods on a graph are related to mesh. The main idea is to hide the watermark bits on the mesh coordinates or mesh coefficients. In mesh data watermarking, the watermark has been embedded on the mesh coordinates have been projected on to the eigenvectors of Laplacian matrix of the mesh connectivities [11]. However, it requires a high computational cost ($O(N^3)$) and it is sensitive to any modification in the connectivity of the mesh. In another work [12], a blind hiding method has been proposed for mesh data, by reorganising these projected coordinates. This method causes a visual distortion of the mesh (graph topology) and has a limited robustness. Similar works based on the manifold harmonics in [13], [14] for meshes. These methods used eigen decomposition of Lapalacian matrix of mesh graphs and applied them onto the node coordinates, as opposed to considering the spread spectrum hiding methods for the data recorded at these mesh nodes.

III. THE PROPOSED GRAPH SPREAD SPECTRUM WATERMARKING

The graph spectral theory is an important aspect of the graph theory, which is related with the eigenvalues and eigenvectors. Eigenvalues and eigenvectors are the most significant invariant vectors of the graph spectral decomposition. The main goal of the spectral graph theory is to conclude the structure and principal attributes of the graph using its spectrum. Our proposed watermarking framework starts with the graph spectral decomposition, which we call the Graph Fourier Transform (GFT). Then we analyses the spectral coefficients to propose a new embedding process, followed by the inverse GFT to reconstruct the watermarked graph data. We consider two watermarking scenarios: blind and non-blind. The watermark extraction algorithm starts with the GFT followed by the extraction process and authentication. The non-blind scenario uses the original graph for extracting the watermark. The embedding and extraction framework is shown in Fig. 1.

A. Graph Preliminaries

Let G be undirected graph without self-loops and multiple links between nodes. It can be represented as $G = (V, E, W)$, where V represents graph nodes with N length, $|V| = N < \infty$, E represents the edges, $i.e.$, the connection between the nodes and W is a weight matrix, which gives the weights for each node. The adjacency matrix A of a graph G is defined as:

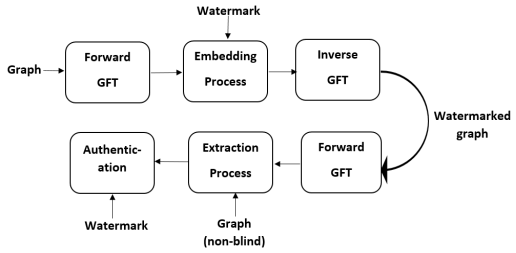

Fig. 1: The block diagram of the proposed watermarking framework.

$$A = \begin{cases} W_{i,j}, \text{if} \quad there\ is\ an\ edge\ between\ v_i\ and\ v_j, \\ 0 \quad \text{, otherwise .} \end{cases} \tag{1}$$

Graph signals can be represented as a vector $f = [f(1), f(2), ..., f(N)]$, such as $f : V \rightarrow R$. The non-normalized Laplacian L can be given as:

$$L = D - A, \tag{2}$$

where D is a diagonal matrix of vertex degree, which represents the sum of weights of all links connected to a given vertex. The Laplacian matrix is symmetric and it has real and non-negative eigenvalues λ_ℓ with associated real and orthonormal eigenvectors u_ℓ. The decomposition of eigenvalue of non-normalized Laplacian matrix such that

$$L = U\Lambda U^t = \sum_{i=1}^{N} \lambda_i u_i u_i^t \tag{3}$$

where $u_1, u_2, ..., u_N$ are the eigenvectors corresponding to eigenvalues $\{0 \leq \lambda_1 \leq \lambda_2 ... \leq \lambda_N\}$.

B. Graph Fourier Transform

The classical Fourier transform on R can be given as:

$$F(w) =< e^{iwx}, f >= \int_R f(x) e^{-iwx} dx. \tag{4}$$

It can be expanded in terms of eigenvectors of the Laplacian graph by projecting the graph signal f onto the eigenvectors u in R^2 which are the basis functions. The Laplacian eigenvectors give interpretation similar to classical Fourier transform in terms of providing a harmonic analysis of graph signals. The classical Fourier has fixed basis functions, while the Fourier graph has unfixed basis functions, which depend on the connectivity between the graph nodes and the Graph Laplacian type. Fig. 2 shows the basis functions of an example path graph with 8 nodes. It is important to mention that the first eigenvector is a constant vector and depends on the number of graph nodes, which is equal to $1/\sqrt{N}$ for all graph types, which is similar to the DC component of the conventional transforms. The Graph Fourier Transform (GFT)

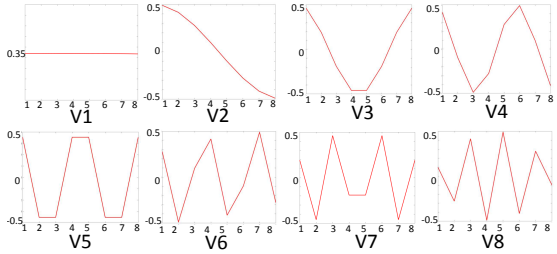

Fig. 2: The basis functions of path graph.

can be computed as in the following equation:

$$\hat{f}(\lambda_\ell) = \langle u_\ell, f \rangle = \sum_{i=1}^{N} f(i) u_\ell(i). \tag{5}$$

The inverse Graph Fourier Transform can be defined as the following:

$$f(i) = \sum_{\ell=0}^{N-1} \hat{f}(\lambda_\ell) u_\ell^t(i). \tag{6}$$

The Graph Fourier transform satisfies the Parseval's theorem, which means the sum of the square graph signals is equal to the sum of the square graph Fourier coefficients as follows:

$$||f||_\ell^2 = \sum_{i=1}^{N} |f(i)|^2 = \sum_{\ell=0}^{N-1} |\hat{f}(\lambda_\ell)|^2 = ||\hat{f}||_\ell^2 \tag{7}$$

Most of the energies are in the first half of the coefficients $(1 : N/2)$ which represents the low frequency corresponding to smaller eigenvalues while the high frequency coefficients are associated to the larger eigenvalues [5].

C. Non-Blind Watermarking

Magnitude based multiplicative watermarking widely forms as the basis for non-blind watermarking [15] [16]. We embed the watermark in to the graph Fourier coefficients $\hat{f}$ as follows:

$$\hat{f}_w = \hat{f}(1 + w\alpha), \tag{8}$$

where α is the watermark strength and w is the watermark value computed as $w = bM$, where the binary watermark bit, $b = \{0, 1\}$ and M is the length of watermark sequence. In order to provide a balance between the robustness and error distortion in the spectral coefficients, α can be adapted to the increasing frequency. Our experiments suggest by choosing $\alpha_l \propto l$, where l is the eigenvector number is a good approach to achieve this balance. For the simulations shown in this paper, we group, eigenvalues into 3 groups: low, mid, and high frequencies. Each frequency group uses a different α value as $\alpha_{low} < \alpha_{mid} < \alpha_{high}$, respectively for low, mid and high frequencies.

In the extraction process, the watermark bits $\hat{b}$ extracted as shown as follows:

$$\hat{b} = \begin{cases} 1, & \text{if } \hat{w} \geq M/2, \\ 0, & \text{if } \hat{w} < M/2, \end{cases} \tag{9}$$

where

$$\hat{w} = \frac{\hat{f}_w/\hat{f} - 1}{\alpha}. \tag{10}$$

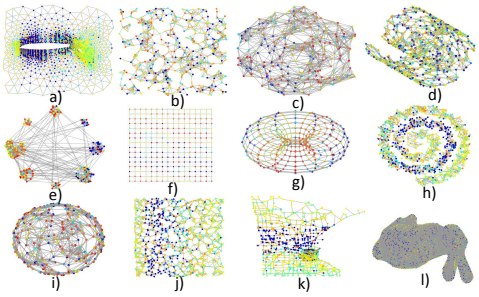

Fig. 3: 12 types of graphs. a: Air foil. b: David sensor network. c: Cube. d: Swiss-roll. e: Community. f: 2D-grid. g: Torus. h: Spiral. i: Sphere. j: Sensor. k: Minnesota. l: Bunny.

D. Blind Watermarking

The graph Fourier coefficients $\hat{f}$ are modified as given in the following equation:

$$\hat{f_w} = \hat{f} + c, \tag{11}$$

where $\hat{f_w}$ is the watermarked graph Fourier coefficient and c is the watermark parameter which is computed as follows:

$$c = \begin{cases} \beta/2 - s, & \text{if } b = 0 \\ 3\beta/2 - s, & \text{if } b = 1 \end{cases}, \quad where \ \beta > 0 \tag{12}$$

where β is a watermark strength parameter and $s = mode(\hat{f}, 2\beta)$ [17]. The watermark strength parameter plays an important role to balance the watermarking robustness and distortion. In this case also, for the simulations shown in this paper, we group, eigenvalues into 3 groups: low, mid, and high frequencies and $\beta_{low} < \beta_{mid} < \beta_{high}$, respectively for low, mid and high frequencies.

In the extraction process, the watermark is extracted from the watermarked coefficients as shown in the following equation:

$$\hat{b} = \begin{cases} 0, & \text{if } 0 \leq p \leq \beta \\ 1, & \text{if } \beta \leq p \leq 2\beta \end{cases}, \tag{13}$$

where $p = mode(\hat{f_w}, 2\beta)$.

E. Authentication Process

The extracted watermark is authenticated by comparing the Hamming Distance(D).

IV. Results and Discussion

The methods are tested on a set of 12 types of graphs (as shown in Fig. 3) and 2 watermark types: set of 5 binary logos (as shown in Fig. 4) and pseudo-random binary sequences. The performance of watermarking is investigated in terms of error distortion, robustness and capacity.

A. Experimental Results

Comprehensive experiments are performed to evaluate the robustness and error distortion of the proposed methods. The experiments are divided into two parts: non-blind and blind experiments. Fig. 5 shows Sensor and Airfoil graphs before and after embedding the watermark using the proposed methods.

Fig. 4: 5 binary watermark logos. a: ieee. b: logo-inverse. c: medicine. d: logo-university. e: arrow.

TABLE I: PSNR of various graphs (non-blind)

Graph type	No.watermark bits	PSNR (dB)
Community(256 nodes)	125	41.54
Cube(300 nodes)	150	44.47
Sphere(300 nodes)	150	40.29
Torus (320)	160	42.47
David-sensor(500 nodes)	250	41.76
Bunny(2503 nodes)	1250	41.02
Minnesota(2642 nodes)	1300	46.78
Sensor(3240 nodes)	1600	42.48
Spiral(3240 nodes)	1600	41.39
Swiss-roll(3200 nodes)	1600	41.15
2dgrid(3249 nodes)	1600	47.57
Air foil(4253)	2000	47.94

A.1. Non-blind Watermarking Experiments

To investigate the effect of many factors on the proposed method performance such as: increasing the number of graph nodes, graph type, watermark type, dynamic range of graph signals and various attacks, the sensor graph with 3240 nodes and dynamic range $[1, 2^8]$ is used to hide the binary watermark bits. For all experiments, the watermark strengths $\alpha_{low} = 0$, $\alpha_{mid} = 0.01$ and $\alpha_{high} = 0.1$ were used. Table I shows the embedding error distortion for pseudo-random binary sequence with different number of bits is embedded in different graphs. It can be seen that the graph type has affect on the watermarking performance in spite of using the same number of nodes. For example, cube has the same number of nodes as the sphere but it has a higher PSNR value. This is mainly due to the different connectivities present in various graphs.

Another factor is dynamic range of the graph signals. The sensor graph with N nodes and 3 dynamic ranges: $[1, 2^4]$,$[1, 2^8]$ and $[1, 2^{12}]$ are used to hide the pseudo random binary sequence with length $M = N/2$. The results (Table II) show that the best performance of the proposed method when the graph signals are in dynamic range $[1, 2^{12}]$. This is mainly due to the modified value due to embedded watermark in low dynamic range data is large compared to the upper value of the dynamic range.

Also, to show the effect of using different types of binary watermark logos, 5 binary logos are embedded in the Sensor graph with dynamic range of graph signals $[1, 2^8]$. Table III shows the proposed method yields the best performance when the logo-Inverse is used because it has more zeros which means the modified coefficients are less than the other logos. Also, the watermark type affect the watermarking performance, for example, if the watermark is pseudo random binary sequence, the better performance is achieved when the sequence has more zeros compared to other watermark sequences.

TABLE II: PSNR of watermarked Sensor graph using 3 dynamic ranges of graph signals (non-blind)

Dynamic range	PSNR(dB)
$[1, 2^4]$	48.29
$[1, 2^8]$	51.40
$[1, 2^{12}]$	57.59

TABLE III: PSNR of sensor graph using different watermark logos (non-blind)

No.Sensor nodes	Binary logo	PSNR (dB)
3240	ieee(40×40)	42.22
10000	arrow(70×74)	40.77
10000	medicine(77×76)	41.21
8100	logo-university(64×64)	41.23
8100	logo-inverse(64×64)	43.88

TABLE IV: PSNR of watermarked Air foil using different frequencies (non-blind)

Frequency bands	PSNR(dB)
Low frequency coefficients	42.89
Middle frequency coefficients	44.41
High frequency coefficients	47.14

TABLE V: PSNR of watermarked sensor using different watermark strength parameter β (blind)

β	PSNR(dB)
1	53.58
2	47.70
3	44.10
4	41.60

The most important factor is the embedding frequency band which is used to hide the watermark bits. Table IV shows the best performance of watermarking when the high frequency coefficients are used because the distortion in these coefficients is low compared to the low frequency band coefficients, due to most of the graph energy is in the low frequency components.

A.2. Blind Watermarking Experiments

To investigate the effect of the watermark strength parameter on the performance of the watermarking method. The binary watermark logo $ieee$ is embedded in the middle and high frequency coefficients of the sensor with (3240) nodes and dynamic range signals $[1, 2^8]$ using various watermark strength values β. As shown in Table V, the proposed method yields the best performance when $\beta = 1$. Therefore, for all experiments, the watermark strengths $\beta_{low} = 0$, $\beta_{mid} = 1$ and $\beta_{high} = 2$.

Another experiment is to show the effect of using different dynamic ranges of graph signals on the performance of the watermarking. Table VI shows that the proposed method

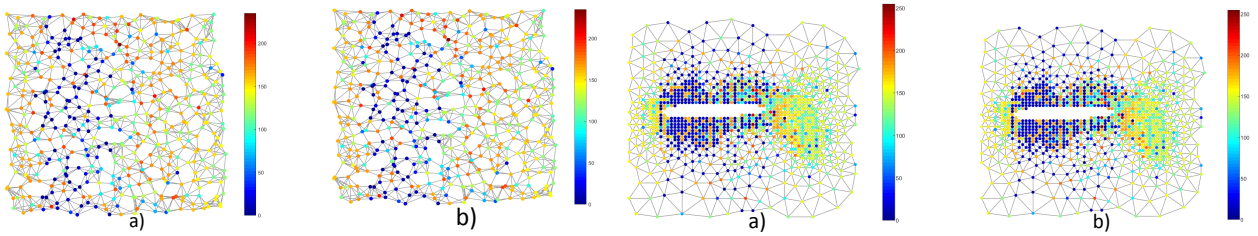

Fig. 5: Sensor and Airfoil graphs after applied the proposed method. a: original graphs. b: watermarked graphs.

TABLE VI: PSNR of Sensor graph using 3 dynamic ranges of graph signals (blind)

Dynamic range	PSNR(dB)
$[1, 2^4]$	27.78
$[1, 2^8]$	52.80
$[1, 2^{12}]$	76.63

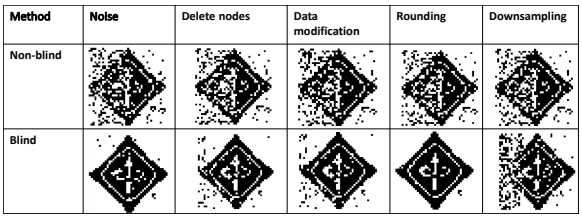

Fig. 6: Extracted watermark after various attacks.

achieves the best performance when the graph signals are in the range $[1, 2^{12}]$.

To evaluate the robustness of the proposed methods, various attacks, such as, adding random noise with $\sigma = 0.2$, rounding, data modification, nodes deletion and down-sampling were considered. Fig.6 shows the watermark after various attacks. Blind algorithm shows more robustness to noise and rounding compared to the non-blind algorithm

V. Conclusions

In this paper, we have proposed graph spread spectrum watermarking for authentication of networked sensor data. The proposed method represents the sensor data as a graph and explores its connectivity to derive the Laplacian matrix whose eigenvectors are used as the transform basis to define the graph Fourier transform. Then the properties of these coefficients are explored to hide the watermark. We have considered both blind and non-blind watermarking scenarios. In order to balance the distortion and robustness performance, we have varied the watermarking strength parameter according to the increasing eigenvector number. We have evaluated the embedding performance for various graph data, comprising of graph structures, number of nodes, dynamic ranges of the data, various watermark types and the watermark strength parameters. The results show that the watermark can be survived after various attacks: noise, data modification, data deletion, rounding and down-sampling.

References

[1] G. Qu and M. Potkonjak, "Analysis of watermarking techniques for graph coloring problem," in *Proc. of the int. conf. on Computer-aided design*, 1998, pp. 190–193.

[2] A. Saha, D. Bhaumik, and S. Pathak, "Signature hiding and recovery in a graph coloring solutions using modified genetic algorithm," in *Int. Conf. on Computer and Inf. Technology (ICCIT)*, 2011, pp. 50–55.

[3] X. Zhao, Q. Liu, H. Zheng, and B. Y Zhao, "Towards graph watermarks," in *Proc. of the Conf. on Online Social Networks*, 2015, pp. 101–112.

[4] D. Bhowmik and C. Abhayaratne, "Quality scalability aware watermarking for visual content," *IEEE Transactions on Image Processing*, vol. 25, no. 11, pp. 5158–5172, 2016.

[5] D. I. Shuman, S. K. Narang, P. Frossard, A. Ortega, and P. Vandergheynst, "The emerging field of signal processing on graphs: Extending high-dimensional data analysis to networks and other irregular domains," *IEEE Signal Processing Magazine*, vol. 30, no. 3, pp. 83–98, 2013.

[6] D. K. Hammond, P. Vandergheynst, and R. Gribonval, "Wavelets on graphs via spectral graph theory," *Applied and Computational Harmonic Analysis*, vol. 30, no. 2, pp. 129–150, 2011.

[7] J. Fang and M. Potkonjak, "Real-time watermarking techniques for sensor networks," in *Electronic Imaging*, 2003, pp. 391–402.

[8] F. Koushanfar and M. Potkonjak, "Watermarking techniques for sensor networks: foundation and applications," *Security in Sensor Networks*, 2006.

[9] R. Sion, M. Atallah, and S. Prabhakar, "Resilient rights protection for sensor streams," in *Proc. of int. conf. on Very large data bases*, 2004, vol. 30, pp. 732–743.

[10] I. Kamel and H. Juma, "A lightweight data integrity scheme for sensor networks," *Sensors*, vol. 11, no. 4, pp. 4118–4136, 2011.

[11] R. Ohbuchi, S. Takahashi, T. Miyazawa, and A. Mukaiyama, "Watermarking 3D polygonal meshes in the mesh spectral domain," in *Graphics interface*, 2001, vol. 2001, pp. 9–17.

[12] F. Cayre and B. Macq, "Data hiding on 3-D triangle meshes," *IEEE Trans. on signal Processing*, vol. 51, no. 4, pp. 939–949, 2003.

[13] Y. Liu, B. Prabhakaran, and X. Guo, "A robust spectral approach for blind watermarking of manifold surfaces," in *Proc. of the workshop on Multimedia and security*, 2008, pp. 43–52.

[14] K. Wang, M. Luo, A. G. Bors, and F. Denis, "Blind and robust mesh watermarking using manifold harmonics," in *Int. Conf. on Image Processing (ICIP)*, 2009, pp. 3657–3660.

[15] M. Oakes, D. Bhowmik, and C. Abhayaratne, "Global motion compensated visual attention-based video watermarking," *Journal of Electronic Imaging*, vol. 25, no. 6, pp. 061624–061624, 2016.

[16] D. Bhowmik, M. Oakes, and C. Abhayaratne, "Visual attention-based image watermarking," *IEEE Access*, vol. 4, pp. 8002–8018, 2016.

[17] C. Jin, Z. Zhang, Y. Jiang, Z. Qu, and C. Ma, "A blind watermarking algorithm based on modular arithmetic in the frequency domain," in *Advances and Innovations in Systems, Computing Sciences and Software Engineering*, pp. 543–547. 2007.