Intermédialités
Histoire et théorie des arts, des lettres et des techniques
Intermediality
History and Theory of the Arts, Literature and Technologies

Storing Authenticity at the Surface and into the Depths: Securing Paper with Human- and Machine-Readable Devices

Aleksandra Kaminska

Numéro 32, automne 2018

cacher
concealing

URI : https://id.erudit.org/iderudit/1058474ar
DOI : https://doi.org/10.7202/1058474ar

Aller au sommaire du numéro

Éditeur(s)

Revue intermédialités

ISSN

1920-3136 (numérique)

Découvrir la revue

Citer cet article

Kaminska, A. (2018). Storing Authenticity at the Surface and into the Depths: Securing Paper with Human- and Machine-Readable Devices. *Intermédialités / Intermediality*, (32). https://doi.org/10.7202/1058474ar

Résumé de l'article

Cet article se penche sur les technologies médiales qui attestent de l'authenticité d'un document. À l'aide des exemples des passeports et du papier-monnaie, l'article examine les mesures de sécurité (ex. dispositifs graphiques, holographes, puces électroniques) qui jouent les rôles d'espace de stockage fiable et de protection et de communication de l'authenticité, et ce, à travers l'espace et le temps. Ces dispositifs d'authentification sont examinés de deux manières différentes mais interreliées : 1) en tant que technologies aux contraintes temporelles particulières, limitées par leur obsolescence technique et leur durée de vie fonctionnelle; et 2) en tant que technologies pouvant être continuellement réinventées par le biais de fraudes ou de contrefaçons. Ces deux enjeux ont mené à l'élaboration de stratégies de dissimulation qui font évoluer le processus d'authentification lui-même : d'une action réalisée par les humains à la surface du papier, il devient une opération dissimulée dans les profondeurs du média, dépendant de la lecture par une machine. Bien que cette stratégie augmente la sécurité, elle est aussi un exemple de la quantité d'informations dans l'environnement qui échappent aujourd'hui à la perception humaine.

Storing Authenticity at the Surface and into the Depths: Securing Paper with Human- and Machine-Readable Devices[1]

Aleksandra Kaminska

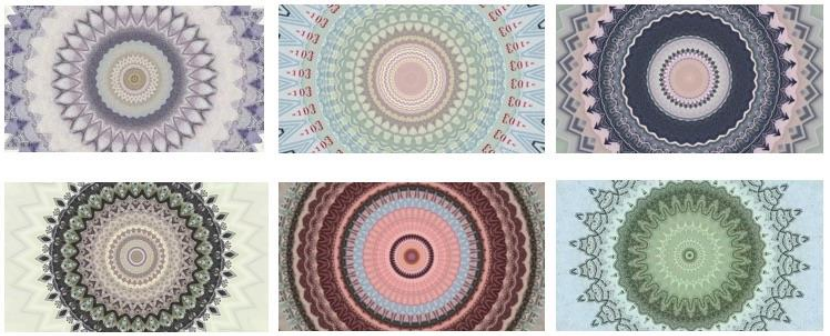

Fig. 1. Screenshots/stills from *Dominant Policy*, single channel HD digital video, Laleh Mehran, 2013. Courtesy of the artist.

In her video work *Dominant Policy* (2013), the Iranian-American artist Laleh Mehran treats currency as a visual technology, creating a kaleidoscopic display of the image-making techniques that produce the abstract and recognizable patterns, lines, and colours that characterize paper banknotes and that have marked currencies across the spans of both history and geography (see Fig. 1). Mehran draws our attention to the overlooked intricacies of an essential everyday object to consider the "decades of graphical change as monarchies reign, regimes fall, values fluctuate, and counterfeiting increases."[2] These graphic marks are visual security features that identify the notes as real, functioning in this role as *authentication devices*. Money and passports, both of which are the focus here,[3] are some of the most sophisticated

[1] This research was supported by the Social Sciences and Humanities Research Council of Canada.

[2] Laleh Mehran, "Dominant Policy," single channel HD digital video, http://lalehmehran.com/Dominant-Policy (accessed 5 August 2017).

[3] Authentication devices are, however, used for objects of all kinds, including credit cards, electronics, medical supplies, artworks, memorabilia, certificates, and luxury and branded goods.

objects in terms of the "baroque complexity of security features"[4] they contain: the fine patterns of guilloche, the surprising transparency of polymers, the splatter of microdots, the blast of florescent threads and UV inks, the evermore refined shimmering of colours in holographs and other iridescent images, or the discomforting intrusions of chips and biometric encodings. This assortment of visual, haptic, and connected devices forms a technical ecosystem of security measures that assures and "secures" the authenticity of a material object, and in these cases, of paper.[5] While there is a sustained preoccupation in media scholarship with the effects of the digital on the destabilization and rearticulation of materiality, things themselves face enormous pressure to maintain their value in an environment with accessible and proliferating technologies of reproduction, whether in fabrication or manufacturing.[6] It is in this environment of material insecurity that authentication devices for paper things—from seals and watermarks to holographs or chips—strive to be "irreproducible" features that secure value and meaning by guarding against unwanted tampering and replication.

¶2 Whether designed to represent, inform, or decorate, authentication devices become the way that we know and trust that certain appropriately marked papers can be used as currency or as an identification document. The techniques used for this "magical" transformation of a substrate into valuable "fancy paper"[7] rarely garner public attention, however, as they work in the slow, steady, and often secretive rather than spectacular, corners of high-tech media innovation. When it comes to currency, "we rarely stop to think about the money that passes through our hands,"[8] and passports face a similar fate: "The passport is a bizarre and unique object. Think

[4] Lisa Gitelman, *Paper Knowledge: Toward a Media History of Documents*, Durham, NC, Duke University Press, 2014, p. ix.

[5] In this article I use "paper" in a broad sense to include those substrates that are traditionally defined as paper (organic and cellulose-based), and also those that are emulations using polymers.

[6] For example, counterfeit and IP-infringing goods make up 2.5% of global trade, estimated at over USD $460 billion. OECD/EUIPO, "Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact," OECD Publishing, Paris, 2016, p. 11, http://dx.doi.org/10.1787/9789264252653-en (accessed 17 June 2018).

[7] Thomas Levenson, *Newton and the Counterfeiter*, London, Faber and Faber, 2009, p. 190 and p. 242. Here I am extending Levenson's use of the word "magic," which he uses to describe how a metal disc is transformed into legal tender with the presence of the image of the King's head on the coin.

[8] Emily Gilbert, "Currency," in Mark B. Salter (ed.), *Making Things International 1: Circuits and Motion*, Minneapolis, MN, University of Minnesota Press, 2015, p. 300.

about it: The goal is to put it in the hands of millions upon millions of people—and for none of them to ever understand the technology that's at work in their wallets."[9] The "technology at work" is precisely the collection of techniques that inscribe, embed, encode, and otherwise work to distinguish certain paper things as real, and without which others become mere unauthorized hacks, illicit reproductions, counterfeits, forgeries, and fakes.[10] In effect, "realness"—authenticity, legitimate identity, originality, veracity—is inscribed, mediated, and communicated by and through this category of media artefacts called "the authentication device."

¶3 The question of realness is not positioned here in a philosophical debate about the nature of the/a real, but as a material standard that contributes to the ordering, classifying, and categorizing of the world of things. It builds from the preliminary assumption that there are certain things that are circulated as authentic—with all of the value and meaning that this may conjure—and that, conversely, there are things that are fakes, in the sense that they are culturally, economically, politically, or otherwise considered to be illegitimate. As a result, authenticity is treated as a question of both duration and materiality, one that is examined through the continuously changing devices ("mediators") that allow us to inscribe ("write") and recognize ("read") the realness of material things. This understanding of media not as fixed objects but as "dependent on reading and retrieval" in particular social contexts[11] further helps explain the lifecycle of authentication devices as they transition from the secretive domain of security printing into imitable techniques of inscription and encoding, and as they move from human to machine legibility.

¶4 Passports and money have been studied extensively by researchers as explanatory objects for understanding the political and economic workings of societies and cultures. This work includes a consideration of passports in the history of identification strategies used by governments to classify and order their citizens,

[9] Kelsey Campbell-Dollaghan, "Your Passport's Complex Security Tech, Explained by Forgery Pros," *Gizmodo*, 5 February 2015, http://gizmodo.com/your-passports-complex-security-tech-explained-by-forg-1683950188 (accessed 20 July 2017).

[10] Though they are different, I will not distinguish here between these various unsanctioned productions. See, for example, Hillel Schwartz, *The Culture of the Copy: Striking Likenesses, Unreasonable Facsimiles,* New York, Zone Books, 1996; or Nick Groom, "Original Copies; Counterfeit Forgeries," *Critical Quarterly*, vol. 43, 2001, p. 6–18.

[11] Johanna Drucker, "Understanding Media: Craig Dworkin's 'No Medium'," *Los Angeles Review of Books*, 9 July 2013, https://lareviewofbooks.org/article/understanding-media-craig-dworkins-no-medium/ (accessed 20 July 2017).

namely through the fragmentation and objectification of identity. [12] Money, meanwhile, helps tell the story of payment, exchange, and ensuing social relations,[13] and it is an artefact that has been central to how we think about value and representation. Paper notes specifically introduce the crucial moment of abstraction, whereby value becomes independent and extrinsic of the material itself, unlike with coins with specific weights of silver or gold that had an intrinsic value.[14] Passports and banknotes are both examples of objects that must be accepted as legitimate, which explains the interest in the various informational and representational elements that constitute their authority, such as signatures.[15] It also explains why they become objects with unique technical histories: marbled paper was already used on the first paper notes issued by the Bank of England in 1695, explicitly as a way to prevent counterfeiting,[16] while in American passports seals, watermarks, binding techniques, and the weave of the paper were early features meant to help distinguish between real and fake documents.[17] A material understanding of how these official papers work can therefore be gleaned by tracing the story of these many individual techniques and materials.[18] Considering that a modern passport can contain over thirty different such elements,[19] it quickly becomes apparent that these "papers" are complex media

[12] Jane Caplan and John Torpey (eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World,* Princeton, Princeton University Press, 2001; Valentin Groebner, *Who Are You? Identification, Deception, and Surveillance in Early Modern Europe,* transl. Mark Kyburz and John Peck, New York, Zone Books, 2007; David Lyon, *Identifying Citizens: ID Cards as Surveillance,* Cambridge, UK, Polity Press, 2009; Craig Robertson, *The Passport in America: The History of a Document*, [2009], New York, Oxford University Press, 2012.

[13] For an overview, see Emily Gilbert, "Common Cents: Situating Money in Time and Place," *Economy and Society*, vol. 34, no. 3, 2005, p. 357–88.

[14] See, for example, Frances Robertson, "The Aesthetics of Authenticity: Printed Banknotes as Industrial Currency," *Technology and Culture*, vol. 46, no. 1, 2005, p. 31–50; Levenson 2009.

[15] For a historical perspective, see M.T. Clanchy on signing documents in *From Memory to Written Record: England 1066–1307,* [2006], 3rd edition, Malden, MA, Wiley-Blackwell, 2013.

[16] Levenson, 2009, p. 133.

[17] Robertson, 2012, p. 39.

[18] For example, in her historical study of paper notes Robertson integrates a technical discussion of watermarking and the spirograph-like patterns produced by the rose engine. See Robertson, 2005.

[19] Though the official numbers on how many security features there are in paper documents can vary greatly. For example, the security printer De La Rue claims there are "over

technologies. One of the challenges of this kind of technical inquiry, however, is the protective nature of the security printing industry, which makes it difficult to precisely and comprehensively assess the scope of its innovations and contributions. For instance, it has been noted that in currency there should be around twenty security features that are not shared with the public,[20] while the International Civil Aviation Organization (ICAO), which sets worldwide standards for passports, specifies that they ought to be produced using materials not accessible to the public.[21] Despite these challenges, authentication devices are nevertheless key to understanding the transformation of paper into functional and genuine identification document or currency.

¶5 In many ways, this technical story is a response to the threat of unwanted replication, which also explains the evolution of authentication devices as technologies whose effectiveness relies on their ability to guarantee and communicate their authority across space and time. With this in mind, authentication devices are here examined in two interconnected ways: 1) through their specific temporal conditions; and 2) as technologies that must be continuously reinvented. First, authentication devices are time-sensitive technologies whose effectiveness relies on both their technical stability in time as they are circulated about the world—what will here be described as their (technical) longevity—and the duration of their functional value—what will be termed as their (functional) lifespan. The latter is a precarious condition, continuously under the looming threat of forgers and hackers, imposters and intruders, which explains why devices have a limited shelf life. This leads to the second point, the ongoing need for new techniques that make "reading and retrieval" evermore complex, namely by controlling and tuning how authenticity is revealed or

400 security features" in the UK passport it produces. See De La Rue, ICAO 2018 newsletter, October 2018, https://www.delarue.com/icao_2018 (accessed 1 November 2018).

[20] Ross Anderson, "Security Printing and Seals," in *Security Engineering*, [2001], 2nd edition, Tokyo, New York, Wiley, 2008, p. 249.

[21] "Materials used in the production of travel documents should be of controlled varieties, where applicable, and obtained only from reputable security materials suppliers. Materials whose use is restricted to high security applications should be used, and materials that are available to the public on the open market should be avoided" (ICAO, "Doc 9303: Machine Readable Travel Documents. Part 2: Specifications for the Security of the Design, Manufacture and Issue of MRTDs," 7th edition, report, Montreal, International Civil Aviation Organization, 2015, https://www.icao.int/publications/Documents/9303_p2_cons_en.pdf (accessed 24 July 2017), p. App A-2.

concealed. To achieve this, authentication devices move from the overt and perceptual domains of visual and haptic inscription, to the covert and relational mechanisms of concealed and computational encoding, processing, and calculation. With machine-readable devices, what once was "human-readable" becomes restricted and hidden, fueling renewed configurations of the "three-dimensional coordinate axis of visibility, legibility, and instrumentation."[22] Through this analysis, the aim is to consider how and why authenticity, as a kind of stored information with particular temporal conditions, moves from the perceptible human surface and into the imperceptible machine depths. By doing so, it suggests that this distancing points to an ontological concealing of authenticity provided by covert digital storage, becoming an example of the mounting inability for humans to themselves "read" (see, detect, process, assess, know) what, and who, is "real." Finally, underlying this analysis of secured paper is the question of how authentication devices operate as media technologies, and how they do the work of reliably storing, protecting, and communicating authenticity across both space and time.

Securing the Real in Space and Time

¶6 Authentication devices are mobile technologies that preserve and communicate realness as they move about the world. As they travel in space, they assist in the technical governance and management of circulation[23] within and across infrastructural, institutional, and logistical systems, or in how things and people are legibly and legitimately ported[24] from one site to another. Since they are technologies that communicate the quality of authenticity, they act as a technical *lingua franca* that eases and secures exchange between structures, serving a translative function that assures rightful passage from one system or place to another: to authenticate is to give credibility and passage to go elsewhere. Moments of authentication therefore act as gateways towards further movement, portals into other or further circuits and trajectories—whether in migration, war, or trade. Paper bills and passports work as

[22] Matthew Kirschenbaum, *Mechanisms: New Media and the Forensic Imagination,* Cambridge, MA, MIT Press, 2008, p. 3.

[23] Mark B. Salter, "Introduction," in Salter (ed.), 2015, p. vi–xxii; Michel Foucault, *Security, Territory, Population: Lectures at the College de France, 1977–78*, transl. Graham Burchell, Bassingstoke, UK, Palgrave Macmillan, 2007.

[24] Reference to the idea of "porting" comes thanks to the Porting Media conference organized at McGill and Concordia universities in Montreal, 12–14 October 2017.

currency and identification document because of the technologies they contain, which operate as authorized hinges between the material and the institutional or infrastructural. Through their form and function, authentication devices are "agents of security" that "link to and reinforce the goals of security," thus becoming an example of the way that "security is something people do with various *things*."[25]

¶7 This ability to communicate authenticity in movement also requires that authentication devices are stable, resistant to damage, corruption, and other forms of obsolescence caused by not only mobility, but also the passage of time: they must be able to store authenticity, or to store the ability to prove authenticity, regardless of miles crossed and time passed. In this sense, authentication devices are not just symbolic inscriptions but material ones, and they must be durable and long-lasting without deterioration, distortion, or disintegration. Authentication devices are thus technologies of duration that hone material structures precisely to overcome the destructive effects of time.

¶8 In his work on the map as a form of inscription, Bruno Latour makes a helpful point on the value of "things" that circulate, and specifically that, like the maps produced by early explorers, have specific value as items brought back from one place to show in another:

> You have to go and to come back *with* the "things" if your moves are not to be wasted. But the "things" have to be able to withstand the return trip without withering away. Further requirements: the "things" you gathered and displaced have to be presentable all at once to those you want to convince and who did not go there. In sum, you have to invent objects which have the properties of being *mobile* but also *immutable*, *presentable*, *readable* and *combinable* with one another.[26]

Like the map, the authentication device is also a form of "convincing" inscription where the particular techniques that are chosen do make a difference "in the way we

[25] David Grondin and Shah Nishah, "Secrets," in Mark B. Salter (ed.), *Making Things International 2: Catalysts and Reactions*, Minneapolis, MN, University of Minnesota Press, 2016, p. 92–93 (emphasis in original).

[26] Bruno Latour, "Visualisation and Cognition: Drawing Things Together," in Henrika Kuklick (ed.), *Knowledge and Society Studies in the Sociology of Culture Past and Present,* Greenwhich, CT, Jai Press, vol. 6, 1986, p. 6 (emphasis in original).

argue, prove and believe."[27] They are also "things" that require both mobility and stability, and it is no coincidence that Latour uses money as one example of such an "immutable mobile."[28] With money as in passports, it is not just the wear and tear of the substrate that must be controlled (through its specific composition), but of all of the devices it contains. After all, in passports an expiration date is what notes the end of this document's life, not its physical degradation. This steadiness of devices in space and time can be described as their technical longevity.

¶9 Functional lifespan is another form of temporality that inflects the authentication device. This is the time during which each specific technical feature can be *trusted as* an authentication device. Here it is useful to note that these technologies are not merely "features" but functional *devices*. The device belongs in the constellation of concepts and words used to name, describe, and categorize the technical universe, but has received less attention than many of its counterparts. A recent definition suggests that it is "an artefact, a piece of equipment or an instrument made or adapted for a particular purpose, as well as a plan, method, trick or intrigue, and finally a design or motif. To use the notion of the device is therefore to call for the simultaneous consideration of object, purpose and effect."[29] The etymological meaning of device also alludes to a plan or strategy, something that in computational terms could be called a protocol: a set of conventions or procedures for how to operate, apply, implement, and run a technical device within and as part of a larger system, apparatus, infrastructure, or culture.[30] This protocol is also a measure of trust. As William Walters and Daniel Vanderlip note, objects like banknotes and passports materialize trust using the specific materials and techniques of authentication devices: "But once you materialize trust, you open up the possibility for replication or imitation. The passport becomes a research frontier: an ongoing

[27] *Ibid.* p. 5.

[28] However, there is a distinction, as is made here, between the object itself (money, a map) and the devices that inscribe authenticity, which expands the characteristics of inscription beyond those outlined by Latour (e.g. reproducible; paper-based).

[29] Anthony Amicelle, Claudia Aradau, and Julien Jeandesboz, "Questioning Security Devices: Performativity, Resistance, Politics," *Security Dialogue,* vol. 46, no. 4, 2015, p. 294.

[30] See, for example, Craig Robertson, "'You Lie!' Identity, Paper, and the Materiality of Information," *The Communication Review*, vol. 17, no. 2, 2014, p. 69–90; Lisa Gitelman, *Always Already New: Media, History, and the Data of Culture*, Cambridge, MA, MIT Press, 2006.

experiment in the materialization of trust set against a 'technological race' between issuers, regulators, and forgers."[31]

¶10 This "technological race"[32] refers to the ongoing need to produce new and evermore complex devices that are, at least for a while, beyond the reach of illegitimate reproducers. Since the authentication protocol of any technical device can only last as long as its reproducibility can be highly controlled and restricted to authorized copiers, its viability is perpetually threatened by the ingenuity and speed of the counterfeiter. The period of this "irreproducibility" is the functional lifespan of a feature as a security device: as soon as it can be illegitimately produced it can no longer be absolutely trusted, therefore losing its authenticating protocol.

Storing Authenticity

¶11 Storing is, in some manner and for some time, to preserve information so that it can be retrieved, sooner or later. Authentication devices are technologies of duration that must mobilize techniques of storage both as a strategy to ensure the uncorrupted longevity of the information they carry, and to prolong the useful lifespan of the techniques implemented. As storage technologies, authentication devices benefit from Matthew Kirschenbaum's analysis on the difference and interdependence of forensic and formal materiality, which together are "able to articulate the operation" of devices.[33] This difference between the forensic and the formal, which accords "with the fundamental duality of a mechanism as both a product and a process," rests "on the twin textual and technological bases of inscription (storage) and transmission (or multiplication)."[34] This controlled rapport between storing and sharing explains the specific workings of authentication devices as technologies that must carry and prove their originality, but do so in a manner that always remains resistant to unfettered dissemination.

¶12 Despite the centrality of storage to the history of media technologies, it has been a somewhat uneven preoccupation for media scholars, a niche interest for those

[31] William Walters and Daniel Vanderlip, "Electronic Passports," in Salter (ed.), 2015, p. 14.

[32] Walters and Vanderlip borrow the term "technological race" in this context from Andreas Fahrmeir, "Governments and Forgers: Passports in Nineteenth-Century Europe," in Caplan and Torpey (eds.), 2001, p. 218–234.

[33] James Allen-Robertson, "The Materiality of Digital Media: The Hard Disk Drive, Phonograph, Magnetic Tape and Optical Media in Technical Close-Up," *New Media & Society*, vol. 19, no. 3, 2017, p. 458.

[34] Kirschenbaum, 2008, p. 15.

working at the intersections of material history and technical functionality. This is, as Wolfgang Ernst notes, partially due to the need to have both "sound technological knowledge on the one hand, and media philosophical curiosity on the other."[35] One way to think storage has been as inscription, or "a kind of writing machine"[36] that can exist across the gamut of analogue and digital reading and writing systems that allow information to last. This is a way of thinking media history across its support systems, from graphic marks on a variety of substrates including paper, to those that translate information into various systems of holes, pits, and grooves (including punched cards, vinyl, and optical discs), to the hardware-software of computer memory and its forms and formats of progressive data compression.[37] Storage as inscription thus refers to a broad range of techniques that wed information to material affordances so that it allows for a thinking about how information is made to last across a range of mediating supports and how it shifts from human to machine readability.

At the Surface

¶13 At the surface level, authentication devices use a variety of visual and haptic forms of inscription to store authenticity. Visible devices such as those displayed in *Dominant Policy* are called *overt* devices. This means they are recognizable through the cursory examination of direct observation, or a basic sensory level of detection referred to as first-line inspection.[38] The inscription at the surface is what allows each of us to "decide subconsciously" whether an object is acceptable,[39] or a trained border guard or bank teller to detect or interpret the validity of passports and bills through informed senses, primarily vision and touch. Until at least the mid-twentieth century even quality control was done manually: banknote inspectors (primarily women) in money-printing facilities, such as the Canadian Bank Note Company or the US

[35] Wolfgang Ernst, "Tempor(e)alities and Archive-Textures in Media-Connected Memory," in Andrew Hoskins (ed.), *Digital Memory Studies: Media Pasts in Transition*, London, Routledge, 2017, p. 143–155.

[36] Kirschenbaum, 2008, p. 19

[37] See, for example, Friedrich Kittler, *Gramophone, Film, Typewriter*, [1986], transl. Geoffrey Winthrop-Young and Michael Wutz, Stanford, CA, Stanford University Press, 1999; Lisa Gitelman, *Scripts, Grooves, and Writing Machines: Representing Technology in the Edison Era*, Stanford, CA, Stanford University Press, 2000; Kirschenbaum, 2008; Gitelman, 2014.

[38] Rudolf van Renesse, "Human Factors of First Line Security," *SPIE* 3314, Proceedings of the Conference on Optical Security and Counterfeit Deterrence Techniques II, San José, CA, 28–30 January, 1998, p. 97–108, http://vanrenesse-consulting.berloth.net/index.php?page=spieconference.htm (accessed 24 July 2017).

[39] Anderson, 2008, p. 248.

Bureau of Engraving and Printing, verified that what was distributed as legitimate money was always printed correctly, visually checking paper bills before they went into circulation (see Fig. 2).

Fig. 2. Inspecting paper currency. Canadian Bank Note Company, Ottawa, Ontario, 1957. Photograph by Herb Taylor. Library and Archives Canada.

¶14 The ability to perfectly reproduce bills, with all of the devices they contain, is one of the ways that the public has historically become convinced that paper can be trusted as money.[40] It is through a standardized and "machine aesthetic" that an "objective" standard of judgment could be agreed upon and a real note could

[40] Robertson, 2005.

subsequently be distinguished from an irregular fake.[41] Already in the nineteenth century qualities of paper such as a distinctive colour, thinness, transparency, feel, watermark, finish, and strength, were considered as characteristics that could be used as measures against forgery and counterfeiting.[42] Today, the Bank of Canada website educates the public on these detectable features, urging us to "look," "feel," "tilt," and "flip" our bills to assess their veracity.[43] The devices that produce such perceptible effects are technologies of imaging, display, and printing produced by security printing companies with largely unrecognizable names—DeLaRue, CARTOR, OpSec, SICPA, Giesecke & Devrient—but long histories (e.g. DeLaRue was founded in England in 1821). These companies are responsible for the production of authoritative devices, with a technical arsenal that includes holographs and other optically variable technologies, see-through polymers, guilloche, fluorescent or metalized thread, thermochromic and other specialized inks, watermarks, microprinted features, and others. These techniques can in turn be applied in elements like stamps, seals, and emblems, patterns and splatters, signatures and portraits, and other informational, representational, or abstract elements.

¶15 Surface features are also haptic. Referring to another kind of document that needs to assert its legitimacy, Lisa Gitelman notes, "[o]ne doesn't so much *read* a death certificate, it would seem, as perform calisthenics with one, holding it out and then holding it close, flipping it one way and fingering it another."[44] Tactile properties can be the result of substrate composition, such as in the particular recipes that produce the distinctive and recognizable feel of the synthetic polymer of Canadian bills or the cotton-linen blend of American paper notes. They can also include resurfacing techniques like *intaglio* or letterpress that create textured reliefs and depressions to form topographical impressions. Since some features such as raised inks or specialized forms of paper-making are both visual and haptic, these are not mutually exclusive categories. What characterizes these overt devices is that they are closed systems, in the sense that in and of themselves they can be read as marks of

[41] *Ibid.*, particularly p. 33–34.

[42] *Ibid.,* p. 37.

[43] Bank of Canada (n.d.) Security features, http://www.bankofcanada.ca/banknotes/bank-note-series/polymer/security-features (accessed 4 January 2017). In the US, the public security features on bills are explained on the website of the U.S. Currency Education Program: https://www.uscurrency.gov/ (accessed 3 September 2018).

[44] Gitelman, 2014, p. ix (emphasis in the original).

authenticity: they marshal the human ability of perception, detection, and recognition so that a person can evaluate, through sensory means, the legitimacy of a device, and thus the thing (and by extension person) that it is securing.

¶16 Gitelman goes on to describe the epistemological work of documents, as essential artefacts of bureaucracy, through their "know-show" function, or "the kind of knowing that is all wrapped up with showing, and showing wrapped up with knowing."[45] Like in other documents, the authentication devices in passports play an essential role in this process as they "know" and "show" the value of the printed paper. When authenticity is stored at the surface, overt devices are examples of the technical infrastructure of media being homologous with their surface appearance, what Mark Hansen describes as a pre-computational characteristic of media technologies.[46] Indeed, the surface as support is part of the longer historical lineage in media studies that precedes computation, a time when the substrate was "king."[47] At the surface what matters is the technical accuracy of the device since, as noted, this is all that differentiates it during first-line inspection from a similar but poorly executed copy. Along these lines, Craig Robertson argues in his work on passports that overt devices work and are recognized as authentic not because of their content, but through the "presence of inscriptions" and the authority that they have been given: it matters less whose signature is on a dollar bill than the fact that there is a signature.[48] This "fact" of the signature, or of other overt inscriptions, is a matter of technical execution. The fact and the matter, or the matter of (the) fact, together materially inscribe and store authenticity; the material accuracy of the device contains evidence of its own veracity.

¶17 As overt devices and their forms of inscription remind us, storage technologies are not just preoccupied with duration, but also with space and visibility. Just as we store physical things by finding places where they might fit, storing becomes a form of hiding that moves things away and into so that they do not, in their full expanse, get in the way. In this perspective, storage becomes a form of miniaturization and compacting that aims to reduce the amount of space that

[45] Gitelman, 2014, p. 1.

[46] Mark B. N. Hansen, "New Media," in W.J.T. Mitchell and Mark B.N. Hansen (eds.), *Critical Terms for Media Studies*, Chicago, University of Chicago Press, 2010, p. 178.

[47] Allen-Robertson, 2017, p. 456.

[48] Robertson, 2014, p. 80.

things take,[49] perhaps even to make them, in effect, invisible. By putting the emphasis on visibility, storage becomes a question angled towards the spatial and preoccupied with the sites and techniques of concealment. Thinking storage as a collection of technologies that allow for durable and controlled visibility is useful across analogue and digital media artefacts. Authentication devices thus remind us of the multiplicity of media histories and theories of storage that can exist, outside or beyond a trajectory that necessarily arrives at the problem of the temporal instability of computing, as it animates ongoing work on digital preservation, memory, and the archive.

Deep Surfaces

¶18 Holographs are today one of the most common authentication devices, playing with the interactions of light and matter at the surface for visual effect. The impression that there is more behind the surface is the first indication of depth, and holographs, as optical variable devices (OVDs) are also a good example of the way that surfaces can be deceiving, or at least more complicated than they first appear. These technologies play visual tricks at the surface, their "variability" denoting a shifting and iridescent quality. It is notable that despite his interest in both storage as a central function of media technologies and in the techno-physical dimensions of optical media, Friedrich Kittler did not pay heed to a technique like holography. Rather, in his work bridging the gap between literary and media studies, such as in his lectures on optical media, he covered technologies like painting, photography, and film, rather than, for instance, holography or UV inks, which are indeed optical even if not generally or conventionally included in media histories or discussions on media as they are used in cultural expression.[50] Yet when Kittler states that he is examining how images are "first learned to be stored and then also to move,"[51] he could have been writing about holography. [52] As examples of "unsung and offbeat" [53]

[49] The history of computing and various media technologies can be understood as a history of compression. See, for example, Jonathan Sterne, *MP3: The Meaning of a Format,* Durham, NC, Duke University Press, 2012.

[50] Holography, however, has been of sporadic interest to artists and scholars, though often suffering from a reputation as being gimmicky. See Sean F. Johnston, *Holographic Visions: A History of New Science*, Oxford, Oxford University Press, 2006.

[51] Friedrich Kittler, *Optical Media*, Cambridge, UK, Polity Press, 2009, p. 22.

[52] The fact that his focus in this text are technologies of the nineteenth century and that holography is a technique that appears in the second half of the twenty-first might provide an explanation for his choice but, arguably, an incomplete one.

[53] Gitelman, 2014, p. 19.

technologies, holographs, and other OVDs can provide a different way to examine optical technologies as technical objects working with light, colour, matter, and substrate, helping to insert some overlooked mediations, inscriptions, and circulations into the story of media technologies.

¶19 While holography as a storage technology was never fully developed and implemented, the potential for optical surfaces to store has now become part of a larger speculative trend towards what are alternatively called informatic or programmable matters, and smart or meta materials.[54] Nanotechnology has played a key role in developing these new materials, some specifically designed and black-boxed by the security printing industry. Similar to holographs in their iridescent visual effect, nano-optical variable devices are an example of how the "technological race" has led to the production of more technically complex "holograph-like" devices. Rather than being produced through techniques of inscription based on laser writing like traditional holographs, nano-OVDs are designed at the nano-scale level of material structure, creating a physical system of pixilation that produces structural colour, and that can also store information on the infrared, invisible, spectrum. Such devices are making their way onto currencies, passports, and other showcases.[55] Nano-OVDs provide first-line inspection through their iridescent visual effects, and can provide an additional layer of security through the concealment of information. Since this covert information requires specific "retrieval" tools to be read and decoded (for example, a reader like a smartphone), counterfeiters must not only be able to fabricate the authentication device, but also to understand and reproduce the way that all of its covert information is "revealed." The same is true for other kinds of devices that also open up the surface by storing machine-readable information: barcodes, for example, are superficially visual, but meaningful only when read by a machine. Like nano-optical technologies, they straddle surface and depth and are thus designed for both human and nonhuman reading. Meanwhile, the requirements for the identification page of machine-readable passports laid out by the ICAO include both

[54] See, for example, Daniel Black, "An Aesthetics of the Invisible: Nanotechnology and Informatic Matter," *Theory, Culture & Society*, vol. 31, no. 1, 2014, p. 99–121; Eugene Thacker, *Biomedia*, Minneapolis, MN, University of Minnesota Press, 2004; Susanne Küchler, "Technological Materiality: Beyond the Dualist Paradigm," *Theory, Culture & Society,* vol. 25, no. 1, 2008, p. 101–120.

[55] Russell Douglas, "TED 2014 NanoTech Security's First Customer for Its Butterfly-Inspired Holograms," *Canadian Business*, 19 March 2014, http://www.canadianbusiness.com/technology-news/nanotech-security-holography-ted/ (accessed 3 September 2017).

a "visual inspection zone" (VIZ), which is meant to be read by a person, and a "machine readable zone" (MRZ) intended for an optical character recognition (OCR) reader.[56] The MRZ provides verification of the information in the VIZ (name, place and date of birth, issuing state, etc.), but may also be used to "provide search characters for a database inquiry," and "to capture data for registration of arrival and departure or simply to point to an existing record in a database."[57] In this hybrid situation, machine readability is used "in the interest of accelerating the clearance of passengers through passport controls,"[58] but human verification of the document remains possible. Thus the surface is still legible, but is has depth, concealing information in a space beyond human perception.

In the Depths

¶20 Covert devices are habitually understood as those requiring the assistance of a machine, or reader, to perform their authenticating function. This can mean that they need to be made visible by machines, such as with invisible inks that necessitate UV light in order to be revealed. Or it can mean that they must be read by machines because they contain encoded stored information, which must then be detected, decoded, decrypted, processed, matched, or in some way made sensible using a computational intermediary. They are also called digital devices. The ICAO more precisely categorizes security features that require machine verification into three categories: 1) structure features, which have part of their physical construction verified by a machine, such as through a specific interaction with light; 2) substance features, which include a material that would not be detected visually, such as special pigments or fibers; and 3) data features in which there is concealed information, such as in steganography where digital information is hidden in an image.[59] Such images "become visible when the data object is subjected to the appropriate formal processes,

[56] ICAO, "Doc 9303: Machine Readable Travel Documents. Part 1: Introduction," 7th edition, report, Montreal, International Civil Aviation Organization, 2015, https://www.icao.int/publications/Documents/9303_p1_cons_en.pdf (accessed 24 July 2017), p. 3–6.

[57] ICAO, "Doc 9303: Machine Readable Travel Documents. Part 3: Specifications Common to all MRTDs," 7th edition, report, Montreal, International Civil Aviation Organization, 2015, https://www.icao.int/publications/Documents/9303_p3_cons_en.pdf (accessed 8 October 2018), p. 16.

[58] ICAO, "Doc 9303: Part 1," 2015, p. 1.

[59] ICAO, "Doc 9303: Part 2," 2015, p. 3.

which is to say when the appropriate software environment is invoked."[60] In passports electronic chips are digital devices that store information, some of which is humanly legible elsewhere in the VIZ area of the passport, while other is only contained as concealed in the chip.[61]

¶21 Chips help passports with one of their central challenges, providing both "official certification and proof of individuality."[62] Indeed, passports perform verifications of various order: they must prove that they are real documents, they must identify a person, and they must assert that the two belong together. Since authentication can only be completed if the object is linked to the right body, one of the "technical fixes to this identity problem"[63] has become the biometric chip,[64] which uses the body to validate that the document is associated with its rightful owner.[65] With this chip, an additional level of protection is however required. Indeed, despite the plethora of devices stockpiled on an ePassport,[66] it is arguably "only as secure as the biometric and biographic information contained in its chip."[67] Because protecting the data has now become paramount in securing the passport, the paper object has become dependent on digital security, relying on, most significantly, public-key-infrastructure (PKI) technologies that algorithmically validate the unique digital signature contained on a chip, but also regulations establishing standards that limit the distance at which contactless chips can be detected by electronic readers.

---

[60] Kirschenbaum, 2008, p. 13.

[61] Information stored on a passport biometric chip includes a duplicate of the MRZ data, "globally interoperable biometric data that can be used as an input to facial recognition systems, and, optionally, to fingerprint or iris recognition systems," as well as discretionary data as per the issuing state (ICAO, "Doc 9303: Machine Readable Travel Documents. Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs," 7th edition, report, Montreal, International Civil Aviation Organization, 2015, https://www.icao.int/publications/Documents/9303_p9_cons_en.pdf (accessed 8 October 2018), p. 1).

[62] Groebner, 2007, p. 224.

[63] Walters and Vanderlip, 2015, p. 8.

[64] For an example of another object using biometric chips, see Elizabeth Cobbett, "Biometric MasterCard," in Salter (ed.), 2015, p. 311–327.

[65] Of course, this aggregation of biometric information as a form of "security" leads to questions regarding where, how, and by whom data is stored, as is articulated through concerns over surveillance and the protection of privacy.

[66] An ePassport is a passport with a biometric chip.

[67] Walters and Vanderlip, 2015, p. 11, quoting ICAO, "ePassport Implementation and the ICAO PKD," *ICAO MRTD Report* 7, no. 3, 2012, p. 7.

¶22 Chips transform the passport into a paper document that cannot be entirely read by humans. A chip cannot, in itself, at a first-line glance or manual inspection, be the mark of authenticity. Rather, this "datafication," which has converted authenticity into symbolic bits of data that are in need of decoding, produces a distancing of human legibility. This reflects the same trend as in mechanisms of identification where there is a "perceived need to lessen the role of individuals"[68] and an *assumption* that we should use machines.[69] Moreover, it is no longer enough to trust the "machine aesthetics" of the document: the introduction of machine-readable elements in passports has brought "new cryptographic schemes," and new parties (such as chip and reader manufacturers) make "the underlying trust model, trust assumptions and trust relationships much more complex."[70]

¶23 By assuming that machine readability makes the assessment of authenticity more reliable and accurate, digital authentication devices are designed to surpass human perception, judgement, and interpretation, and rather invoke a standardized and automated processing of what and who is real. Using algorithmic and mathematical calculations and assessments, authenticity becomes objectified, constituted through all of the stored data that together can guarantee that this thing is real, and that it belongs to that person. This "augmentation" through concealment means authenticity—as a material quality—moves from being in the thing, to the extent that it is legible and verifiable by the human senses, to the relation between non-human things. Authenticity is no longer a material surface condition that is fixed or stable, but rather becomes a property that is interdependent and processual: what is stored is not the material "fact" of authenticity, but the potential or possibility of performing and connecting in the correct—"truthful"—manner. [71] Indeed, the perceptible elements of security devices—the things that we can flip, touch, and see—are "only the tip of the iceberg" of what David Lyon calls the "data-berg," with each device "represent[ing] a much fuller techno-organizational apparatus, which, like an iceberg, lies out of sight, below the surface."[72] Below water is where devices are linked

[68] Robertson, 2012, p. 17.

[69] Lyon, 2009.

[70] Dario Carluccio, Kerstin Lemke-Rust, Christof Paar, Ahmad-Reza Sadeghi, "E-Passport: The Global Traceability; or, How to Feel Like a UPS Package," *Information Security Application*, vol. 4298, no. 391–404, 2007, p. 392.

[71] This is not to say that overt devices are not also relational, in the sense that people must read them and that they exist in specific social contexts. The focus of the distinction proposed here is based on the human ability to perform the verification through their senses, versus an authentication that requires a computational process.

[72] Lyon, 2009, p. 43.

to other data and databases, where there is an overlapping of security and media infrastructures in transnational communication and logistical systems, and where concealment of the rules of processing adds another level of complexity and protection. This moves the focus of the enterprise onto digital security, so that the material is only as secured as the data which it contains, the databases and network to which it connects, and the computational links from one to the other. In this concealment through covert digital devices, trust has been placed onto machines as readers and retrievers. Yet in many cases, the companies responsible for such computational systems are part of what Lyon calls the "card cartel" that, unlike the companies that produce overt devices, have more familiar names: IBM, Oracle, Sun Microsystems, Microsoft. These corporations form an oligopoly that controls the networked infrastructure of identification and authentication and the apparatus in place to make it work: scanners, biometrics systems, smart card applications, etc.[73] While an overt authentication device exists to authenticate, a covert one exists to authenticate but also to provide or link to additional data and networks. This migration into technologies of surveillance converges the matter of trust with that of security, a relationship that materializes in the sociotechnical object of the authentication device.

¶24 While efforts to make currency entirely digital are still in their early stages (as yet there is no central-bank digital currency, or CBDC), money no longer needs a physical counterpart to be circulated, as we know from credit and debit cards, or the stock exchange. With digital currency, the value of money becomes even further abstracted and separated from representation in paper form as both the thing and the security of the thing reside outside the realm of human perception. It is worth noting however that, like with the biographical pedigree provided by RFID tags,[74] the blockchain system of a currency like bitcoin assures authenticity through its lineage: a currency in which blocks are approved by a network and are linked and secured together through encryption form a public ledger that is timestamped and cannot be independently altered, thus offering a transparent way to verify and authenticate transactions. More generally, unlike passports that still produce a connection

[73] *Ibid.*, p. 64.

[74] Radio frequency identification (RFID) tags are "track-and-trace" technologies that are particularly important in the logistical systems that support global trade. They can track the movement of items through the supply chain by noting locations, timestamps, and the details of each transaction using unique serial numbers, product codes, and other conventional systems of identification. This allows to track movement following a kind of biographical logic, in the sense of determining the "pedigree" of an object through the places it has been.

between a paper form and a digital network, digital currency moves away from the domain of security printing as it becomes fully folded into concerns over the security, and hacking, of data.

Conclusion

¶25 The need to produce techniques that allow for the circulation and duration of "immutable" authenticity across space and time outlines a genealogy of media technologies centred on articulating the attachments between materiality and information as driven by a necessity to mark, secure, and control certain things as reliably real. What has been at stake here is the authentication of *things*, and particularly the securing of paper through an assortment of human- and machine-readable devices that are attached to the paper they are securing. Overt devices belong to the study of visual, haptic, and printing technologies, while covert devices, especially digital ones, contribute to furthering work on encoding, processing, computation, and the digitization of inscription. Specifically, authentication devices help write the story of evermore complex storage as they move from a structural and overt relationship between information and materials, to one where data is legitimated through the "deep storage" of processes and potential relations that rely on the covert operations of machine legibility. As inscriptions become entirely hidden, fragmented into data, the ability for humans to evaluate authenticity becomes dependent on a machinic intermediary, creating an unreadable gap between humans and the world of things. Finally, in their need to continuously reaffirm complexity, ingenuity, and novelty because of their limited functional lifespan, authentication devices provide a way of bringing together a materialist enquiry and a broader sociopolitical analysis on the mechanisms of technological innovation, techniques of control, and the materialization of trust. In this sense, authentication devices are an example of the way that technological affordances must still be placed within and as part of social, economic, and political structures and environments. Indeed, they regularly conceal the realities not only of their own (technical) making, but also of their reason for being: what they do and how they function submerged from public perception, readability, and inspection.

Storing Authenticity at the Surface and into the Depths: Securing Paper with Human- and Machine-Readable Devices

Aleksandra Kaminska, Université de Montréal

ABSTRACT

This article examines the media technologies that mark paper as authentic. Using the examples of passports and paper banknotes, it considers the security features (e.g. graphic marks, holographs, chips) that do the work of reliably storing, protecting, and communicating authenticity across both space and time. These overt and covert authentication devices are examined in two interconnected ways: 1) as technologies with specific temporal conditions, constrained both by technical longevity and functional lifespan; and 2) as technologies that must be continuously reinvented to outpace counterfeiters and forgers. Together, these attributes have led to strategies of concealment that shift authentication from a human-legible activity at the perceptible surface to one that is concealed in the depths of machine readability. While this adds a level of security, it is also an example of how the material environment becomes rich in information that is inaccessible to human processing.

RÉSUMÉ

Cet article se penche sur les technologies médiales qui attestent de l'authenticité d'un document. À l'aide des exemples des passeports et du papier-monnaie, l'article examine les mesures de sécurité (ex. dispositifs graphiques, holographes, puces électroniques) qui jouent les rôles d'espace de stockage fiable et de protection et de communication de l'authenticité, et ce, à travers l'espace et le temps. Ces dispositifs d'authentification sont examinés de deux manières différentes mais interreliées : 1) en tant que technologies aux contraintes temporelles particulières, limitées par leur obsolescence technique et leur durée de vie fonctionnelle; et 2) en tant que technologies pouvant être continuellement réinventées par le biais de fraudes ou de contrefaçons. Ces deux enjeux ont mené à l'élaboration de stratégies de dissimulation qui font évoluer le processus d'authentification lui-même : d'une action réalisée par les humains à la surface du papier, il devient une opération dissimulée dans les profondeurs du média, dépendant de la lecture par une machine. Bien que cette stratégie augmente la sécurité, elle est aussi un exemple de la quantité d'informations dans l'environnement qui échappent aujourd'hui à la perception humaine.

NOTE BIOGRAPHIQUE

Aleksandra Kaminska is Assistant Professor in the Department of Communication at the Université de Montréal. She is currently working on a media history of authentication and security printing, and on practices of recognition in the media arts. www.aleksandrakaminska.com