Rotterdam May 15 2020

TACTICAL WATERMARKS

Thesis submitted to: the Department of Experimental Publishing,
Piet Zwart Institute, Willem de Kooning Academy,
in partial fulfilment of the requirements for the final examination
for the degree of: Master of Arts in Fine Art & Design:
Experimental Publishing

Adviser — Marloes de Valk
Second Reader — André Castro

Word Count — 8110

Pedro Sá Couto

TABLE OF CONTENTS

I am a privileged student. I have always been part of universities where I had access to paywalled academic journals. The reality in academic publishing nowadays is universities and governments outsourcing the publishing of research papers to private companies such as JSTOR and Elsevier. These journals are maintained within paywalls that demand payment of approximately 30 euro per article, making access practically impossible to anyone who is outside institutions that have a subscription. Strategies such as watermarking are used by these companies to discourage the distribution of proprietary material, making users more liable for their actions. Book publishers enforce similar policies, where customers are not able to share files they have paid for. My research departs from the critical research question — how can publishing bypass surveillance and what counter-measures are playing an active role within this process? I will look into the motivations behind alternative strategies that open access to published material. I will explore established reactive measures that help users evade surveillance in publishing. At the same time, I will question how we can tackle this problem through the reappropriation of digital watermarks.

I will start by addressing how analogue media played a vital role in bypassing surveillance from oppressive regimes. At this moment, the mainstream usage of the internet enables files and political ideas to go viral among bigger audiences. A wide variety of infrastructures exist to publish files that have been made exclusive for a broad diversity of reasons from protected governmental secrets, to copyrighted material. In the first chapter, I will look into extra-legal libraries and archives while questioning the current impact of these spaces and their roles preserving the digital memory of sensitive information.

In the second chapter, I will address how digital surveillance manifests through different channels. In the publishing realm, the primary strategies focus on making users who illegally download, distribute, and make available copyrighted material more accountable and easily identifiable for their online actions. Publishers started to limit access to illegal copies, by appending imprints like the downloader's geolocation, IP address, MAC address, email address, and others. What is the impact of constantly reminding readers they can become targets?

The last chapter will focus on my project *Tactical Watermarks*, where I explore the use of watermarks as alternative forms of anonymisation. This chapter gives an overview of different creative responses, questioning authorship, protecting users' identity and appending evidence of hidden processes required to subvert surveillance in physical and digital media. As a publisher, I always had as my main concern how archives are documented and how provenance is displayed. Converting physical media into digital files is hard, and often information gets misappropriated in the process. With Tactical Watermarks, I reflect on the shreds of evidence that make the ones who download and share accountable. As a response to these strategies of digital surveillance, I question how we can reappropriate and regain control over personal traces.

Bypassing Surveillance

To understand how corporations enforce digital surveillance, we must step back and recognize how censorship and surveillance were deeply connected in repressive authoritarian regimes. The reasons may differ, but tools and goals resemble. Today in China and Turkey, reactive measures *mirror* the present state of surveillance. Actions such as restricting internet access, filtering content, monitoring online behaviour, or even prohibiting internet use entirely are put in place (Kalathil and Boas, 2001). These measures have political agendas, restricting the flow of culture and limiting freedom of speech is a way of avoiding dissent. Online strategies as the use of Virtual Private Networks and internet extensions are playing an essential role in establishing encrypted and secure connections online, providing privacy and helping users to bypass surveillance. These tactics bear a resemblance to how different analogue media shaped parallel streams of prohibited communication throughout history.

After the Second World War, through the 40s and 50s, the Soviet Union made the circulation of art and music from the West illegal, making these kinds of cultural expression extremely limited. Against this, the *stilyagi*, members of youth counterculture in the Soviet Union found a way to bootleg and smuggle western records. While the main problem with DIY vinyl was acquiring the material to use in homemade record presses, a new method consisted of going through hospital dumpsters and collecting used x-ray sheets. Music would then be engraved in this vinyl material x-rays, and the middle hole to fit on the spindle would be burnt with a cigarette. More often than not these types of vinyl would picture old images of bones and medical material, and started to be called *music on the ribs*, and *bone records*, creating space for a black market, leading to a cultural revolution (Grundhauser, 2015).

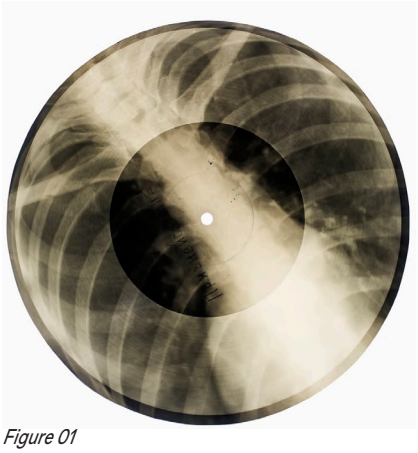

Figure 01
Bone Record (Unknown, n.d.)

During the 60s, within the American, Western European and Asian context, illegal or clandestine publications start to emerge. Dominant governmental, religious, or institutional groups would prohibit any publications that weren't officially approved before publishing (Miles, 2016). The term *underground press* refers to all the underground periodicals and publications that arose associated with the counterculture of the 60s and early 70s. Underground periodicals were inspired by predecessors, such as the *POW WOW*, standing for *Prisoners Of War - Waiting On Winning*. *POW WOW* was a periodical published in Germany during World War II, considered "the only truthful newspaper in Germany", also advised, "to be read silently, quickly in groups of three". Prisoners of war published it in the *Stalag Luft I* camp in Nazi Germany to give insights on what was happening outside of the camp. It ended up being the most circulated daily underground newspaper in Germany during World War II (Smith and Freer, 2012). Another notable endeavour within the phenomena of the *underground press* was the *samizdat* a *do-it-yourself* underground publishing movement that operated in the Soviet Union during the cold war (Kind-Kovács and Labov, 2015). Across the Eastern Bloc, readers would reproduce censored materials

by hand, and these would be passed from reader to reader. Harsh punishments existed to anyone caught possessing these publications. Vladimir Bukovsky gives an overview of this phenomenon as: “Samizdat: I write it myself, edit it myself, censor it myself, publish it myself, distribute it myself, and spend time in prison for it myself.” (Bukovskiĭ, 1988).

POW-WOW

Volume III, Number 14 June 6, 1944

INVASION!

YANKS-BRITISH LAND IN EUROPE!!!

THEY'RE COMING BOYS!

B-u-l-l-e-t-i-n

German Radio, late this afternoon, reported a major naval battle off the coast of Belgium.

Nazi Communique of June 5: "Despite German effort to exclude home from the battle area, American armored formations penetrated to the center of the city in the morning of June 4. Bitter street fighting continued until the evening."

Nazi Communique of June 6: "American armored afore es were repulsed at Vivoli, fourteen miles north-west of Rome. North Compound, evening June 6: Our ground-luther guerillas pushed their e-

Figure 02

D-Day - June 6, 1944 - Front (Kuptsow, 1944)

Inspired by the free press and counter-culture, zine culture started to emerge in the 80s’ within the underground publishing panorama, emancipating print when it comes to overcoming repressive power structure. Zines speak from and to an audience of underground cultures. Zines are self-published media, either with original or appropriated images and texts with small-circulation and small-scale editions. Zines enable almost anyone to publish, making use of photocopiers and mimeographs for cheap and fast print runs. Zines are personal statements targeted to like-minded communities. Their positioning is in between open letters and magazines, almost always not for profit, and even more common; publishers ended up losing money with them (Duncombe, 2017). Zines main thematics are broad, from politics to pop culture. Networking zines also stand out, such as the *Factsheet 5* periodical founded in 1982 by Mike Gunderloy. Networking zines were fundamental to broadcast, index and publicize other zines. As a result helping to spread these DIY publications, contributing by increasing the audiences and the access to such published material, and leading to the beginning of the emancipation of self-publishing as a strong response to repressive regimes.

The circulation of zines is puzzling. Zines circulated among amateurs. Without the negative connotation of the word, *amator* from the Latin was the definition of the ones who love. With all the limitations that zines imply, the ones who were involved, from publishers to readers used this medium as a place to communicate and explore innovative ways of thinking (Duncombe, 2017). Printed zines were passed to hand, and became key to engage within smaller communities. Zines would circulate among trusted people only. This intimate movement of culture was significant when it came to building communities — more than reading texts; zines stimulated meetings between likeminded enthusiasts.

Contrasting fast paced spaces

In contrast to the close circulation of material in zine culture, the way how we circulate content online has changed. Digital media have been responsible for some of the most wide-ranging changes in society over the past quarter-century (Schroeder, 2018). Our notion of control adapted, and our perception of physical spaces may be changing how we perceive distance (Munster, 2011). The website *GeoCities* is an example of this phenomenon, founded in 1994 as *Beverly Hills Internet*, a name that didn't last long. *Geocities* was organized in different regions, "Hollywood" spaces were assigned to webpages dealing with entertainment, and "SiliconValley" to computer-related web-hosted areas. Not only these web spaces started to create a different perception between virtual and real spaces, but communities were also built remarkably inspired by what happened with passing zines by hand. Users navigated within different web spaces organized around shared interests. Webpages were linked in *webrings*, which were collections of sites linked in a circular structure.

Currently, public discourse and discussions happen online. The circulation of media and opinions is now viral. Political statements penetrate internet spaces, a lot of the times hidden, such as through memes. Memes function as a virus, as an easy way to propagate an idea. They are used by both left and right wings to spread political agendas. Memes are used to mask messages, and to evade digital censorship. They play a crucial role in present-day protests and are used by the resistance of today as contemporary political posters (Metahaven, 2014). In China, the *Grass Mud Horse Meme* gained popularity because of its ambivalence. While exploring a dual linguistic feature, it evades digital censorship. In Chinese, when pronouncing *Grass Mud Horse* one way, it refers to an innocuous mythical animal apparently related to the Bolivian alpaca. However, when pronounced another way, it means "*fuck your mother*" (肏你妈) (Wu, 2019).

Figure 03
Grass Mud Horse (russelgz, n.d.)

Analyzing strategies that enable access

On July 5 1993, *The New Yorker* published a cartoon from Peter Steiner where we can read, "On the Internet, nobody knows you're a dog" (Steiner, 1993). It pictures two dogs interacting, and one is behind a computer. It symbolized the understanding of internet privacy, where users could interact with a certain degree of identity anonymity. Now, it is different, the use of nicknames and pseudonyms is not as present, and a user must display their real identity. Not only the use of a name is enforced, but it is almost mandatory to connect a face to this name. As an example, Facebook demands real names, abandoning pseudonyms and making us use our real identity. Mark Zuckerberg, CEO of Facebook, even defends this position stating that portraiting two identities is an example of a lack of integrity (Kirkpatrick, 2012).

"On the Internet, nobody knows you're a dog."

Figure 04
On the Internet, nobody knows you're a dog (Steiner, 1993)

Corporations neglect users' right to privacy. Technology to surveil and control the individual is expanding. Users are more liable for what they consume and share online. At the same time, companies become less accountable for what they do with users data (Mann, 2003). Lawrence Lessig points out that both in privacy and copyright users lost control over their data. There is a dire need for stricter regulations protecting users privacy, yet nothing is happening. When it comes to copyright protection on the other hand, companies have pushed for regulations and have gotten their way (Lessig, 2008). When comparing these two interests, the right to privacy is not protected because the parties interested lack power and influence, unlike the entertainment industry who has the authority, the power and the means to demand change.

Strategies to create access to copyrighted materials and protected research journals started to emerge. Because researchers were bumping into expensive paywalls that were unaffordable for many, tactics were put together to make research widely available. Online spaces such as archives and extra-legal libraries provide areas to access media through alternative channels, and their structures play a crucial role in who gets to access them. Users are filtered, restricting access to certain communities, protecting them and enabling curators to answer more specific needs. This user filter is implemented using tactics, such as invitations, or requiring particular technological knowledge. When thinking about extra-legal publishing streams, we have to consider how these shape the way different digital files are accessed and by which audiences. What are the available strategies and resources that enable public access? I will introduce infrastructures, policies, and tactics that protect the ones who host and make use of such platforms. Within shadow libraries, libraries that exist in the margins of the law, different systems exist; from public shadow libraries, where everyone is allowed to download and upload digital material to more restricted libraries where proxies and invites are required.

Library Genesis started in 2008 as a successor, from *library.nu*, previously *ebooksclub.org* and *gigapedia.com* even before that. Between 2008 and April 2014, this library grew at a fast pace, with 1.2 million records by 2014 (Balázs, 2018). The website owners describe themselves as "random book collectors", they don't focus on curating materials and don't accept file requests. The topics are broad: from economy and geology to housekeeping. All users are encouraged to upload and download content. There's no score to maintain, necessary log-in, or price to pay. The platform regularly fights against shut-down attempts. Strategies, to increase the lifespan of the collection are put in place, such as encouraging the creation of *mirrors*. *Mirrors* allow hosting voluntary copies of entire collections or parts of them over different servers and points of access, making these more challenging to control. Within their context, they seem to distance themselves from the idea of bringing academic research for people without access. Although this vast library supposedly gathers information without any specific methodology, the reasons behind it look more as a political statement against copyrighted material rather than trying to please a particular

crowd. The focus on dimension rather than curation provides clues to their primary goal, publishing the most proprietary content as possible, dissolving the idea of ownership. The main page of the website links to a letter of solidarity demanding for action, a manifesto for standing up for what they believe in, incentivising the dissemination of knowledge.

> *We find ourselves at a decisive moment. This is the time to recognize that the very existence of our massive knowledge commons is an act of collective civil disobedience. It is the time to emerge from hiding and put our names behind this act of resistance. (Custodians, 2015)*

aaaaarg.fail is a shadow library that stands out because of the demographics of its users. It is mainly used by researchers, academics, students and people interested in theory. To become a member, you need to get invited, and it might feel like you are in a private club, where you don't spot any advertising or demands for donations. Strategies, such as incorporating RSS: creating a panel where users can discuss and displaying a contact list on the landing page allows users and maintaners to connect more closely. As a member, you can not only upload and download but also request new titles through a messageboard, augmenting the sense of community and solidarity that exists in this online space.

Libraries like *The library* and *Clockwise libraries* operate within the *dark web*. Standard web engines do not index their content. Instead, these libraries are indexed in specific web pages just as *http://mx7rwxcountermqh.onion/*. In this index, you can find an annotated list of URLs, with a small description on the focus of each space. These libraries are harder to come across; you have to use Tor, the onion browser to access them. They work as webrings, and this brings a sense of community to the numerous projects found. Such archives appear to be personal libraries as *Pokedudes Archive of Interesting and Odd Files*, a place where they curate what is described as being "a small list of weird or interesting files".

A more informal system of file sharing is a Facebook group titled, *Ask for PDFs from People with Institutional Access*. It brings the ones who are part of an institution and the ones who are not and cannot afford research papers together. The use of centralised social media to create an accessible community of scholars is fascinating. The appropriation of Facebook groups' design features, such as the cover picture, is compelling. In this area, they display a graphic (see figure 05) to help guide newcomers. This group transforms the act of sharing copyrighted material less specific to a hacker community and banalises it. The workflow is as simple as if you were part of this group, you post asking for a pdf you need. Users interested in getting the same item comment "F" on the post, which stands for following. Due to the design of the platform, if you comment you will be notified whenever there is activity on the post. It is an informal community of academics, sharing items among themselves, uploading pirated material to this platform and creating a social library.

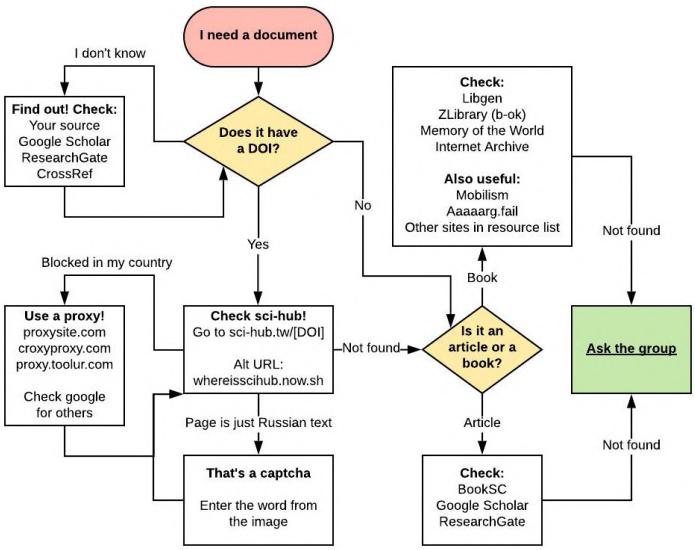

Figure 05
Cover picture: Ask for PDFs from People with Institutional Access (Unknown, 2019)

Apart from shadow libraries, systems such as archives that document and organize perishable sensitive information also exist. *MayDay Rooms* is an example where infrastructures and counter-strategies demanded to publish experimental culture, play equal parts. *MayDay Rooms* is an educational charity founded as a safe haven for historical material linked to social movements, experimental culture and the radical expression of marginalized figures and groups. It was set up to safeguard historical documents, and it is not only a digital archive. Online users can browse a catalogue and read pdf's, but *MayDay Rooms* also deals with physical items. The home for this archive is the *Birmingham Daily Post's* former London office refurbished in 2012 and 2013. This building is not only used as space to hold material, or as an infrastructure to its digital archive. It also offers communal areas, such as reading, meeting and screening rooms and a canteen. It is a place for informal researching, gathering, and activation of the social aspect of the archived materials, for example, by digitizing and distributing them online (MayDay Rooms, n.d.).

After looking into shadow libraries and digital archives, strategies to distribute and preserve copyrighted material, their users and the political agendas behind them, my research will delve deeper into the phenomenon of watermarks. Watermarks are often used to identify file owners' as sources of copyrighted material, intimidating them, raising concerns of liability, and as a result, discouraging sharing. I will focus on this tactic of protecting intellectual property and expand on how this technique is negatively impacting the sociability that comes with sharing texts and restraining the flow of files within online digital spaces.

Background on Watermarking

The internet as a carrier of digital media changed how we share music, books, video and other media. The integration of digital watermarks is becoming more popular to fight the fast-paced spaces opened to share pirated material. Currently, the research on watermarks predominantly focuses on strengthening security; embedding robustness with respect to compression, image-processing operations, and cryptographic attacks (Shih, 2017). We now understand watermarks as being both digital and physical, but they are not a new phenomena.

The art of papermaking has its roots in China in the 1st Century. The process was first documented in 105 A.D. and ascribed to Cai Lun (Basbanes, 2014). Watermarks only appeared later in 1282. Watermarking happens during the process of making a sheet of paper whilst the paper is still wet. Watermarks are a result of changing the thickness of a specific part of the paper, creating a highlighted area and as a result, its shadow. We track the beginning of watermarks in the town of Fabriano (Hunter, 1987). It is essential to acknowledge the historical importance of the Italian city of Fabriano. From the name *Fabriano*, in Latin *Faber > Făbrĭcĭus*, meaning *craftsman*, *artificer*, *maker* (Latdict, n.d.). The practical skills in forging metal and shaping wire were crucial for building the frames used to remove excess water, gather the pulp and to start forming the first sheets of paper.

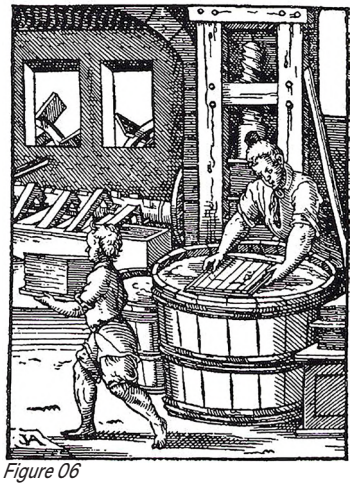

Figure 06
Papermaking (From The Book of the Trades) (Amman, 1568)

Watermarks analogue Intention

The history of watermarks is still relatively obscure. It is not possible to fully trace back their ancient significance. A few different theories have been discussed on the actual purpose and use of these venerable imprints. One that I came across with was to help with the production of the sheets of paper. Watermarks were used to identify the size of a frame and leave an imprint in the produced output (Hunter, 1987). Another hypothesis is that the craftsmen working in the production of paper were illiterate. Watermarks were then a strategy of appealing with pictures or symbols. Communicating in this way would lead to a smaller chance of creating misunderstandings. The first applications of watermarks compel these possibilities, but it is also possible that these might have been an artistic production of the papermakers. Watermarks can also be no more than a fashionable imprint left by the artists making the frames, as a way to identify themselves, creating an aesthetic enhancement or a signature of quality (Watkins, 1990).

Watermarks establish provenance to manufacturers of papers, paper mills and manuscripts. Across Europe, Africa and the Middle East their use contributed to increasing the desire for specific papers and was a critical factor in recognizing paper quality. Nowadays, watermarked sheets carry pieces of evidence documenting their lifespan and transactions.

It is wrong to immediately establish the provenance of a book to one particular place solely based on the watermarks due to the commercial trades of paper. While an Italian watermark may be found in a sheet of paper, this only sets provenance to where the paper was manufactured and not its afterlife. Watermarks would comprise graphics such as animals, plants and sacramental imagery but were also representations of geographical territories and in general depictions of Western culture. In Umbria, Italy, for example, the Benedictine monasteries endorsed the 3-hilled mount topped with a cross as their symbol. Developed by the French and Venetians, we identify watermarks imagery of the tre lune/ three crescent moons. These strategies were adopted because of Muslims in the Ottoman market. They were expected to choose in favour of papers with these kinds of imagery rather than Christian motifs (makingmanuscriptsblog, 2017).

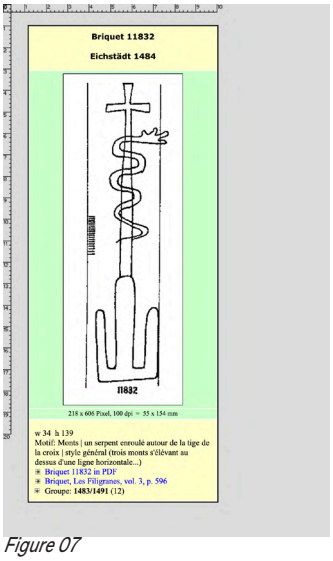

Figure 07
3 Mountain Hill, Snake and Cross (Österreichische Akademie, 1484)

Connecting watermarks and library stamps

There is an active link between watermarks and the introduction of library stamps — both creating a body of evidence when trying to establish connections in a collection. Library stamps are also perceived as an imprint left visible, sometimes glued, and able to question property and acquisition. In libraries, books are stamped to declare ownership, establishing a physical relationship between the physical medium and the infrastructure. At the same time, traces of provenance are added to these collections. Library stamps do not associate a reader to a book, nor did they intended to do so, the focus is on documenting circumstance and date of acquisition.

Though library stamps are helpful to determine the time frame and history of an item in a collection, the process of stamping a book is not necessarily performed when they enter a collection. Unlike watermarks where it is unlikely that the act of tempering the paper fibres doesn't occur simultaneously to when a paper sheet is made, stamps were commonly applied at a later date than acquisition. This lead to mistakes that are now widely recognized. Alongside with stamps, to build a body of evidence for determining both the circumstance and date of acquisition clues may be found on bindings, bookplates or inscriptions (Duffy, 2013).

Figure 08
Left: Oval hand stamp for manuscripts with the words BRITISH LIBRARY.
Centre: India Office hand stamp for non-small 'claim material' items. These items were treated as part of the British Library collection.
Right: Library stamp from previous Oriental and India Office Collections. Use of this stamp ceased on 1 September 2005 (Unknown, n.d.)

Watermarks got more relevant with the introduction of paper currency. One of the notable shifts identified is when they were first applied to banknotes in England, by a papermaker named Rice Watkins in 1697 (Mockford, 2014). Watermarks were added as a way to deter counterfeits and to make the act of forging more difficult, enabling easier targeting to the ones who were doing it. In England, 1773, the death penalty was extended to those who would create watermarks with the name of the Bank of England.

Just as in paper money, watermarks are now used to establish authenticity and their digital implementation, started to get more popular. Emil Hembrooke patented the first digital watermark, "Identification of sound and like signals", US Patent 3,004,104 Filed 1954, Issued 1961. In the US patent, we can read: "The present invention makes possible the identification of the origin of a musical presentation and thereby constitutes an effective means of preventing such piracy" (J. Cox and L. Miller, 2002).

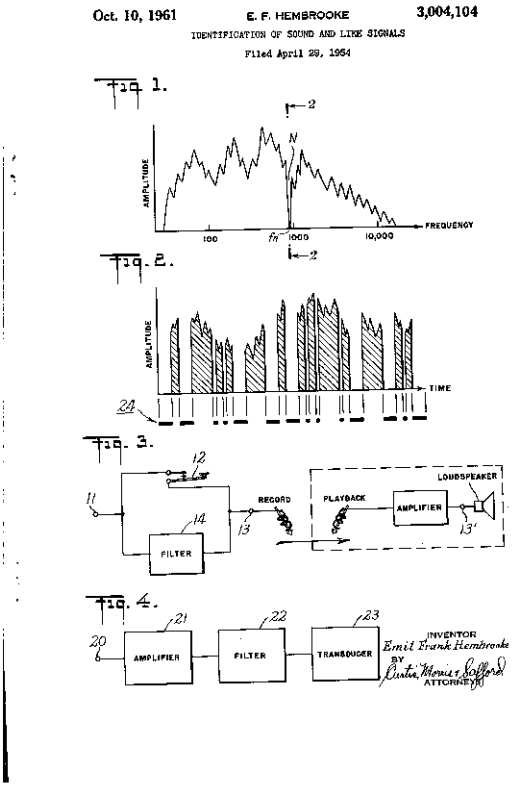

Figure 09
Identification of sound and like signals Patent (Frank, 1954)

In the 90's the interest in watermarks increased drastically. Currently one can find them in various forms of copyrighted watermarked material. As most information and data are stored in digital formats and not in physical ones, providing legitimacy and proving authenticity is progressively representing a more urgent task (Shih, 2017). Digital watermarks are mostly known as being visual. The normalization of their use in photographs, and on video stored on DVDs is a reality by now. In trial software, these also appear often. Instead of restricting the use of a programme, while exporting the final version of the work watermarks are appended. I read this action as an arrogant way of advertisement and making users a commodity. Instead of profiting from software licenses, users are indefinitely broadcasting companies logos within their work. This technique is enforced to deter the use of trials and provides only one option; it forces the ones who need the software to buy it.

Another significant shift on the use of watermarks happens with their appropriation in the publishing business. Watermarks are now used to create a body of evidence on users, adding traces that relate to the subject more precisely with geolocation, IP addresses, MAC addresses, email addresses, etc. An excellent example of this phenomena is the enforcement by Verso Books publisher. Their books are sold in an online ebook store where they append a new page in the beginning of each file with the downloaders' name and his or hers email address. It also watermarks the IP address of the downloader in the footer of the first page of every chapter.

I stumbled across the article *Verso Books Shows That it is Possible to Use Customer-Friendly DRM While Still Calling Customers Pirates* by Nate Hoffelder about different forms of DRM during my research. In this article, the writer starts with a disclaimer where he portrays himself as "a supporter of milder types of DRM like digital watermarks" (Hoffelder, 2014). What caught my attention was how the mode of address changed when he starts to identify all the unnecessary strategies implemented by *Verso Books* in their ebooks. More important, we can understand that their watermarks didn't pass unnoticed to the store users. A source interviewed states: "Personally, I felt like I was constantly being sent a stalker's note saying, 'I know where you live.' It put me off reading the books entirely." (Hoffelder, 2014). The increase of imprints that identify us as downloaders and as printers is alarming. Verso Books are calling out their users as pirates and companies, such as BooXtream are making this possible, using us as an asset to capitalize on.

I was able to identify the company that develops the watermarks for *Verso Books*. It is a Dutch DRM company called *BooXtream®*. It is worrying how they portray themselves; the first quality that they promote about their DRM methods is traceability. We can read in a bold font: "A publication that has been BooXtreamed can be traced back to the shop and even to the individual customer." (BooXtream, n.d.). Watermarks are now perceived as something to fear, and make us feel uncomfortable. Surveillance might be quickly spotted as it commonly happens with CCTV because we can establish a physical connection with it, we can see it, we can choose a different path to walk from it or even try to disguise ourselves. We can accept that digital surveillance is a reality, but we don't feel a close connection to it just yet. Digital watermarks might be the vehicle establishing this direct connection. It is still tricky, though, to predict what will be the impact of these techniques if users are afraid to share an ebook they have bought.

Surveillance in publishing not only manifests itself in obvious ways. The *Electronic Frontier Foundation* published an article, raising awareness of the Machine Identification Code. First published by PC World as *Government Uses Color Laser Printer Technology to Track Documents* in 2004, this code is formed by a pattern of dots appended by the printer's software to every printed page. These are almost imperceptible yellow dots carrying information as the date of print, time, and the serial number of the machine. Similar technology is used when you try to scan a banknote. A sequence of printed yellow dots in the paper triggers the printer to overlay a striped pattern on the top of the copy, preventing duplications.

I tried to understand if this code was still in use, and I had to be able to prove its existence. I started by using methods to identify these invisible dots, such as UV lights, different printers, from *HP* to *Canon* and from Inkjet to Lasers printers. Almost when I was giving up, disappointed with all the time invested in this, I started to reverse engineer this code and implementing my own. While creating messages printed in minimal font size and scanning these printed pages, I began to understand how to make this pattern visible. With a new scanner with a resolution of 1200 dpi, and after inverting the document colours, the dots suddenly appeared. Just as by magic, a mesh of my experiments and the tracking dots started to emerge. Ultimately, I was able to identify them in all the school printers in the Blaak building. It is worrying that this hidden code infiltrates documents and can be seen by anyone. It is not only used if you are suspect of a crime, but it is

available for everyone at all times. Coming across them made me rethink what it means to publish through printed media, how safe is it, and how it affects the ones who depend on these forms of publishing.

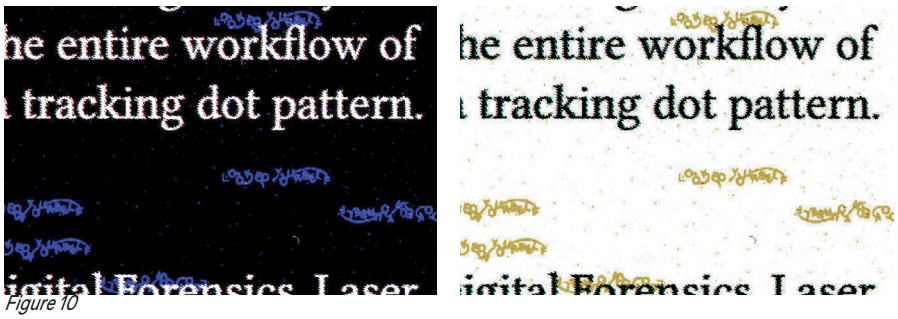

Figure 10
Tracking Dots found in the university printers (Sá Couto, 2019)

During this second chapter, I explored the progression of watermarks. From their background, until their appropriation, as an asset to incite fear, self-awareness, and to remotely control and constrain user actions. It was essential for the development of my project to emphasize the current value of ancient watermarks. During the next chapter, I will expand my research from the point of view, where I consider the early framework of watermarks necessary to resurface. I desire to demonstrate that what lies at the heart of their use is the ability to portray crucial interrupted actions and moments in history, granting insights into hidden processes of fabrication, documented in the sheets of paper. And at the same time carrying clues to comprehend their artisans, the historical timeframes and different imagery. I will then expand on the use of digital watermarks apart from what I recognize as their misappropriation, exploring that the current attitude towards digital watermarking is not the only valid one. I focused my research on how the discourse around these reinforcements of copyright can be flipped around. I will delve into the tactics that seem mainly negative and re-reappropriate them.

Introduction to my creative response

My project, *Tactical Watermarks*, is an online republishing platform. I actively make use of digital watermarks as a means to explore topics such as anonymity, paywalls, archives, and provenance. I describe ways of living within and displaying resistance against a culture of surveillance in publishing. It is relevant to understand and explore what it is living in a culture of constant tracking, rather than aiming to solve the many problems of surveillance.

In this platform, users can upload and request different titles. While talking with enthusiasts from the *Library Genesis forum*, I understood the need to create a tool that allows people to share watermarked pdf's in a safe way. My platform is not a library, and it is also not an archive. I don't keep the files or intend to archive them. What I will open is a space to de-watermark files, and append new anonymous watermarks with the technical and personal regards around sharing specific texts. In the end, these stories will circulate alongside the main narrative. This is an automated republishing stream that enables me to spread the produced files to different libraries, from *aaaaarg.fail* to *Library Genesis*.

My use of watermarks and more specifically, my creative response, has the primary objective of creating a positive discourse around the act of watermarking. This discourse will enable the creation of a top layer of information, able to embed traces of provenance in different texts. By provenance, I intend to express all the trails not used to surveil users but the ones able to trace historical importance to files and that facilitate precise documentation within an archive or library. Tactical Watermarks is not only a theoretical system, but I will also delve into how it can be deployed, comparing it to other projects or approaches that I have encountered, and reflect over their influence in my practice.

I wanted to challenge centralised distribution channels and wondered on how the process of adding stains can be twisted and revived. Stains are what I will call user patches or marks that are difficult to remove and that do not play an active role in archives. While exploring the process of adding imprints, different uses arose: as a way to obscure previous ones, of commenting on the situation and encouraging behaviours, to create relations and communities, augmenting the sense of solidarity in archives, for digital enhancements, marks of quality, etc.

I aim to link my creative response to what has been happening in parallel within different cultures, from graffiti culture to other controversial artistic practices. Watermarks may form a discourse around topics such as anonymity, borders, archives, and provenance. While rethinking watermarks, I explore their hidden layers and aspects of surprise, visibility or invisibility, on different forms of communication. It is essential to acknowledge that watermarks have the power to infiltrate, perform different roles and create parallel streams of information within various texts. When it comes to publishing, how can watermarks create a critical discourse around the right to access knowledge and represent the ones that fight for it?

1 — Displaying provenance of a medium

I will start by consolidating how I will use the term provenance. By provenance, I unify all processes that provide clues and evidence from the origin of a file, until the moment it enters a collection. These traces may identify the source of a text, its place of origin, or even the motivation behind why an individual made it public. All these voices will be unified as part of a stream of empathy, decisions, hidden tasks, and actions.

The flow of texts, downloads, and users is always constrained by the politics of platforms that grant access and disseminate them. Different platforms share the same documents and versions of a file. With Tactical Watermarks, I aim to document this hidden activity and make it visible. With watermarks, and without compromising on the users' identities, I aim to set ground to what I find noteworthy. Such as finding ways to translate the movement of users and texts, within this complex mesh. To achieve this, I aim to materialise the hidden tasks behind the process of uploading a file to a digital space. These actions may compel, processes such as digitising, or even the motivations behind the selection.

2 — Signatures

In Tactical Watermarks, I also propose that digital watermarking may be used as a signature, as in graffiti culture or *crack intros*.

Just as distributing copyrighted material and cracking software, graffiti is controversial. It has a rich background dating back to several cultures like the Egyptians, Greek or Romans, where writing or drawing in walls or other surfaces was common to be found. Graffiti is seen as a form of artistic expression without permission. Simultaneously, in crack intros, we can discover pseudonyms to protect identities and thwart prosecution, in graffiti, a subculture to challenge authority, the same thing happens.

In *Crack intros*, such signatures referred to as "crack screens" were customarily included in-game title screens displaying the game name, the logo of the producer, and a graphic that provided the player with a glimpse of the game theme. *Crack intros* appeared for the first time in the '80s and were not commissioned for a commercial purpose. Instead, these were introduced by a programmer or a group of coders, graphic artists, and musicians that were responsible for removing the software's copy protection and that made a crack public (Green, 1995). The signatures were initially simple statements, such as "cracked by …", sometimes intentionally misspelt as "kracked by …" (Reunanen et al., 2015). While crack intros are in many ways similar to graffiti, crack-intros invaded the private sphere and not the public space (Cubitt and Thomas, 2009).

A link between these forms of signatures and watermarks is found in their ancient imagery. Craftsmen would explore pseudonyms, in this case, in the form of pictograms built in the paper frames. This forms of anonymity open a path to explore digital watermarking as an arrogant way of identifying users as liable for the processes and decisions behind realising a file into the public sphere, without carrying any liability whatsoever. Tactics as using pseudonyms will be reappropriated to challenge authority, digital identity and accountability.

3 — Watermarks to obscure

Tactical Watermarks is not only about revealing hidden layers and augmenting the memory of an archive. It is also about creating strategies to suppress unwanted information. It is valuable to stress that in the contemporary panorama of digital watermarking, calling out to a user identity is the ultimate goal. While recognising the intention to remove this layer of information, it is relevant to create parallelism to the project *SecureDrop*. This project was first released under the name *DeadDrop*, designed and developed by Aaron Swartz and Kevin Poulsen. *SecureDrop* is a free software platform that enables safe communication between whistleblowers, journalist and different organisations. In this platform, whistleblowers, which are the sources, submit documents and data while avoiding most common forms of online tracking (Ball, 2014). During this process, sources are also assigned a random user name, allowing a journalist to contact and privately chat with them.

The main intention of both my project and *SecureDrop* is the creation of strategies to anonymously disseminate files not intended to be part of the public sphere. Both facilitate a place where users anonymise data; *SecureDrop* mostly deals with private or public organisations trying to protect secrets and as a response whistleblowers trying to get them out. Tactical Watermarks will deal with publishers protecting copyrighted material and readers seeking to share them with their peers. In *SecureDrop*, this happens by using private, isolated servers, and using encryption and decryption tools. In Tactical Watermarks by using watermarks as a way to obscure already existing imprints aimed at making users accountable, overlaying new ones, and re-writing new subjective metadata to documents.

4 — As a means of expression

Within this framework, through the act of watermarking, I will create a space to publish undercovered personal, political and other kinds of messages. With my creative response, I consider users commenting and publishing their thoughts disseminated person-to-person with the actual circulation of a file is relevant. Having the power of saying that I am here, and I disagree with how paywalls, borders, and how rules are structured and reinforced is compelling and pertinent. These messages must be public.

Commenting as a strategy of contemporary political resistance also happens in cracked software, such as *Adobe Zii*. *Adobe Zii* or *Adobe Zii Patcher* is a one-click software program patcher or activation tool for Mac. The developers of this software inserted the quote “why join the navy if you can be a pirate” during the actual process of patching the desired software. It is striking how this discourse differs from the one seen in *Crack Intros*, commenting on a situation and encouraging provocative behaviours. The reference is established through the act of patching rather than exposing the individuals behind it.

Watermarks will be used to reflect on power structures and to disseminate beliefs related to struggles within free access to knowledge and information. By infiltrating new digital watermarks, we are not only able to reach the ones that are already fighting within this culture, but also the ones that might be uninformed users of shadow libraries and alternative publishing streams.

During the first chapter of this thesis, I have explored how different media are used to bypass surveillance and to publish within alternative streams of access. This used to happen through zines, the underground press or other types of publishing as the samizdat. Currently, parallel publishing streams exist mainly in the form of digital online platforms, maintained to make public all sorts of copyrighted and forbidden material. Within the context of Tactical Watermarks it seems relevant to delve further into strategies that facilitate communication, especially the use of steganography.

Even though several forms of communication responsible for avoiding conventional methods of surveillance are mainly achieved by writing encoded messages and by the use of decoding systems when they reach their target, with steganography, this happens differently. The message is hidden in plain sight as the main strategy. Steganography allows two parties to broadcast a message hidden or disguised as other data. Watermarks and steganography both happen in digital and analogue formats. While both terms can be applied to the transmission of information hidden or embedded in other data, they are often wrongly merged and it is vital to clarify them. Steganography relates to undercover point-to-point communication between two parties. Watermarking has the extra demand of robustness towards potential attacks (Katzenbeisser and Petitcolas, 2000).

Steganography is a subdiscipline of information hiding. In the book, *A Cookbook of Invisible Writing* by Amy Suo Wu, alternative forms of communication are published in the format of recipes documenting techniques borrowed from spies to prisoners, but not only old tactics of steganography exist. In China, researchers understood that while digital communications and data security are becoming more sophisticated, there is still the need to develop ways of sending hard copy messages securely. Scientists developed a printing technology which can only be read with a UV light over the printed medium (Davis, 2019).

All these techniques of communication led me to explore which strategies we can reappropriate using watermarks as a way of annotation. How can we open space for communication between users of a system while maintaining their anonymity? One might have felt the thrill when a downloaded file from *Libgen* or similar library still contains traces of previous users. Relating, through such traces, to someone we don't know can be quite amusing. You feel part of a movement, as you had a glimpse of a moment, captured in time.

With Tactical Watermarks, I will open a space for dialogue, as well as, demonstrations of solidarity. I do not plan to make this something you may find by chance; I aim to explore the possibilities of making someone thrilled to see these messages as a compulsory or a regular habit.

At last, digital watermarks still have space to produce sensorial enhancements. Enacted through watermarking and with a background in the practice of graphic design, I reckon that we can establish different rhythms and hierarchies within a narrative. Just as introduced earlier in this text, watermarks might have had their origin concerning manufacturing processes, but they might have been an artistic expression by papermakers as well. Within Tactical Watermarks, digital watermarks may substitute the impact that graphic design has in the process of creating books as a physical medium, where they can be recognised as an object by themselves.In graphic design, choices such as the paper, the binding, or even how different chapters are separated become part of an endeavour to heighten the narrative. Mixed attitudes exist in this process, either by trying to respect the narrative, without overpowering it, but also, as a way of exploring it as a medium where restructuring may form new ways of reading. Two constants are then present, the exploration of repetition, its absence, and the experimentation regarding reading flows.

The main drive during this research was to explore how analogue techniques can be appropriated and transported into digital watermarking. I find particularly amusing unconventional strategies, such as the use of scented paper in print. Such methods allow us to rethink the flow of information and take part in shaping the perception we have from texts. Through this scented technology, we explore the vision and the scent at the same time, transporting us to different realities, creating a stimulus that we don't usually experience while reading. In digital files, I compare this to the feeling of encountering graphic elements that exist outside the main narrative. While most digital files lack personality, with new visual elements appended, I aim to incite new sensation while building new experiences through paratextual components.

CONCLUSION

Delving into tactics enforced by organisations that close access to published material could have been discouraging. But it wasn't. While companies are investing money to protect their sources of income, it is exciting to feel that volunteers continue to be motivated to create reactive measures against closed access publishing. Throughout this text, I have unpacked the reactions regarding digital surveillance and the motivations behind these countermeasures. Every time that we make use of such projects, they seem like finished products, where no effort from our side is necessary to make them work. This thesis aimed to create a space to introduce some of the platforms, tools, and users that contribute and exist behind projects that make access widely available.

My project, Tactical Watermarks, is motivated by all the invisible individuals behind alternative publishing platforms, from curators, the ones who host, upload and even download material. With my creative response, I intended to create one more tactic to bypass surveillance in the publishing realm. Though, it does not try to be the foolproof answer to opening access to published material. It is reassuring to feel that a wide variety of infrastructures, from shadow libraries to online digital archives already exist as temporary solutions to the main problematic. It is also comforting that users display daily acts of voluntary resistance amongst them, from researchers creating informal groups to share copyrighted material to users *mirroring* collections in attempts to extend their life span. My project starts focused on acknowledging the importance of informal communities of resistance and on the individuals that make this possible. Tactical Watermarks reflects on the social, political and cultural aspects behind the use of restrictive measures in publishing. It is not a finished project, and it doesn't intend to be, it embraces that the possibilities of tactical watermarks will continue to reveal themselves through the extensive use of the tool.

Researchers need to react against the organisations creating monopolies and closing access to published material. We need to build new online spaces where people can connect. Users need access to online forums where counterstrategies are widely available. We need to organise workshops and build communities to bypass the control of corporations only focused on the monetary outcome from research. It is important to continue sharing texts and opening access to our resources collectively. We need to *mirror* collections and produce new and unpredictable reactive actions against closed publishing streams. When it comes to opening access to paywalled material, a lot is yet to be done. Tactical Watermarks is a way to stimulate new reactive measures, embracing a positive discourse when it comes to subvert digital surveillance.

REFERENCES

Balázs, B. (2018) *"Library Genesis in Numbers: Mapping the Underground Flow of Knowledge." In Shadow libraries: access to educational materials in global higher education*. Ottawa : International Development Research Centre: The MIT Press.

Ball, J. (2014) *Guardian launches SecureDrop system for whistleblowers to share files.* The Guardian, 5 June. Available at: https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents (Accessed: 24 October 2019).

Basbanes, N.A. (2014) *On paper: the everything of its two-thousand-year history*. New York: Vintage Books.

BooXtream (2019) *BooXtream: Social DRM To The Max.* Available at: http://www.booxtream.com/ (Accessed: 2 March 2020).

Bukovskiĭ, V.K. (1988) *To build a castle: my life as a dissenter*. Washington, D.C.: Ethics and Public Policy Center.

Cubitt, S. and Thomas, P. (2009) *Re:live Media Art Histories 2009 conference proceedings*. Melbourne: The University of Melbourne & Victorian College of the Arts and Music.

Custodians (2015) *In Solidarity with Library Genesis and Sci-hub*. Available at: http://custodians.online/ (Accessed: 7 February 2020).

Davis, N. (2019) *Scientists invent new technology to print invisible messages. The Guardian*, 25 September. Available at: https://www.theguardian.com/science/2019/sep/25/scientists-invent-new-technology-to-print-invisible-messages (Accessed: 30 October 2019).

Duffy, C. (2013) *A Guide to British Library Book Stamps: Collection Care blog*. Available at: https://blogs.bl.uk/collectioncare/2013/09/a-guide-to-british-library-book-stamps.html (Accessed: 12 October 2019).

Duncombe, S. (2017) *Notes from underground zines and the politics of alternative culture ; with a new afterword: Do zines still matter?* Portland, Or.: Microcosm Publishing.

Green, D. (1995) *Demo or Die! Wired, 1 July.* Available at: https://www.wired.com/1995/07/democoders/ (Accessed: 10 January 2020).

Grundhauser, E. (2015) *Soviet Scenesters Used X-Rays to Record Their Rock and Roll*. Available at: http://www.atlasobscura.com/articles/soviet-scenesters-used-xrays-to-record-their-rock-and-roll (Accessed: 30 January 2020).

Hoffelder, N. (2014) *Verso Books Shows That it is Possible to Use Customer-Friendly DRM While Still Calling Customers Pirates.* Available at: https://the-digital-reader.com/2014/06/07/verso-books-shows-possible-use-customer-friendly-drm-still-calling-customers-pirates/ (Accessed: 17 November 2019).

Hunter, D. (1987) *Papermaking: the history and technique of an ancient craft*. New York: Dover.

Miller, M. and Cox, I. (2002) *The First 50 Years of Electronic Watermarking. EURASIP Journal on Advances in Signal Processing*. doi:10.1155/S1110865702000525.

Kalathil, S. and Boas, T. (2001) *The Internet and State Control in Authoritarian Regimes: China, Cuba, and the Counterrevolution. First Monday, 6*. doi:10.5210/fm.v6i8.876.

Katzenbeisser, S. and Petitcolas, F.A.P. (2000) *Information hiding techniques for steganography and digital watermarking.* Boston: Artech House.

Kind-Kovács, F. and Labov, J. (2015) *Samizdat, tamizdat, and beyond: transnational media during and after socialism*. New York: Berghahn Books.

Kirkpatrick, D. (2012) *The Facebook Effect: The Real Inside Story of Mark Zuckerberg and the World's Fastest Growing Company*. London: Virgin Digital.

Latdict (n.d.) *Latin Definition for: faber, fabri (ID: 20146)*. Available at: https://latin-dictionary.net/definition/20146/faber-fabri (Accessed: 25 November 2019).

Lawrence, L. (2008) *Code : And Other Laws of Cyberspace, Version 2.0.* New York: Basic Books. Available at: https://www.worldcat.org/title/code-and-other-laws-of-cyberspace-version-20/oclc/1109503030&referer=brief_results (Downloaded: 3 February 2020).

makingmanuscriptsblog (2017) *Watermarks! Making Manuscripts in the Medieval and Early Modern World.* Available at: https://makingmanuscriptsblog.wordpress.com/2017/10/02/watermarks/ (Accessed: 11 December 2019).

Mann, S. (2003) *Existential Technology: Wearable Computing Is Not the Real Issue!* Leonardo, 36 (1): 19–25.

MayDay Rooms (n.d.) *MayDay Rooms: About*. Available at: https://maydayrooms.org/ (Accessed: 13 November 2019).

Metahaven (2013) *Can jokes bring down governments?: memes, design and politics.* Moscow: Strekla Press.

Miles, B. (2016) *The Underground Press*. Available at: https://www.bl.uk/20th-century-literature/articles/the-underground-press (Accessed: 31 October 2019).

Mockford, J. (2014) *"They are Exactly as Banknotes are": Perceptions and Technologies of Bank Note Forgery During the Bank Restriction Period, 1797-1821.* Available at: https://pdfs.semanticscholar.org/001e/004f8e526855afe09f-cb674b8ba1d9cd602f.pdf.

Munster, A. (2011) *Materializing New Media: Embodiment in Information Aesthetics.* Lebanon: Dartmouth College Press. Available at: http://grail.eblib.com.au/patron/FullRecord.aspx?p=1085079 (Downloaded: 19 November 2019).

Reunanen, M., Wasiak, P. and Botz, D. (2015) *"Crack Intros: Piracy, Creativity, and Communication." In International Journal of Communication*. pp. 798–817.

Schroeder, R. (2018) *"The internet in theory." In Social Theory after the Internet. Media, Technology, and Globalization*. UCL Press. pp. 1–27. doi:10.2307/j.ctt20krxdr.4.

Shih, F.Y. (2017) *Digital watermarking and steganography: fundamentals and techniques*. Boca Raton: Taylor & Francis, CRC Press. Available at: http://www.crcnetbase.com/isbn/9781498738767 (Downloaded: 25 November 2019).

Smith, M. and Freer, B. (2012) *The POW WOW Newspaper.* Available at: http://www.merkki.com/powwow.htm (Accessed: 9 February 2020).

Watkins, S. (1990) Chemical Watermarking of Paper. *Journal of the American Institute for Conservation*, 29 (2): 117–131. doi:10.2307/3179578.

Wu, A.S. (2019) *A cookbook of invisible writing*. Eindhoven: Onomatopee.

IMAGES

FIGURE 01. Unknown. (n.d.) *Bone Record* [Photograph]. Available from: http://www.movietrainer.com/movies/film/roentgenizdat-the-strange-story-of-soviet-music-on-the-bone/2016 (Accessed: 31 October 2019).

FIGURE 02. Kuptsow. (1944) *D-Day - June 6, 1944 - Front* [Scan]. Available from: http://www.merkki.com/powwow.htm (Accessed: 8 May 2020)

FIGURE 03. russelgz. (n.d.) *Horse grass mud* [Photograph]. Available from: https://m.24sata.hr/junior/cupave-al-pake-bolje-da-ju-ne-ljutite-jer-ce-vas-pljunuti-352136 (Accessed: 8 May 2020)

FIGURE 04. Steiner, P. (1993) On the Internet, nobody knows you're a dog [Cartoon]. Available from: https://www.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31/73372600-f98d-11e2-8e84-c56731a202fb_blog.html (Accessed: 8 May 2020).

FIGURE 05. Unknown. (2019) *Cover picture: Ask for PDFs from People with Institutional Access* [Screenshot by author]. Available from: https://www.facebook.com/photo?fbid=10104619526528602&set=p.10104619526528602 (Accessed: 8 May 2020).

FIGURE 06. Amman, J. (1568) *Papermaking (From the Book of the Trades)* [Illustration]. Available from: https://www.wga.hu/art/a/amman/amman1.jpg (Accessed: 8 May 2020).

FIGURE 07. Österreichische Akademie. (1484) *3 Mountain Hill, Snake and Cross* [Scan]. Available from: http://www.ksbm.oeaw.ac.at/_scripts/php/BR.php (Accessed: 8 May 2020).

FIGURE 08. Unknown. (n.d.) *Left: Oval hand stamp for manuscripts with the words BRITISH LIBRARY. Centre: India Office hand stamp for non-small 'claim material' items. These items were treated as part of the British Library collection. Right: Library stamp from previous Oriental and India Office Collections. Use of this stamp ceased on 1 September 2005* [Scan]. Available from: https://blogs.bl.uk/collectioncare/2013/09/a-guide-to-british-library-book-stamps.html (Accessed: 31 October 2019).

FIGURE 09. Emil Frank, H. (1954) *Identification of sound and like signals* [Patent]. Available from: https://patents.google.com/patent/US3004104 (Accessed: 31 October 2019).

FIGURE 10. Sá Couto, P. M. (2019) *Tracking Dots found in the university printers* [Scan]. Available from: https://pzwiki.wdka.nl/mediadesign/User:Pedro_S%C3%A1_Couto/MIC (Accessed: 31 October 2019).

COLOPHON

AUTHOR

Pedro Sá Couto

This work has been produced in the context of the graduation research of Pedro Sá Couto from the Experimental Publishing (XPUB) Master course at the Piet Zwart Institute, Willem de Kooning Academy, Rotterdam University of Applied Sciences.

XPUB is a two year Master of Arts in Fine Art and Design that focuses on the intents, means and consequences of making things public and creating publics in the age of post-digital networks.

https://xpub.nl.

This publication is based on the graduation thesis Tactical Watermarks, written under the supervision of Marloes de Valk.