Florian Cramer

HIDING IN PLAIN SIGHT

Amy Suo Wu's The Kandinsky Collective

ENG

Florian Cramer

HIDING IN PLAIN SIGHT

Amy Suo Wu's The Kandinsky Collective

The history of 20th century painting conventionally identifies abstraction with modernism, and the return of figuration with postmodernism. But abstraction ended much earlier, in a spy operation during World War II when a British intelligence officer, in a stroke of genius, found abstract paintings to be the perfect carriers for secret messages transported across the ocean. For this purpose, he commissioned a painting to Wassily Kandinsky that included a secret message encoded – in the manner of flag signs or Morse code – into its seemingly abstract visual shapes. This anecdote explains steganography: the clever hiding of messages in other messages. Steganographic messages do not need to appear innocuous. At some point, militant jihadists were reported to run pornographic websites as a cover, using porn images for hidden communication. Unlike cryptographic messages, which typically are scrambled, unreadable and therefore visible as encoded message at first sight, steganographic messages are designed to slip under the radar. Amy Suo Wu's steganographic works do this as well, using *Cardan Grille* (the superimposition of grids on texts to uncover hidden text), substitution ciphers and camouflaged *text within text* in combination with invisible inks.

Kandinsky accepted the job for the British intelligence service, and his painting was shipped across the ocean. If we believe official history, this remained a one-time experiment. But how would modern art history need to be rewritten, and abstract painting to be reinterpreted, if the practice really continued? (This may be a less paranoid thought than it first sounds, given the historical fact of the CIA having been a major force in promoting post-war American abstract expressionist painting.)

Anecdote is, according to the Oxford English Dictionary, a "short, amusing or interesting story about a real incident". Edgar Allan Poe's short story *The Purloined Letter* (1844) can be read as an anecdote in this sense, since over the course of time, its status changed from a piece of fiction to an often-quoted, quasi-real life parable. In the story, amateur detective C. Auguste Dupin recovers a blackmail letter that police investigators had failed to find simply because they had searched a room looking for something hidden while he found it hanging there in plain sight. *The Purloined Letter* is thus the extreme example of steganography as a message that is not what and where it seems to be. So it is the seeming paradox of Amy Suo Wu's invisible ink works, and of steganography in general, that they show things in plain sight while hiding them at the same time. Professional steganographers call that which is publicly visible the "plaintext" or "payload" (which can be a painting, a piece of writing, an audio recording or any other medium) and the message hidden in it, the "cyphertext", "covert message" or "package".

Is analog steganography merely a legacy or nostalgic form of information obfuscation today? Especially when using the classical technique of invisible inks, in a digital communication age where few letters are still written by hand on paper?

Not even secret agents seem to use invisible inks any more. In 2011, the CIA declassified its own invisible ink recipes and published them online. This initiated Amy Suo Wu's research into invisible inks. Working at the fringes of graphic design, art, media research and activism, Wu does not reactivate invisible inks for simple aesthetic reasons. Neither is her project just about the post-digital, neo-analog appeal of these inks.

True, cryptography is digital by definition, whereas steganography can be both digital *and* analog. If the previous sentence sounds counter-intuitive, here's more explanation: Modern cryptography – the encryption and decryption of symbols using a code – is mathematical. (It even is a discipline of applied mathematics.) It therefore is digital according to the scientific definition of the word, as information processing of countable units. That means

cryptography is even digital when it does not involve zeros and ones in an electronic computing device (the colloquial definition of "digital"), but the replacement of letters through code numbers on a piece of paper.

But to return to steganography: When steganography is *digital*, it can, for example, involve hiding a text message in a JPEG image file, with the text only becoming visible if one opens the file in a text editor instead of an image viewer. Examples of digital yet non-electronic steganography include secret texts embedded into non-secret texts, for example through the first words of each paragraph. Amy Suo Wu's invisible ink works are good examples of *analog* steganography, since they involve no mathematics and no shuffling of letters and numbers, but only chemistry. Uncovering the covert message is just a matter of heating or chemically treating a piece of paper or canvas.

Based on such simple means and household items, invisible ink makes secret communication accessible for everyone. It makes more sense today than a few years ago when software promised better protection.

On closer inspection, after Edward Snowden's disclosure of global digital communication surveillance, analog steganography has always been a good way of protecting one's privacy instead of being merely a playful device. Yes, hackers and crypto activists made military-grade encryption software (PGP, TOR, OpenSSH, VeraCrypt) available to the masses, freely. But Wu knows the issues of their practical use from first-hand experience. As co-host of a series of CryptoParties in Rotterdam – community events that teach everyone the basics of internet privacy and communication encryption – she witnessed again and again how this software asks too much of people with average computer skills. This turned out to be more than simply a problem of education or training, but amounted to a major privacy issue. Lack of technical expertise leading to incompetent use of encryption software – with only one mistake (such as a weak password) compromising security altogether – created an even more problematic situation in which people compromise their privacy, but communicate carelessly because they think they're safe. This not only concerns safety from government espionage, but also data-mining by

internet corporations, blackmailing through cyber criminals, and, increasingly, hacking into the computers and mobile devices of political activists in order to leak all their personal data to public internet forums. This has become a common practice among members of political subcultures like the "Alt-Right" to discredit black victims of police shootings post-mortem and to harass feminist computer game developers and critics.

False sense of security through incompetent crypto use thus makes things worse in the end, similar to a using a self-defense weapon to literally shoot oneself in the foot. Snowden disclosed that anyone in the world who uses strong encryption software, such as the programs mentioned above, is automatically considered a terrorist suspect by intelligence services such as the NSA, will end up on suspect lists and become a target and 'fair game' for interception and wiretapping.

Memory serves as a tactical weapon in this game: Intercepted messages whose encryption today's computers can't decipher in reasonable amounts of time are routinely being archived so that their encryption may be cracked some day in the future when faster computers are available. Under these conditions of a cold info war, Wu's invisible ink works are more than just highly enjoyable pieces of visual art and calligraphic design (and pieces of truly, socially interactive art and design on top of that). As a combination of exhibition works, toolkit manuals and workshops, they are also pieces of practical media research and activism. But most importantly, they give something useful to people. Bypassing internet surveillance by bypassing the internet is no longer a fringe idea. What was begun by artists like Heath Bunting in the early 2000s and extended to filesharing communities by the 2010s – where movies, music and scanned books are increasingly shared Samizdat-style via hard drives and USB sticks to avoid the legal risk of getting caught online – still lacks an equivalent for person-to-person correspondence. Using under-the-radar techniques such as analog steganography for these purposes is not a bad idea at all. This gallery exhibition literally is an experimentation lab for invisible inks and other steganographic techniques, and therefore just the beginning of a practice that is meant to leave behind the space where it is now being shown.

Of course, calligraphic steganography is not a novel technique. The 15th century Voynich Manuscript, a codex of unknown origins written in an unknown alphabet with cryptic floral and half-nude women illustrations, has not been deciphered until today, despite countless intense efforts of professional and amateur cryptoanalysts since 1912, the year of its acquisition through the antiquarian bookseller Wilfrid Voynich. In 2004 and 2016, its current owner, Yale University, published it as photographic facsimile reproductions, first online, and later also as a print book. If the Voynich Manuscript really is a piece of steganography – the practice was common in its time and first described under this name by the German occultist and polymath Johannes Trithemius around 1499 – then it not only demonstrates the resilience of steganography, but also its extraordinary creative potential, visual-tactile richness and eccentricity.

A different way of phrasing this: analog steganography in general, and invisible inks in particular, promise to turn privacy from a nuisance into something more enjoyable. While this might sound overly hedonistic or even lazy, its importance should not be underestimated. Fun with steganography bears genuine political potential because it could be a working counter-narrative to the way corporate apps and hardware gadgets – from Facebook's social networks to Google's GMail and the Android smartphone operating system – make their users trade in privacy for enjoyable user experiences. (Using PGP for E-Mail is neither enjoyable, nor creative, and the intellectual reward of having understood asymmetric key encryption quickly gets stale.)

Non-existent and really-existing obfuscation, fact and fiction, paranoid imagination that turns out to be utter realism – these typical parameters make crypto culture an applied mind game, but limit its social scope. "Cryptography for the masses", a typical activist endeavor, therefore has been doomed to fail and end up as an oxymoron.

Newspaper reports from November 2016 suggest that steganography is now being used in computer malware, embedding the virus code into images on infected computers in order to bypass virus scanners. Antivirus software

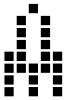
will likely be updated with image recognition algorithms to prevent this in the future. Likewise, invisible ink steganography may no longer fly under the surveillance radar once it becomes widely adopted. (This would be the beginning of a post-digital, post-big data era for intelligence services, following a trend that began in the arts.)

Article 19 of the U.N.'s *Universal Declaration of Human Rights* declares that "everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers". In a time of ubiquitous hate speech trolling combined with governmental-corporate communication surveillance, this concept has been simultaneously hijacked *and* undermined. Despite this, "freedom of expression [...] without interference [...], through any media and regardless of frontiers" still is a sound practical explication of invisible ink experiments. So these words have become a project description instead of a right that everyone has.


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

Florian Cramer
HIDING IN PLAIN SIGHT. Amy Suo Wu's The Kandinsky Collective

PostScript^{UM} #28
Series edited by Janez Janša



Publisher: Aksioma – Institute for Contemporary Art, Ljubljana
www.aksioma.org | aksioma@aksioma.org

Represented by: Marcela Okretič

Proofreading: Philip Jan Nagel
Design: Luka Umek
Layout: Sonja Grdina

pp. 4–5, 8–9
Voynich manuscript, selected pages
Source: https://commons.wikimedia.org/wiki/Voynich_manuscript
p. 13
Amy Suo Wu: *The Kandinsky Code*

Printed and distributed by: Lulu.com | www.lulu.com

Published on the occasion of the exhibition:

Amy Suo Wu
The Kandinsky Collective
aksioma.org/kandinsky.collective

Aksioma | Project Space
Komenskega 18, Ljubljana, Slovenia
18 January–17 February 2017

Supported by the Ministry of Culture of the Republic of Slovenia and the Municipality of Ljubljana.

REPUBLIC OF SLOVENIA
MINISTRY OF CULTURE

City of Ljubljana