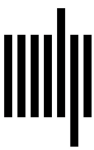
Cryptographic City

Decoding the Smart Metropolis

By: Richard Coyne

Citation:

Cryptographic City: Decoding the Smart Metropolis
By: Richard Coyne
DOI: 10.7551/mitpress/14712.001.0001
ISBN (electronic): 9780262374811
Publisher: The MIT Press
Published: 2023



The MIT Press

12 Hidden Measures

Personal data circulates in the cryptographic city. Algorithms can calculate inferences about individuals, groups, and whole populations from such data. For example, pattern-matching algorithms can categorize people according to the words they use in their social media posts.

Researchers at the University of Cambridge Psychometrics Centre developed a demonstrator program that claims to derive your personality profile, age, and other information from how you use language in a blog, Twitter feed, or email.[1] Anyone can interact with the demonstration program on the Apply Magic Sauce: Trait Prediction Engine website. Calling on machine learning techniques the researchers see this demonstrator as "a modest attempt to reverse the trend in Big Data and empower citizens to not only retain control of their data but also derive meaningful insight from it." The program "learns" from an extensive training set of texts and author profiles. It then estimates the personal attributes and psychological profiles of the authors of new texts. It calculates whether you are likely to be conservative or liberal, impulsive or organized, competitive or trusting, relaxed or succumb easily to stress.

The Cambridge program demonstrates the potential of text and other data harvesting. Pattern-matching algorithms can take the content of our social media posts and even our sequencing of keyboard strokes to make inferences that put us into categories as individuals or groups. The idea is that our digital footprint reveals more about us than we state explicitly, and some of it can be gleaned not only from what we write, but also from actions such as our choices of images we put on Instagram, TikTok, or Snapchat. From such incidental data, machine learning might estimate our educational attainment, ethnic background, social circle, disposable income, purchasing habits, the kinds of holidays we take, and alcohol consumption.

Your digital footprint also provides a rough guide to your politics. Such systems are not always accurate in assessing personality or background, but they don't have to be. They serve to narrow the target for public information, advertising, propaganda, and social interference campaigns to exert influence or disrupt the opinions and habits of citizens. Accurate, individual personal profiling from your digital footprint is error-prone, but it is the aggregation of such assessments across whole populations that provides the benefits to advertisers, persuaders, and political actors as outlined in chapter 11. If political campaigners can target enough people with a message tuned to voters' social and personality profiles, then that could be sufficient to tip a vote in favor of one candidate over another.

With this kind of personality profiling, social media platform developers can also fine-tune their systems to maximize revenue by generating controversy and hence engagement. The release of the trove of papers ("The Facebook Papers") by whistle-blower and former Facebook employee Frances Haugen in 2021 suggests that Facebook presents its newsfeed content to polarize opinion and keep people engaged, if not "addicted," in their social media news feeds. At a US Congressional hearing, Haugen asserted, "I'm here today because I believe Facebook's products harm children, stoke division and weaken our democracy."[2] The charge of harming children related to making "young girls and women feel bad about their bodies."[3] The reference to democracy suggests the programs that configure your newsfeed on Facebook tilt what you read toward controversial posts authored by readers and contributors, further influencing people's politics. The "active measures" outlined in chapter 11 can also exploit such methods. That's part of the opportunity, challenge, and peril of big data in the cryptographic city.

Where they occur, these monitoring processes are covert, involving company policies that are hidden from users, but also involve algorithms that are little understood by people who use the platforms. Similar hidden processes are at work in online retail and booking systems. We become aware that some calculation is happening in the background of our interactions when we receive directed advertising, or the platforms appear to come preloaded with preferences derived from our purchasing history on this or other platforms.

Online retail is a key instance of the cryptographic economy and relies on methods for hiding and securing transaction information. Such processes also rely on their own hidden protocols as they interface with users.

Shoshana Zuboff exposes how these patterns provide information about consumer behavior, much of which constitutes a hidden commodity traded and sold between companies, often without our knowledge or explicit consent.[4]

Algorithms Everywhere

Processes of online selection, booking, and purchasing are at the interface of the platform experience for many urban consumers and Internet users. So far, I have invoked terms such as *programs*, *systems*, *applications*, *apps*, *platforms*, and *algorithms* as the vehicles for these hidden data-harvesting processes. The word *algorithm* pertains to information processing via computer, as "a precisely defined set of mathematical or logical operations for the performance of a particular task" (OED). The word shares its derivation with *algebra*, which is a term I am prepared to associate with a specialized knowledge and was a significant and intimidating aspect of my own schooling. Social media commentators have directed their attention to the "algorithm" as a target of concern. For example, in her recent study into digital technology Ruha Benjamin poses the challenge, "What do 'free will' and 'autonomy' mean in a world in which algorithms are tracking, predicting, and persuading us at every turn?"[5]

It is worth examining what algorithms mean to the cryptographic city. To elaborate on the OED definition, algorithms are precise and repeatable procedures for accomplishing a computable task. An algorithm is a component of a computer program directed at a particular subtask and with an identifiable logic. So there are algorithms well known to programmers for searching a text file or database for the occurrence of a particular word, and algorithms for compiling and sorting lists of words, and processing decision trees.[6]

It is a commonplace to remark that algorithms are typically "hidden." They are "black boxes," the content of which may be known only to the author of the algorithm. In fact, computer programmers typically draw on libraries of algorithms to assemble their own algorithms. Some of these library elements are specific to the operating system or the brand of microchip the computer program is running on. In so far as *algorithm* serves as a useful term to describe what happens in digital systems, algorithms are combined, configured, and nested and are transparent and visible to

varying degrees in their development and deployment and for different programmers, engineers, developers, and users.

Algorithms are responsible for encrypting and decrypting files and data flows, and create, process, and compare hash strings. Algorithms also activate the pixels on a display screen to form text and images, open and close files in response to mouse clicks, manage and transmit bit strings through networks, and perform countless benign operations that any computer user is unlikely to know or care about.

The algorithms that draw opprobrium from some critics are likely those that surreptitiously monitor our purchasing habits, mouse clicks, screen attention, and flows of social media data. Whether they implement covert social media monitoring or enable web search, algorithms and their combinations inevitably embody values. I have referred to Ruha Benjamin's commentary on algorithms. Her book is really about racial biases in the digital realm: *Race After Technology*. She writes, "It is certainly the case that algorithmic discrimination is only one facet of a much wider phenomenon, in which what it means to be human is called into question."[7] Appropriate and inappropriate bias is impossible to eradicate, though fair and open social discourse and action requires that we are always prepared to challenge our biases.[8]

Bias is common in any technology. As an urban example, until special interest groups lobbied regulators and designers to make buildings more accessible, buildings would limit access to people with a particular range of physical mobilities. Architects realized that the width, swing direction, threshold, and opener of the ubiquitous and ordinary office doorway could include or exclude people who would otherwise need to use the door.[9] Prior to that awakening, and legislation, a value system was in play behind the affordances of doorway design that many designers would take for granted. So too, the design of a smartphone assumes a certain dexterity and visual acuity that able-bodied designers take for granted. Interaction design also assumes certain value systems grounded in assumptions about cognition, consumption, communication, and sociability.

Bias is evident in the algorithms, but also the data, the structuring of the data, and what the algorithm admits or excludes as data in the way it is designed. In some cases bias is coded into weightings attached to different data components. As a further urban example, the UK's Consumer Data Research Centre provides data and maps to indicate where residents

are poorly served by public facilities and where incomes are low, in other words, areas of multiple deprivation.[10] The algorithms process and display relevant data about income, numbers of people in households, and distances from amenities.[11] Controversy arises about the respective weighting applied to each of these factors in identifying and mapping areas of poverty. The weightings inevitably and explicitly encode biases, and different weightings produce differing distributions of deprivation on the maps.

Who is responsible, and therefore accountable, for what an algorithm does? Who feeds the values into the design of an algorithm? In the case of a building design there are many "authors," secreted within the value systems of manufacturers, suppliers, consultants, owners, regulators, funders, professional bodies, and educators. So too there are many authors of a typical computer program. In her book *Cloud Ethics*, Louise Amoore asserts that "the algorithm already presents itself as an ethicopolitical arrangement of values, assumptions, and propositions about the world."[12] This multiauthor view informs her account of "algorithmic ethics."[13] We want to identify the human agent responsible for biases, errors, and inequities we encounter online. Yet responsibility resides with a multitude of agencies.[14] By this reading, the focus on algorithms as the purveyors of hidden bias is an attempt to identify people and things that are ethically accountable.

Programmers write algorithms to disrupt or confound the functions of other algorithms, and to break through cryptographic defenses as in the case of the espionage measures described in chapter 11. In that chapter I also described algorithms and methods that deploy obfuscation as a means of confounding the operations of platforms, infrastructures, and even social organization. These tactics can operate in service of either the predator or the prey, the aggressor or the victim.

On the side of the "prey," agents that seek to protect consumers have devised obfuscation tactics to confound data harvesting. The app called AdNauseam disrupts the operations of web platforms that profile you according to the ads you click. When installed in your browser the app automatically sends clicks to the server for every ad on a page. According to the adnauseam.io website: "As the collected data gathered shows an omnivorous click-stream, user tracking, targeting and surveillance become futile."[15]

Advertisers and profilers also want to know where you are. To confound this locational information the TrackMeNot browser plugin sends false

navigation data to the server that is trying to surveil you. It obscures your locational coordinates. TrackMeNot blends fake and actual search data to obfuscate profiling. The trackmenot.io website says, "With TrackMeNot, actual web searches, lost in a cloud of false leads, are essentially hidden in plain view."[16] In their book *Obfuscation: A User's Guide for Privacy and Protest* (referenced in chapter 11), Brunton and Nissenbaum offer a range of consumer-oriented obfuscation tactics.[17]

Feature Variables

The average user of a computer program will not know or care about the myriad algorithms it deploys. The whole program is hidden as are its functions and procedures. Algorithms make use of slots in computer memory into which are stored numbers and characters as binary coded variables. All we consumers see is the interface and a subset of variables relevant to our interactions.

Some variables exist on a numerical scale, identified as quantities: age, SAT score, income, house number, property area. If I only know the dimensions of my property, then the area is a variable that is hidden until I calculate it from the dimensions. However, some variables are more hidden than that.

The identification and influence of hidden variables is one of the major challenges of statistical and machine learning methods deployed in big data analysis. Unknown factors may lie latent in the data as "confounding variables." That is another category identifying variables that are invisible because we do not have precisely the right information that brings them to light. Techniques for clustering concepts serve to identify and instantiate the values of variables. These include statistical analysis and neural network methods of machine learning.[18]

Considering the high premium placed on the visual affordances of the built environment, automated feature detection offers high rewards for organizations. Amazon offers a service for businesses to identify features in large collections of images. According to the aws.amazon.com/rekognition website, the service provides automatic labeling of elements in a picture (e.g., here is a person on a bike, there's a traffic jam). A company can identify if its brand label happens to appear in a news report, identify image rights violations, detect inappropriate or dangerous content or objects,

recognize celebrities, and check whether people are wearing the right personal protective equipment (PPE).

The Google Cloud Vision AI platform provides an API (application programming interface) for researchers to identify features within large numbers of publicly visible images, as on photo-sharing platforms (Flikr, Snapchat, Instagram) or an individual's own private image collection.[19] That has potential uses in detecting what people focus on as important, attractive, interesting, or "instagrammable" about a place. Several platforms offer similar capability. The features detected are typically words (house, tree, sky, etc.) with a confidence number attached. Unlike the tags or metadata people sometimes attach to their digital photos, the platform's algorithms generate these as feature lists automatically.

Microsoft Word provides automatic "alt text" creation based on features for image content that text-to-voice readers can recite for people with visual impairment. Figure 12.1 shows an urban image and the features Google Cloud Vision API plugin detects automatically, along with a confidence ranking. With this plugin, users of the software can select the features they want to adopt as tags to assist in search at some later date, or as the basis of their own alt text descriptors.

Google generates feature tags based on its access to very large stores of online imagery in which photographers, users, or human operators have already identified the content.[20] These word tags help the search algorithms identify and filter images as well as match images that have similar features. The current incarnation of the Google Image search facility (Google Lens) on a smartphone matches locations as well as images and returns links to relevant websites. The app will even identify species and types of animals, plants, and human-made objects. The platform also delivers collections of similar images that have also been tagged automatically with such features. Automated feature detection is accessible to anyone with a networked computer or a smartphone.[21]

Feature detection within images deploys various machine learning techniques. As I have already suggested, a machine learning algorithm scans thousands of "training" images that are prelabeled with relevant feature descriptors. The algorithm adjusts the numerical variables in its network data structure to reproduce those same labels when it encounters those images again. It thereby "learns" to re-identify those features. More important, the variable adjustments are such that the algorithm can detect the

Labels				Objects	
Cloud	97%	Monochrome Photography	76%	Building	90%
Sky	96%	Façade	75%	Person	89%
Building	95%	Crowd	75%	Building	88%
Daytime	95%	Human Settlement	74%	Building	87%
Window	93%	Pedestrian	74%	Building	79%
White	92%	Mixed-use	73%	Clothing	77%
Black	90%	Street	71%	Person	77%
Infrastructure	89%	Downtown	70%	Person	76%
Street Light	87%	Travel	69%	Person	74%
Style	84%	Winter	68%	Person	73%
Urban Design	82%	Walking	68%	Person	73%
Tree	82%	Event	68%	Person	71%
Neighbourhood	82%	Street Fashion	67%	Person	64%
Public Space	82%	Spring	65%	Clothing	61%
Road Surface	82%	Stock Photography	63%	Person	59%
Road	80%	Apartment	62%	Person	51%
Sidewalk	80%	Tourism	61%		
City	79%	Town Square	61%		
Thoroughfare	79%	Cobblestone	58%		
People	78%	Recreation	57%		
House	78%	Commercial Building	57%		
Metropolitan Area	77%	History	55%		
Monochrome	77%	Transport	54%		
Metropolis	77%	Plaza	52%		

Figure 12.1

Feature detection in a photograph. Tabulated lists are from the Google Cloud Vision API which also identifies and outlines areas in the image to which the tags apply. The Google Lens app delivers similar information, including a collection of pictures from the web that are similar. Automated text generation by Microsoft Word provides alt text: "A group of people walking on a sidewalk next to a street. Description automatically generated with medium confidence." Photograph by the author.

same features in new images it has not previously scanned. This is a neural network approach to machine learning. Amazon describes its feature (object) detection algorithm as one such "deep neural network": "It is a supervised learning algorithm that takes images as input and identifies all instances of objects within the image scene. The object is categorized into one of the classes in a specified collection with a confidence score that it belongs to the class."

The "learning" process is not entirely automated. Neural network developers have to devise the network configuration, decide what constitute inputs and outputs to the network, the layers in between (hidden layers), and the sensitivity of the network's numerical variables—weightings, probabilities, network connections (edges), and threshold values.

Louise Amoore explores the ethical dimensions of designing a neural network: "This spatial arrangement of probabilistic propositions is one of the places where I locate the ethicopolitics that is always already present within the algorithm. The selection of training data; the detection of edges; the decisions on hidden layers; the assigning of probability weightings; and the setting of threshold values: these are the multiple moments when humans and algorithms generate a regime of recognition."[22] She is critical of the reductive nature of feature detection. In any case, though they are effective in processing large numbers of images, automated feature detection algorithms are less accurate or nuanced than human beings. The algorithm misses the "features" in figure 12.1—that there's a marquee in the frame, a glass-roofed atrium, or that it is windy—and is incapable of delivering the meaning and significance of the picture as a whole to its various human interpreters and audiences.

Automated feature detection in imagery is a useful test case for the ethics of machine learning, though the application of the techniques extends to other sensory modalities as evident in surgical procedures that include multiple sensory skills such as touch and precise movement. Amoore makes the case that machine learning highlights the conflicted nature of attributing responsibility. Who is responsible for errors and misjudgments? Mistakes in robotic surgery procedures, errors in automated drone strikes, harm to noncombatants and false matches in image analysis provide obvious examples. She suggests that the surgeons, drone operators, and photographers who create the training sets on which the machine learning is based carry some

responsibility. I would argue that the ethical responsibility extends to those who design, select, adjust, and deploy the learning algorithms.

The argument about shared and conflicted attribution is similar to discussions about authorship, originality, and intellectual copyright within the creative professions. I agree with Amoore that attribution is contextual, and fraught, and is resolved by human judgment: "Ethicopolitical life is about irresolvable struggles, intransigence, duress, and opacity, and it must continue to be so if a future possibility for politics is not to be eclipsed by the output signals of algorithms."[23]

Probabilities

Machine learning algorithms that match images of the kind I have just described typically provide sets of features detected with a confidence or probability value attached as in figure 12.1.

Statistical information also helps establish the probability that a particular event will occur, such as the probability that any individual will be involved in a traffic accident. For example, the probability that a traffic accident is due to driver carelessness is over 50 percent according to some studies.[24] Statistical analysis can also establish that one event followed another, so that the probability that a traffic accident will be followed by hospitalization of the accident victims might be 12 percent. Algorithms that control traffic lanes or self-driving cars can take such events and sequence probabilities into account to make predictions. The class of computational techniques for this kind of calculation are the Hidden Markov Models (HMM) referenced in chapter 4, with applications ranging from managing urban mobility to gene prediction.[25] Some automated speech recognition and language translation programs also deploy HMMs to process information about word sequences. To the technologies of writing and print in chapter 2, we can add speech-to-text, text-to-speech, and automated language translation as factors in the operations of the cryptographic city.[26]

Andrey Andreyevich Markov (1856–1922) was a mathematician who devised methods for modeling probabilistic processes. Sequences of events linked by probabilities in the way I have described is called a Markov chain. That is a chain of events for which the probabilities of any event A (such as a traffic accident) will be followed by another event B (hospitalization) irrespective of what events preceded A.

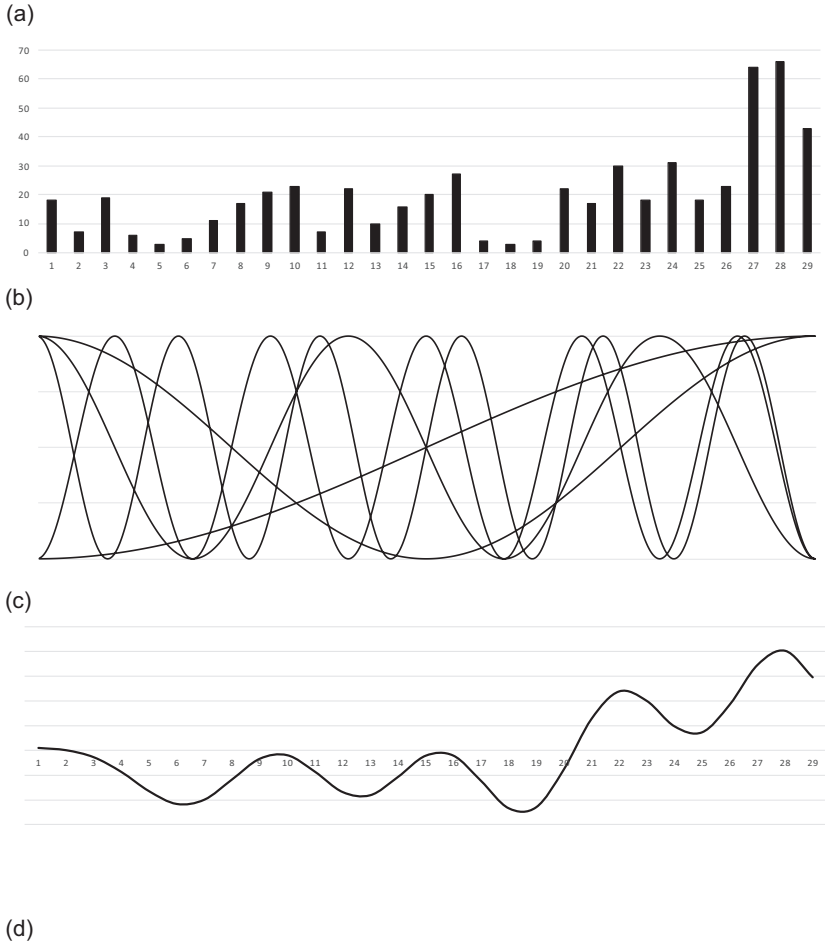
Generalizing this method, the nodes in a network diagram could be decision points, such as navigating from one web page to another, or road junctions encountered while a driverless car navigates through the city. The links in the Markov chain network are labeled with the probability that the driverless car would take that path given statistical data about congestion or road gradient.

Markov modeling is a further example of information "hidden" within data that exploits probabilities and informs operations in the cryptographic city. The second element in the algorithmic armory of big data is to exploit the repetitive nature of much human and machine actions, and of data flows that repeat.

Coefficients

There exists a class of urban problem-solving that reduces complicated variations in data values to a series of simple cyclical patterns of different frequencies. The method determines the contribution of each of those frequencies to the overall pattern in the data. The process identifies the main frequencies and a series of coefficients that show the percentage of each frequency in complex data as explored in chapter 10. That is a useful type of analysis as it helps tease out patterns in data and thereby identify variables hidden within it. One such method is known as discrete cosine transform (DCT).

A key article by Ahmed et al. on the DCT method presents it as a means of recognizing patterns in data.[27] In figure 12.2 I show a simple experiment in which I attempted to capture regular cycles in publicly available local data about COVID cases at the early stages of the pandemic. The automated process attempts to match a series of repeating cosine curves to the data. The result is a series of coefficients, numbers that represent how much each cosine curve contributes to the overall wave pattern in the data. The DCT method also serves as a way of compressing complex data, as you only need to store the coefficients and simple indices that designate each cosine curve. The data here is in just one dimension, showing numbers of infections over a short time period. This is a demonstration and founded on the assumption that there are time-based regularities that contribute to the COVID case count, such as people's weekly activity cycles, alterations in the virus, waves of resistance, immunity, other diseases, other



(d)

frequency	1	2	5	10	11
coefficient	–86.93	73.91	40.95	–60.67	41.76

Figure 12.2

Discrete cosine transform (DCT) analysis of the number of people who reported COVID-19 each day in Scotland over a twenty-nine-day period in March 2020. (a) Numbers of cases over twenty-nine days. (b) The five most prominent component frequencies detected in the data by DCT adjusted to the same amplitude and with smaller frequencies filtered out. (c) Reduction of the original data to its major frequencies. (d) The most prominent frequencies and their contributions to the data as coefficients. *Source:* Author.

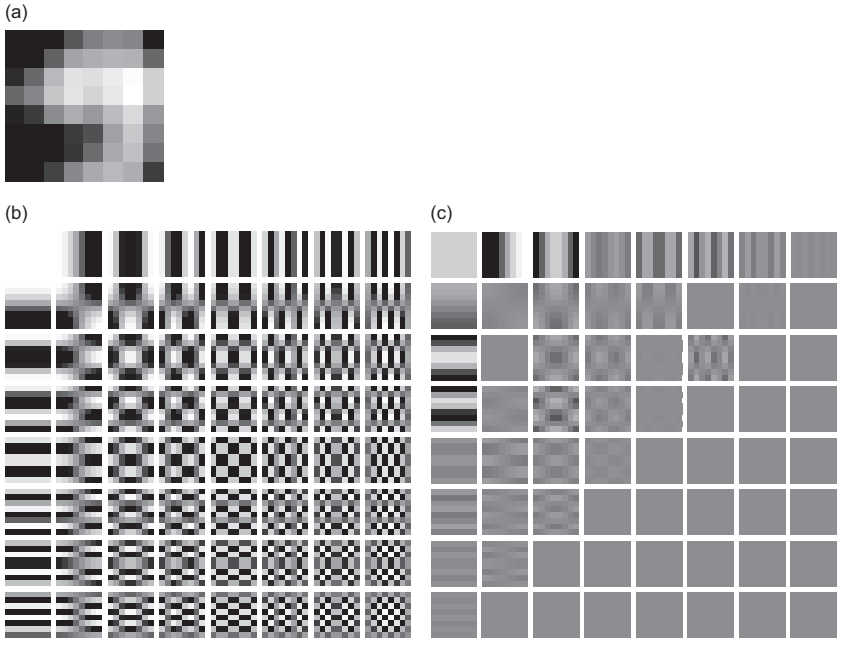


Figure 12.3
Reducing the color frequencies in an 8×8 target image (a). The second image (b) shows 64 frequency variations in gray across an 8×8 array of pixels. The variations follow simple cosine distributions at different frequencies in the x and y directions. The 2D discrete cosine transformation (DCT) method effectively tests each of the 64 8×8 variations in the array (b) against the target image (a) to detect the percentage of their presence. The second 64 variations array (c) shows the presence of each frequency as variations in luminosity. When overlayed, each of the 8×8 pictures in the second array would approximate the target image. The frequency variations that appear mostly in gray contribute little and can be filtered out when the file is saved. JPEG compression uses this method to reduce file size. Cryptographers can use the gray areas to store hidden information as a steganographic technique. *Source:* Author.

environmental responses of the virus, or the introduction of new vectors for transmission.

The DCT method can also be applied to 2D information, as in the case of mapped data or pictures. DCT helps to analyze or compress picture images (figure 12.3). As outlined in chapter 10, the JPEG method of image compression uses DCT coefficients to filter out inconsequential variations in color intensity across an image. It breaks an image into 8×8 pixel squares and stores the major coefficients for each square.

Watermarking of images and steganography (described in chapter 9) must deal with image-compression algorithms, which adjust pixel color values and potentially purge the data of hidden values, as in the case of LSB (least significant bit) methods of hiding images. Algorithms that compress, hash, and encrypt data converge in their indifference to the content or meaning of the signals they are processing. Digital encryption cares little about what the data means.

I include this 2D example here as it pertains to the automated detection of features in images. The coefficients are hidden features, scarcely recognizable by a human observer, yet important for algorithms that process, search, and match images, as well as those that hide information in pictures. Data, information flows, and images harbor hidden frequencies, cycles, and rhythms. Similar analysis reveals rhythms hidden within the city.

Rhythms

One of the distinctive features of city living is the concentration of rhythmic patterns. Rhythms permeate the city, and these rhythms overlap, combine, aggregate, and interfere with one another. That is the gist of Henri Lefebvre's (1901–1991) book entitled *Rhythmanalysis*.[28]

By my reading the concept fits within the genre of research concerned with *everydayness*, the *quotidian*, which implies a concern with ordinary things and everyday phenomena that repeat. Lefebvre's book first appeared in 1992 before the boom in big data. Few commentators at the time saw any potential for computers to do justice to the ordinary and everyday experience of repetitions, cycles, and rhythms.

As I explored in my book *The Tuning of Place*, mundane and ordinary events are also everyday events, that is, events that occur every day, repeatedly, and relate to people's habitual activities.[29] So, a rhythmanalysis will focus on ordinary events and things that we take for granted. The book *City Rhythm* by Caroline Nevejan, Pinar Sefkatli, and Scott Cunningham recruits rhythm to explain cities and their internal diversity, as well as to account for differences between cities.[30] Their book also introduces the application of HMM as a way of explaining what happens in cities. *City Rhythm* amplifies the rhythm metaphor by mapping what the authors refer to as "beats," "base rhythms," and "street rhythms" across cities in The Netherlands.

I think by "beats" the authors mean the dominant rhythms of a region, exemplified by the ebb and flow of the volume of pedestrian and road traffic. By their reading, base and street rhythms "show significant transitions over time for the specific area."[31] I'm interested in the authors' claim that this kind of analysis can bring out similarities and differences between regions. According to the book, rhythms influence how people feel in each other's company: "When sharing rhythm, people feel more at ease with each other."[32] Rhythms engender trust: "When recognizing each other, people synchronize and tune their rhythm to each other."[33]

The rhythm concept also helps explain the mismatch between citizens and the systems of the city, in particular the road system: "The roads are too wide and busy, and the traffic lights are too short to cross the streets. This situation is reflected on the mismatch in the rhythms between the elderly and the rather fast rhythms that the neighbourhood presents."[34] Such rhythmanalysis helps explain conflicts between city inhabitants, as in the case of the insecurities felt by some less-mobile people when in proximity to exuberant youths. One image in the book shows a series of frequency curves, approximating cosine curves, of the intensities of activities across a typical week in the Keizerswaard shopping center.[35] Drawing on Giles Deleuze and echoing some of the ideas I explored in *The Tuning of Place*, Nevejan, Sefkatli, and Cunningham show how: "A territory happens when different rhythms come together and they create their own expressive language."[36] Rhythmanalysis is an example of semi-formal algorithmic analysis applicable to the cryptographic city. The hidden variability of city living is temporal as well as spatial.

Secret Synchronies

I will conclude this chapter by reinforcing the relationship between rhythms and patterns of secrecy in the city. Patterns in cycles are among the panoply of hidden dimensions in the city. The methods I've been describing illustrate a basic truism: events follow one another in sequence, inexorably and in daily, weekly, monthly, and annual cycles. At a personal level, you brush your teeth, you wash your face, you pour the cereal and milk, you eat it, you rinse the bowl, you attend an online meeting, you get dressed, and so the day proceeds. Such sequences follow patterns. In some cases, an automated system might attempt to detect those patterns: to predict what

comes next, to show how to reinforce or break out of a pattern, or to detect the variables that influence those event sequences. We often describe deviations from the norm in terms of cycles. It is a time-worn conception about creativity: to think out of the box you need time out of the schedule, the routine, the humdrum world of everyday matters.

The concept of urban cryptography as a commerce in hidden messages has never been far from my considerations in this chapter. Some writers define the act of keeping secrets with recourse to cycles and frequencies. For example, an online *Psychology Today* self-help article explains that to keep a secret is a "habit of mind," and it is mostly a bad habit—something to break out of.[37]

But to investigate secrets does not require us to make such a judgment. An academic article on "family secrets" by Mark Karpel refers to the "loyalty dynamics in the creation, maintenance, and eventual facing of secrets in families."[38] Secrets require maintenance—repeatedly. Not only are some secret acts performed in repetitive cycles, but secrets of any consequence encounter repeated onslaughts from exposure, require repeated evasion and denial, and yet more elaborate and repeated cover-ups and obfuscations.

We've seen in public forums that secrets are often in the company of lies, and lies are rarely singular, but get repeated, amplified, and woven wickedly into sticky webs. Secrets and lies are habituated exercises in repetition. I first made these observations during the tenure of the forty-fifth U.S. president when commentators would note the repetition of the president's mistruths: the size of the inauguration crowd, that the conversation with the Ukrainian Prime Minister was a "perfect call," that the election the president lost was fraudulent. Lies and propaganda have to be repeated to reinforce them and to resist the weight of contradictory evidence. Such repetitions also make use of weekly and seasonal news cycles. Active measures, infiltration of social media news feeds, and kompromat by foreign adversaries exploit such cycles and repetitions.

I take it for granted that events repeat or fit into a cycle of repetitions. Whether or not they are made explicit as schedules, our everyday lives are permeated with events that occur every day, or every other day, or weekly, annually, hourly, by the lunar calendar, the seasons, tides, breaths or other cycles, and cycles within cycles. Agents of such occurrences may wish to expose events to different constituencies, or hide them altogether, as is the

case when the social media user adjusts the privacy settings for particular postings.

How do you maintain secrets so that they are invisible to others on a cyclical timeline? One method is to resist other people's cycles, simply by operating acyclically or asynchronously. If you've shared a home with someone who goes out in the evening and is back in bed just as you are getting up, then you'll know the relationship between cycles and secrecy.

As I've seen in heist and prison escape dramas, those working in secret operate counter to regular patrols, the sweep of the surveillance camera or spotlight, opening hours, night porter duties, and the usual daily cycle. Habitual criminality weaponizes the counter-schedule. Seasoned criminals work on different cycles from their victims, and the dark arts of cyber criminality adapt to the complex periodicities of 24/7 global communications.

One of the challenges in detecting crime, and the same applies to uncovering secrets, is to know if the events you observe are part of a concerted plan or merely coincidences. I think of a coincidence as the meeting of two or more cycles at a particular moment. Secret deeds give themselves away through coincidence. That is one of the ways to catch someone in a criminal act—align the patrol with the cycles of the criminal.

In his *A Burglar's Guide to the City*, Manaugh refers to homeowners' "rhythms of vulnerability."[39] Most homeowners know about the risks of leaving a place unoccupied and have simple electronic timers that turn the lights on in the evenings while they are on holiday. You can even install a flickering light source that suggests someone has the television set on.[40] Then there's the practice of "oversharing" on social media, by which burglars can easily deduce whether or not you are at home, and sometimes infer the location of your home. There is (or was) a website to test such vulnerabilities called pleaserobme.com.

Cyclical properties of algorithms, variables, probabilities, and coefficients constitute hidden dimensions to the cryptographic city. These hidden features also make worlds, universes, and cities beyond our ordinary apprehension, the subject of chapter 13.

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in ITC Stone Serif Std and ITC Stone Sans Std by New Best-set Typesetters Ltd.

Library of Congress Cataloging-in-Publication Data

Names: Coyne, Richard, author.
Title: Cryptographic city : decoding the smart metropolis / Richard Coyne.
Description: Cambridge, Massachusetts ; London, England : The MIT Press, [2023] | Includes bibliographical references and index.
Identifiers: LCCN 2022021507 (print) | LCCN 2022021508 (ebook) | ISBN 9780262545679 (paperback) | ISBN 9780262374811 (pdf) | ISBN 9780262374828 (epub)
Subjects: LCSH: Smart cities. | Internet of things. | Urban development—Data processing. | Public administration—Security measures. | Data encryption (Computer science)
Classification: LCC TD159.4 .C69 2023 (print) | LCC TD159.4 (ebook) | DDC 004.67/8—dc23/eng/20221011
LC record available at https://lccn.loc.gov/2022021507
LC ebook record available at https://lccn.loc.gov/2022021508

10 9 8 7 6 5 4 3 2 1