MY WEIRD PROMPTS

Podcast Transcript

EPISODE #141

Hidden in Plain Sight: The Secrets of Steganography

Published January 03, 2026 • Runtime: 25:45

https://myweirdprompts.com/episode/steganography-hidden-messages-ai/

EPISODE SYNOPSIS

Join Corn and Herman Poppleberry as they peel back the layers of steganography, the ancient art of hiding messages in plain sight. In this deep dive, the brothers explore how everything from invisible yellow printer dots used by the Secret Service to the latest AI watermarking technologies like Google’s SynthID are used to track and transmit secret data. By examining real-world examples—ranging from Russian sleeper cells using public image galleries to dissidents in Iran bypassing state surveillance—this episode reveals the high-stakes battle between visibility and obscurity. Whether it is a "digital dead drop" in an unsent email or a secret code hidden in a vintage toaster listing on eBay, you will learn why the most effective secrets are those that never appear to be secrets at all.

DANIEL'S PROMPT

Daniel

"We previously discussed operational technology and secret networks. Today, I want to talk about steganography—the practice of hiding messages in plain sight. This is especially relevant now as AI companies begin digitally watermarking their content, which raises concerns about privacy and transparency. Steganography has a long history, from invisible printer dots to modern methods like using eBay listings or unsent email drafts to communicate covertly. It's used by everyone from whistleblowers and dissidents to criminal organizations. I'd like to discuss the modern relevance of steganography and how it's being used today by both those pursuing good and those doing the opposite."

TRANSCRIPT

Corn

Hey everyone, welcome back to My Weird Prompts. We are coming to you from our living room in Jerusalem on this third day of January, twenty twenty-six. I am Corn, and I am joined as always by my brother.

Herman

Herman Poppleberry, at your service. Happy New Year, Corn. I cannot believe we are already three days into twenty twenty-six. It feels like the future is arriving faster every week.

Corn

It really does. And speaking of the future, or perhaps the hidden parts of it, our housemate Daniel sent us a fascinating prompt this morning. He was listening to our recent episodes, specifically episode two hundred forty-six where we dove into operational technology and those secret military networks, and it got him thinking about a different kind of secrecy. Not just secret wires, but secret messages hidden right in front of us.

Herman

Ah, steganography. Daniel always has a knack for finding the connective tissue between our deep dives. It is the perfect follow-up to our talk about shadow webs. While those are about where the data travels, steganography is about how the data hides itself in plain sight.

Corn

Exactly. And Daniel mentioned something that is been all over the tech news lately, which is the push for AI companies to digitally watermark their content. There is this whole debate about privacy and transparency, but at its heart, it is just a modern application of a very old practice. So today, we are peeling back the layers on how people hide messages in images, eBay listings, and even unsent email drafts.

Herman

I am so excited for this one. Most people think of encryption when they think of secret messages, but steganography is fundamentally different. Encryption makes a message unreadable, but steganography makes the message invisible. It hides the fact that a message even exists. If I send you an encrypted file, everyone knows I am hiding something. If I send you a picture of a cat using steganography, no one even looks twice.

Corn

That is the core of it, right? The security of obscurity versus the security of math. But before we get into the high-tech AI watermarking of twenty twenty-six, let's look back. Daniel mentioned those invisible printer dots. I remember hearing about those years ago, but I never realized how widespread it was.

Herman

Oh, it is fascinating and a bit chilling, honestly. It is called the Machine Identification Code. Back in the nineteen eighties and nineties, the Secret Service actually worked with major printer manufacturers like Xerox and Canon. They wanted a way to track counterfeiters. So, every time you print a color document, your printer adds a pattern of tiny yellow dots to the page.

Corn

And these are invisible to the naked eye?

Herman

Almost entirely. They are less than a tenth of a millimeter in diameter. You usually need a blue light or a microscope to see them. But they are there, arranged in a grid that encodes the serial number of the printer and the exact date and time the document was printed.

Corn

That is incredible. So every time a whistleblower prints out a document to leak to the press, they are essentially signing their name on it in invisible ink?

Herman

Precisely. That is actually how Reality Winner was identified back in twenty seventeen. She leaked a classified document to The Intercept, and even though the document was a scan of a printout, the FBI was able to look at those tiny yellow dots and trace it back to a specific printer in a specific office. It is steganography used for state surveillance, baked into the hardware we use every day.

Corn

It makes you wonder what else is baked in that we do not know about yet. But let's talk about how this works digitally. If I have a digital photo, say a five-megabyte JPEG of the Old City here in Jerusalem, how do I actually tuck a message inside those pixels without changing the look of the photo?

Herman

The most common method is called Least Significant Bit steganography, or LSB. Think about how a pixel is represented. In a standard twenty-four-bit image, each pixel has three color channels: red, green, and blue. Each channel is represented by eight bits, which is a number between zero and two hundred fifty-five.

Corn

Right, so if I change that number slightly, the color changes.

Herman

Exactly. But here is the trick. If you change only the very last bit, the least significant bit, you are only changing the color value by one. If a pixel’s red value is two hundred fifty, and you change it to two hundred fifty-one, the human eye cannot detect that difference. It is a microscopic shift in shade.

Corn

So I can take a long string of text, convert it to binary, and then distribute those bits across the least significant bits of thousands of pixels in my image.

Herman

You got it. You can hide an entire book inside a high-resolution photo, and to any observer, or even most basic image analysis software, it just looks like a normal photo. The entropy, or the randomness of the image data, barely shifts.

Corn

This brings us to the AI watermarking Daniel was asking about. Now that we are in twenty twenty-six, we are seeing things like Google's SynthID and other tools being integrated directly into generative models. Is that just LSB on steroids?

Herman

It is much more sophisticated now. Simple LSB is easy to break if you resize the image or compress it. The new AI watermarking works in what we call the frequency domain or the latent space of the model. Instead of changing individual pixels, they make subtle, mathematically-calculated adjustments to the patterns and textures that the AI generates.

Corn

So it survives being cropped or turned into a meme?

Herman

Usually, yes. It is designed to be robust. But Daniel raised a great point about privacy. If every image generated by an AI has a hidden tag that says which account generated it, we are back to the printer dot problem. It is a permanent, invisible link between a person and a piece of content.

Corn

And the companies say it is for safety, to prevent deepfakes and misinformation. But if the tools to read those watermarks are not public, then only the companies and the governments they cooperate with have the key. That lack of transparency is what seems to worry Daniel, and honestly, it worries me too.

Herman

It is a classic double-edged sword. On one hand, you want to know if a video of a politician is real. On the other hand, if a dissident in a place like Iran uses AI to create protest art, they might be unknowingly embedding their own arrest warrant in the file metadata or the pixels themselves.

Corn

Speaking of dissidents, let's talk about some of the more creative ways people are using steganography today. Daniel mentioned eBay listings and unsent email drafts. That sounds like something out of a spy novel.

Herman

It really is. The unsent email draft method is actually a famous one. It was used by David Petraeus and his biographer, Paula Broadwell, but it has been used by various intelligence groups for decades. The idea is that you and I share a single webmail account. I log in, I write a message in the drafts folder, and I never hit send. Then you log in from a different location and read the draft.

Corn

Because the email is never sent, it never travels across the internet as a packet that can be intercepted by traditional signal intelligence.

Herman

Exactly. There is no metadata of a transmission because there was no transmission. It is just a change in a database on a server. It is a digital dead drop. Now, modern forensics can still find it if they have access to the server or the computer's cache, but it bypasses a lot of the automated "dragnet" surveillance that looks for active communications.

Corn

And the eBay thing? How does that work?

Herman

That is even more clever. It is a form of linguistic steganography. Imagine I am an operative and I need to tell my contact that a meeting is back on. I post an eBay listing for a very specific, slightly overpriced vintage toaster. The description might have a specific typo in the third paragraph, or I might use a specific sequence of adjectives.

Corn

So the message is not in the data bits, it is in the context of the public behavior.

Herman

Right. To the casual browser, it is just a weirdly described toaster. But to the person who knows what to look for, the price of forty-seven dollars and ninety-nine cents might mean "meet at the safehouse at eight PM." People have used everything from Craigslist ads to comments sections on obscure blogs to pass messages this way.

Corn

It reminds me of the "numbers stations" from the Cold War, but for the internet age. You hide the signal in the noise of global commerce.

Herman

Precisely. And in twenty twenty-six, with the sheer volume of data being uploaded every second, the "noise" has never been louder. It is the perfect place to hide.

Corn

Let's take a quick break for our sponsors. Larry: Are you worried about the invisible eyes in the sky? Do you feel like your every move is being tracked by tiny yellow dots and secret algorithms? You need the Signal-Shredder Three Thousand! This hand-held device uses patented "chaos-wave" technology to scramble the latent space around your digital devices. Just wave it over your smartphone or printer, and watch as the hidden watermarks simply evaporate into a cloud of harmless sub-atomic static. Warning: May cause temporary loss of Wi-Fi, mild toothaches, or the sudden realization that your neighbor is actually three owls in a trench coat. The Signal-Shredder Three Thousand—because what they can't see can't hurt you, probably. Larry: BUY NOW!

Corn

...Alright, thanks Larry. I am not sure I want to meet his neighbor. Anyway, Herman, back to the serious side of this. Daniel mentioned that steganography is being used by whistleblowers and dissidents, specifically mentioning the situation in Iran.

Herman

Yes, and this is where the stakes get very real. In repressive regimes, using encrypted apps like Signal or WhatsApp can sometimes be a red flag in itself. If the government sees encrypted traffic coming from your IP address, they might not know what you are saying, but they know you are hiding something.

Corn

Right, the "nothing to hide, nothing to fear" fallacy being used as a weapon.

Herman

Exactly. So, dissidents have turned to steganography to make their communications look like mundane activity. There was a case where people were hiding protest coordinates inside the metadata of popular music files or even inside the image data of innocuous memes. If the state censors are looking for keywords like "protest" or "revolution," they will miss a picture of a sunset that secretly contains a map.

Corn

We saw a lot of this during the Arab Spring too, right? People using Flickr and other photo-sharing sites.

Herman

Yes. And it has only become more sophisticated. There is a technique called "Chaffing and Winnowing." It is not strictly steganography, but it is related. You send a massive amount of messages, most of which are "chaff"—just garbage or normal talk. Only a few have the "winnowed" bits of the real message. To an outside observer, it looks like a teenager spamming their friends, but to the recipient with the right key, a secret message emerges.

Corn

It is about blending into the cultural background. If everyone is posting cat videos, you hide your message in a cat video.

Herman

Exactly. But there is a flip side. Criminal organizations and terrorist groups use these exact same tools. Back in twenty ten, the FBI broke up a Russian sleeper cell in the United States. These agents were using a special steganography software to hide messages inside images posted on public websites. They would literally upload a photo of a park or a building, and tucked inside were instructions from Moscow.

Corn

It is crazy to think that those images were just sitting there on the open web for anyone to see, but only ten people in the world knew they were looking at a top-secret briefing.

Herman

That is the power of it. It exploits the human tendency to ignore the mundane. We are wired to look for patterns, but we are also wired to filter out things that look "normal." Steganography is the art of weaponizing that filter.

Corn

So, how do we catch it? If I am a security analyst or a government agency, how do I find a needle in a haystack when the needle looks exactly like a piece of hay?

Herman

That field is called Steganalysis. It is a constant arms race. One of the main ways is through statistical analysis. Even though LSB steganography only changes the pixels by a tiny amount, it still changes the statistical distribution of the colors in the image. If you have a thousand photos from the same camera, and one of them has a slightly different "noise" profile, that is a red flag.

Corn

So you are looking for anomalies in the randomness.

Herman

Precisely. In twenty twenty-six, we are using AI to catch AI. We have neural networks that are trained specifically to spot the subtle artifacts left behind by steganographic tools. They can look at an image and say, "There is a ninety-nine percent chance this file contains hidden data," even if they cannot tell you what the data is.

Corn

It is the same way we talked about detecting operational technology leaks in episode two hundred forty-six. It is all about fingerprinting the "normal" state so you can spot the "abnormal" one.

Herman

Exactly. But as the hiding methods get better—using things like Generative Adversarial Networks to create "stego-objects" that are statistically perfect—the detection has to get even more sensitive. It is a never-ending game of cat and mouse.

Corn

I want to go back to something Daniel touched on regarding the eBay listings and the unsent drafts. That feels much harder to detect with an algorithm because it relies on human context.

Herman

You are absolutely right. That is what we call a "Covert Channel." It is not about the file itself; it is about the behavior. To detect an eBay listing used for spying, you would need an AI that understands the "market value" of a toaster, the typical writing style of a seller, and the frequency of listings.

Corn

So you would need an AI that is basically a social psychologist and an economist combined.

Herman

Essentially, yes. And that is where the privacy concerns really ramp up. If governments start using AI to monitor not just our data, but the "normality" of our behavior to find hidden messages, then we are living in a world of total behavioral surveillance. Every typo, every weirdly priced item, every late-night draft becomes a potential signal for an investigator.

Corn

It feels like we are moving toward a world where "privacy" is becoming a very technical, very difficult thing to maintain. If even a picture of my breakfast can be used to track me or hide a message that gets me in trouble, where is the safe space?

Herman

That is the big question for the next decade. We are seeing a move toward "deniable encryption" and other advanced forms of steganography that are built into our operating systems. But at the same time, the "shadow" networks we talked about last week are becoming more adept at spotting these tricks.

Corn

It is a lot to take in. Let's try to ground this for our listeners. What are the practical takeaways here? If someone is concerned about their digital footprint or interested in how this affects them in twenty twenty-six, what should they keep in mind?

Herman

First, be aware that "deleted" does not always mean "gone," especially with things like email drafts. If you are using a shared platform, the platform owners can see everything you type, even if you never hit send.

Corn

That is a huge one. People often use drafts as a "scratchpad," not realizing it is being synced to a server in real-time.

Herman

Exactly. Second, if you are a content creator, understand that AI watermarking is here to stay. Whether it is Google, OpenAI, or Meta, the images and text you generate likely have an invisible signature. This can be good for proving you created something, but it also means your anonymity is much thinner than you think.

Corn

And for the whistleblowers or those in sensitive positions?

Herman

Steganography is a powerful tool, but it is not a magic wand. If you are using a common, off-the-shelf steganography tool, assume the authorities have a way to detect it. The best steganography is often the most low-tech—using established patterns of behavior that look completely normal to an outsider.

Corn

Like the "toaster" example. It is about the story you are telling to the world, not just the bits you are hiding in the file.

Herman

Precisely. And finally, I think we all need to be more critical of the "transparency" claims made by big tech. If they are embedding hidden data in our content "for our safety," we should be asking who has the keys to read that data and what else is being hidden there.

Corn

I think that is a perfect place to wrap up the core discussion. It is a world of shadows, even in the brightest pixels.

Herman

It really is. I am so glad Daniel sent this in. It really tied together a lot of what we have been exploring lately. It makes me want to go back and look at every photo on my phone with a magnifying glass.

Corn

Well, maybe start with the blue light first, Herman Poppleberry. Before we go, I want to say that if you are enjoying these deep dives into the hidden corners of our world, we would really appreciate it if you could leave us a review on your podcast app or on Spotify. It genuinely helps other curious minds find the show.

Herman

It really does. We love seeing the community grow. And remember, you can find all our past episodes and a way to get in touch with us at our website, myweirdprompts.com. We are also on Spotify, obviously.

Corn

This has been episode two hundred forty-eight of My Weird Prompts. A big thanks to our housemate Daniel for the inspiration today. We will be back next week to fall down another rabbit hole.

Herman

Hopefully one that does not involve three owls in a trench coat.

Corn

No promises. Until next time, stay curious.

Herman

And keep an eye on those yellow dots!

Corn

Thanks for listening to My Weird Prompts. We will talk to you soon.

Herman

Bye everyone!