DNB Working Paper
No. 716 / June 2021

Enhancing banknote authentication by guiding attention to security features and prevalence expectancy

Frank van der Horst, Joshua Snell and Jan Theeuwes

DeNederlandscheBank
EUROSYSTEEM

Enhancing banknote authentication by guiding attention to security features and prevalence expectancy

Frank van der Horst, Joshua Snell and Jan Theeuwes*

* Views expressed are those of the authors and do not necessarily reflect official positions of De Nederlandsche Bank.

Working Paper No. 716

June 2021

De Nederlandsche Bank NV
P.O. Box 98
1000 AB AMSTERDAM
The Netherlands

Enhancing banknote authentication by guiding attention to security features and prevalence expectancy

Frank van der Horst[a], Dr. Joshua Snell[b] & Prof. Dr. Jan Theeuwes[b]

[a] De Nederlandsche Bank, Amsterdam
[b] Vrije Universiteit, Amsterdam

June 2021

Abstract
All banknotes have security features which are intended to help to determine whether a banknote is false or genuine. Typically however, the general public has limited knowledge of where on a banknote these security features can be found. Here we tested whether counterfeit detection can be improved with the help of salient cues, designed to guide bottom-up visuospatial attention. We also tested the influence of the participant's a priori level of trust in the authenticity of the banknote. In an online study (N=422), a demographically diverse panel of Dutch participants distinguished genuine banknotes from banknotes with one (left- or right-sided) counterfeited security feature. Either normal banknotes (without novel design elements) or banknotes that contained a salient cue (a pink rectangular frame) were presented for 1s. To manipulate the participant's level of trust, trials were administered in three blocks, whereby at the start of each block, participants were instructed that either one third, one half, or two thirds of the upcoming banknotes were counterfeit (though the true ratio was always 1:1). We hypothesized (i) that in the presence of a salient cue, counterfeits would be better detected when the cue was valid (whereby the location of the salient element matched the location of the counterfeited security feature) than when it was invalid; and (ii) that this effect would be stronger with lower trust. Our hypotheses were partly confirmed: counterfeit detection improved with valid cues and decreasing trust, but the level of trust did not modulate the cueing effect. As the overall detection performance was rather poor, we replicated the study with a sample of university students (N=66), this time presenting stimuli until response. While indeed observing better overall performance, all other patterns were replicated.

Two lessons can be learned here. Firstly, as lower trust yields better authentication accuracy, central bankers may see merit in raising awareness about the existence of counterfeit banknotes. Secondly, our findings provide a proof of concept for the idea that bottom-up saliency can be used to aid banknote authentication.

Keywords: attention, decision-making, gist, vision, touch, authentication, banknotes, counterfeits.
JEL codes: E40, E41, E50, E58.

1. Introduction

Typically, people accept banknotes as change from another person or at a point-of-sale without consciously verifying authenticity (Klöne & Zondervan, 2019). Reasons for not checking authenticity are that counterfeit rates are extremely low, and that they trust the retailer (van der Horst, De Heij, Miedema & Van der Woude, 2017). A more practical constraint is that the general public has little knowledge of how to authenticate banknotes. On average, a person can mention two security features, but does not know what these features look exactly like, and where on a banknote these features may be found (van der Horst et al., 2017). For instance, 75% of the general public knows that a euro banknote contains a watermark, but only 5% knows what image the watermark depicts (Klöne & Zondervan, 2019). Yearly, the Eurosystem removes around 560 thousand counterfeits from circulation of 24 billion banknotes (ECB annual report 2019). For an overview of the most prominent public security features, as indicated by the Nederlandsche Bank (DNB), see Figure 1.

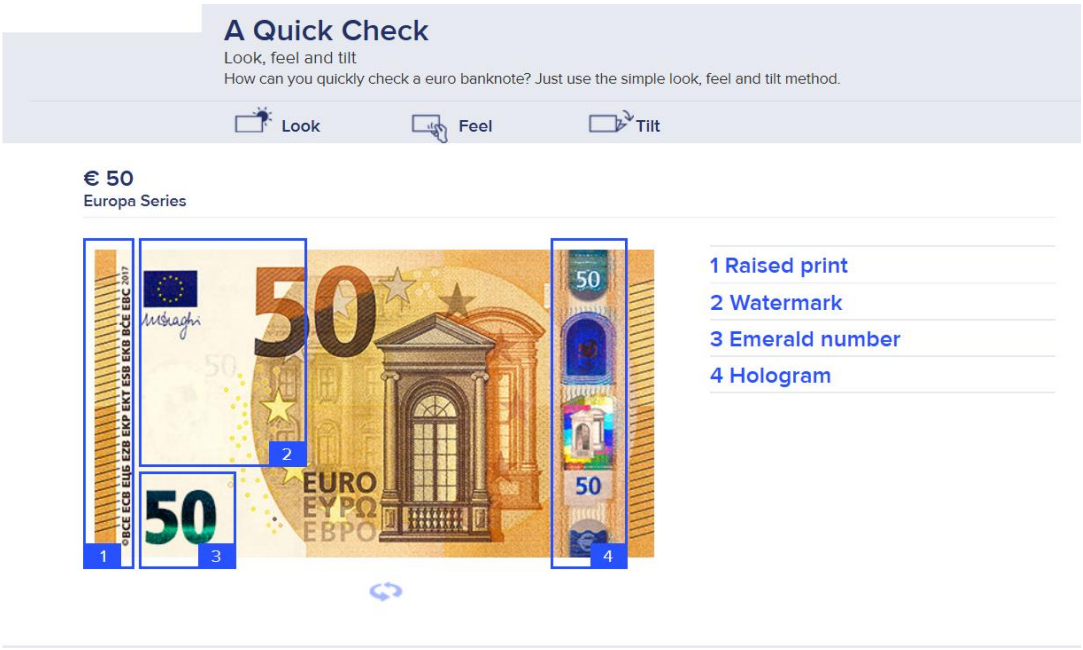

Figure 1. Instructional image on how to check the most prominent security features of a EUR 50 banknote quickly. Source: DNB website (www.dnb.nl/echtofvals).

In short, the public is hardly inclined to check a banknote for its authenticity, but when it does, it lacks the expertise to do it properly. Here we investigated whether counterfeit detection can be improved with the help of additional and novel, salient visual elements, designed to guide visuo-spatial attention to critical locations. Additionally, we assessed the impact of one's a priori trust on attentional orienting.

Our hypotheses were guided by two distinct fields of study. The literature led us to reason that a counterfeited security feature should be detected more readily when attention is directed to the location that contains the security feature. One way to ensure that attention is directed to the critical location is to introduce a visually salient element near the location of the security feature such that attention is captured towards the critical location in a bottom-up way (e.g., Theeuwes, 2010; Wolfe, Butcher, Lee, & Hyle, 2003). With respect to one's a priori of trust, we reasoned that lower levels of trust would increase overall

performance (due to increased effort). We were largely agnostic with respect to interactions between trust and cue validity. On the one hand, one might argue that increased effort (induced by low trust) would cause stronger attentional orienting and consequently stronger capture by salient design elements. On the other hand, an increased contribution of top-down attention might reduce the strength of bottom-up attentional capture. Let us now turn to these attentional dynamics.

1.1 Attentional processes in counterfeit detection

Cash transactions at a point-of-sale are generally performed quickly and automatically (van der Horst & Matthijsen, 2013). People do not give themselves time, or might feel embarrassed when scrutinizing the banknote (De Heij, 2017).

To authenticate a banknote properly, a good strategy is to direct attention to the security features. Attentional orienting can proceed in a bottom-up and top-down manner. Bottom-up attention is usually deployed reflexively due to the characteristics of the scene and stimulus saliency (e.g. Theeuwes, De Vries, & Godijn, 2003). Top-down attention is usually deployed voluntarily in line with one's tasks and goals (Egeth & Yantis, 1997). However, top-down authentication of banknotes is likely hampered by the handler's aforementioned lack of knowledge of where to look and how to process the security features.

It would therefore be ideal if security features were to capture attention in a rapid bottom-up manner (e.g. Theeuwes, 2019). It is worth noting that recently there have been a marked rise of simplified counterfeits without (mimicked) security features (Deutsche Bundesbank, 7-8-2020), suggesting that if attention would be directed immediately and briefly to the relevant location on a banknote this could improve counterfeit detection. This underlines the importance of guiding banknote users' attention to security features.

It may come as no surprise that saliency is a well-known concept among developers of banknote security features. For instance, nano-optic display technology features deliver a sense of movement, 3D depth, and multiple colors. According to manufacturers of these technologies, it make it possible to apply a wide array of custom design options to both capture and hold the user's attention as they inspect and authenticate a banknote (16-11-2020, https://www.nanosecurity.ca/banknote-security/). However, to date there is no scientific dissemination about the effectiveness of security feature saliency. Furthermore, one must take into account the possibility that with increased saliency of one security feature, attention may increasingly be directed away from other security features. One challenge is thus to achieve optimally balanced saliency across features—a challenge enlarged by the fact that features differ from each other in terms of shape and size.

A potential solution—and the focus of this study—is to display a *single* type of salient element near each security feature. As such, the security features themselves can stay as they are, while the novel salient design element may become an established marker for areas worthy of inspection.

As attention can indeed be guided with the help of salient visual elements (Theeuwes, 2010), we must nonetheless be aware of one potential constraint. It is known that the most salient elements in a display typically receive attention first – irrespective of whether they are relevant or irrelevant (Wang & Theeuwes, 2020). Hence, if the salient element is at the same location as the security feature— as in the case of a pink frame around the security feature (emerald number or hologram)—attention would be at the right location; but would it predominantly be directed to the pink frame, or to the emerald

number or hologram itself? In the former scenario, the salient element would be helpful in guiding attention coarsly, whilst interfering at a more detailed level.

We chose the colour pink (desaturated red) for the frame, because of its saliency. In an experiment conducted by Drelie Gelasca, Tomasic, & Ebrahimini (2005) participants had to rank 12 colours in terms of saliency. The colors that had much more hits were red, yellow, green and pink. Those of lower saliency seemed to be light blue, maroon, violet and dark green. Also, in a color experiment in which two groups searched for desaturated targets among saturated and white distractors it was concluded that the pink and peach targets have an advantage over the green, blue, and purple targets concerning reaction times (Kuzmova, Wolfe, Rich, Brown, Lindsey, & Reijnen, 2008).

1.2 The impact of trust

As noted earlier, we expect that persons who have high trust in the authenticity of banknotes, for example because they assume that the counterfeit rate is low, perform worse than persons who expect a higher counterfeit rate. This hypothesis is based on the 'prevalence-effect'. Observers tend to miss a disproportionate number of targets when these targets are rare (Wolfe & Van Wert, 2010). In everyday life the prevalence of counterfeits is very low. The general public mentions this as an important reason for not authenticating (Klöne & Zondervan, 2019).

Lau and Huang (2010) found that the prevalence effect depends on past experience, not on future prospects. In their study, participants were told either that targets would be frequent (50%) or rare (10%), and both these instruction types were provided in settings where the true prevalence was either 50% or 10%; (hence, prevalence and *the expectancy thereof* were orthogonally manipulated). As it turned out, the error rate depended not on the instructions given but on the true target prevalence of the blocks. However, it might have been the case that participants simply did not believe the instructions (i.e., that expectancy was not successfully manipulated).

In fact, other research suggests that both target repetition and target expectation play a role in the prevalence effect (Godwin, Menneer, Riggs, Taunton, Cave & Donnel, 2016). In the study of Godwin et al., one group of participants searched for low- and high-prevalence targets of one particular color throughout the experiment, while another group searched for one target color on high-prevalence slides and a different target on low-prevalence slides. As such participants received differential levels of target repetition across the lower- and higher-prevalence targets. An effect of prevalence emerged in both groups, although it was weaker in the single color condition than it was in the alternating-color condition, suggesting that both target repetition and target expectation play a role in the prevalence effect.

Previous studies have shown that prevalence expectancy can simply be influenced by task instructions For example, in their investigation of lesion detection on chest radiographs, Nocum, Brennan, Huang & Reed (2013) found that expectations of a higher abnormality-prevalence rate, as induced by instructions, impacted doctors' perceptual sensitivity and visual search patterns, even though observers received the same stimulus material.

In the current study, we manipulated expectancy, which is assumed to affect top-down attention, and manipulated the presence or absence of a salient cue around security features, which is assumed to affect bottom-up attention. The manipulation of expectancy is particularly important as it is one of the underlying factors of the trust one has in the

payment system. Obviously, people that have a low trust in the authenticity of banknotes expect that the counterfeits rate is relatively high and therefore are more likely to engage in authentication than those who trust the system very much (van der Horst, et al., 2020).

1.3 The present study

Typically in everyday life the general public does not authenticate banknotes because they trust the banknote to be genuine and because they have insufficient knowledge regarding which features and their locations can reveal whether a banknote is genuine or not. Therefore, in this study, we examined whether salient cues around security features may help the public in authenticating a banknote within a quick glance. It is important to determine whether authenticating can be done rapidly because cash transactions typically occur within a very brief time frame (van der Horst, Snell & Theeuwes, 2020). We hypothesized that displaying a pink frame around a counterfeited security feature would lead to better counterfeit detection. This manipulation is to some extent analogous to the classic Posner exogenous cueing paradigm (Posner, 1980), in which targets are typically detected faster and more accurately when a cue is valid than when it is invalid.

2. Method

2.1 Participants

In order to obtain a representative sample of the general public in the Netherlands, we made use of the LISS panel (longitudinal Internet Studies for the Social Sciences) run by CentERdata at Tilburg University. This panel is representative of the general population in the Netherlands and exists of around 5,000 households in the Netherlands. We aimed for a net sample of 400 participants, but in total 451 participants participated in the experiment. The panelists were 16 years and older. They received a small monetary compensation (EUR 7.50, real money) for their expenses (internet use and time).

2.2 Design

The experiment followed a 3 x 3 x 4 within-subjects design, with the following factors: *Cue* (left, right, none) ; *Trust* (high, mid, and low, corresponding to low-, mid-, high counterfeit expectancy, respectively); *Authenticity* (counterfeit element left, counterfeit element right, genuine, genuine); genuine is mentioned twice to have the same number of genuine versus counterfeit trials.

2.3 Stimuli

The test set consisted of images of genuine euro banknotes that were taken out of circulation and visually altered (counterfeit) versions of the same banknotes. We created counterfeits by replacing a genuine security feature by a cut-out of a counterfeited security feature. There were two types of counterfeited security features: the hologram (silverly stripe) that is positioned at the right side of the banknote and the emerald number that is positioned at the left side of the banknote, corresponding to the counterfeit element right and left conditions, respectively). The cut-outs were obtained from counterfeits taken out of circulation by De Nederlandsche Bank. Additionally, in order to implement the Cue left and Cue right conditions, for all banknote stimuli we created versions with a salient pink

rectangle framing either the left- or right-sided security feature. We chose the color pink because of it is rated as a particularly salient color (e.g. Drelie Gelasca, Tomasic, & Ebrahimini, 2005; Kuzmova, Wolfe, Rich, Brown, Lindsey, & Reijnen, 2008).

We used both EUR 20 and EUR 50 banknotes (denomination not being considered an experimental factor), the complete stimulus set consisted of 24 images, i.e. 2 Authenticity (genuine/counterfeit) x 3 Cue (left/right/no cue) x 2 Security feature (hologram/emerald number) x 2 Denomination (EUR 20/50). Denominations EUR 20 and 50 were used because these are by far the most used *and* counterfeited ones (press release DNB, 22 January 2021). Figure 2 shows examples of manipulated banknotes.

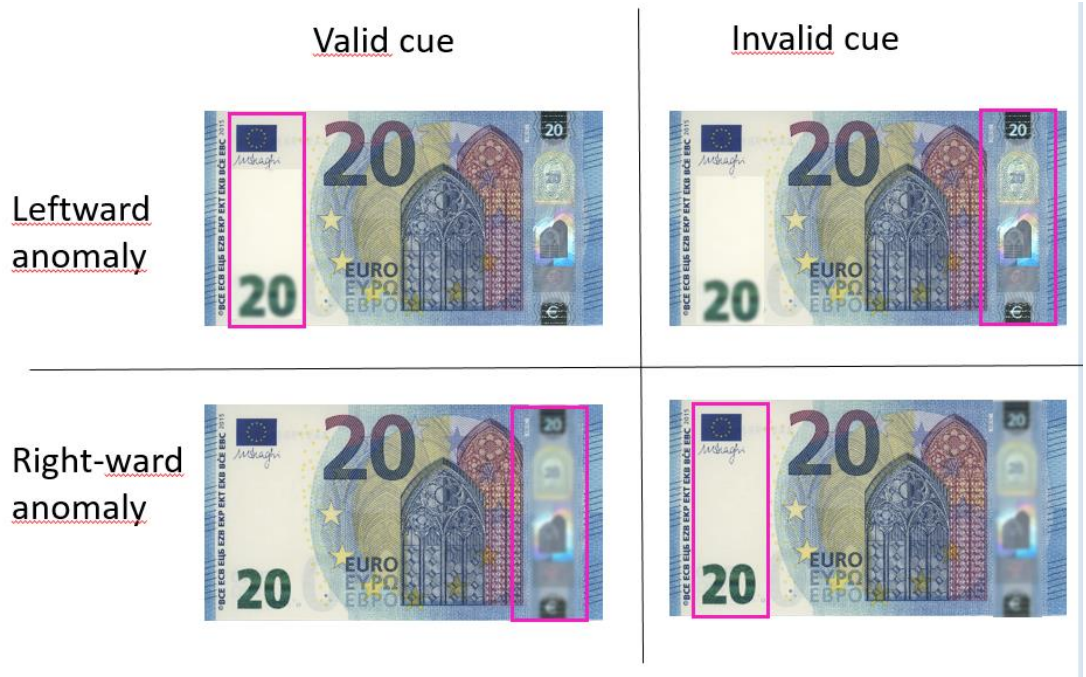

Figure 2. Examples of manipulated banknotes that are part of the test set. The banknotes on top contain a counterfeited emerald number: top-left with a pink cue around the counterfeited emerald number; top-right with the pink cue around a genuine hologram. At the bottom, banknotes with a counterfeited hologram: left-bottom a pink cue around the counterfeited hologram; right-bottom with a cue around a genuine emerald number. The two banknotes on the left are validly cued (the cue is located near the feature that is counterfeited). The two banknotes on the right are invalidly cued: the cue is near a genuine feature while the counterfeited feature is at the other side.

2.4 Procedure

Participants were invited to perform the test online on their own computers. For this reason, there was little control over the degrees of visual angle of our stimuli.

In the instructions participants were told that DNB wanted to test some design elements and that therefore a pink rectangle could be seen on the majority of banknotes. However, according to the instructions these new design elements would have no relation to whether the note was genuine or not. Next, participants were informed that banknotes would be presented for one second. They were instructed to authenticate the banknotes by

typing a ‘z’ for genuine and ‘/’ for counterfeit after the banknote was presented. They were instructed to respond as accurately as possible. They had a maximum of 4,000 ms to respond (after which the response would be considered an ‘error’). Banknotes were presented centrally, albeit with minor jitter (ranging up to 40 pixels) in the banknote’s x- and y-coordinates, so to prevent participants from developing oculomotor strategies. An overview of the trial procedure is shown in Figure 3. To get acquainted with the procedure, participants performed 12 practice trials that were not included in the data analyses.

The participants’ trust in banknote genuineness was manipulated between blocks. All 24 images were presented three times, in three blocks (presented in random order for each participant). Every time before the start of a block, participants were informed on the expected ratio between genuine and counterfeits for the upcoming block: (i) two out of three, (ii) even, and (iii) one out of three. In reality, the genuine vs. counterfeit ratio was always 1:1.

At the end of the experiment, participants received feedback regarding their performance: a percentage correct was provided for all three blocks. Participants were invited to fill in a short survey for demographics, color blindness and cash experience in working life (for the purpose of post-hoc analyses). The experiment took approximately 10 minutes.

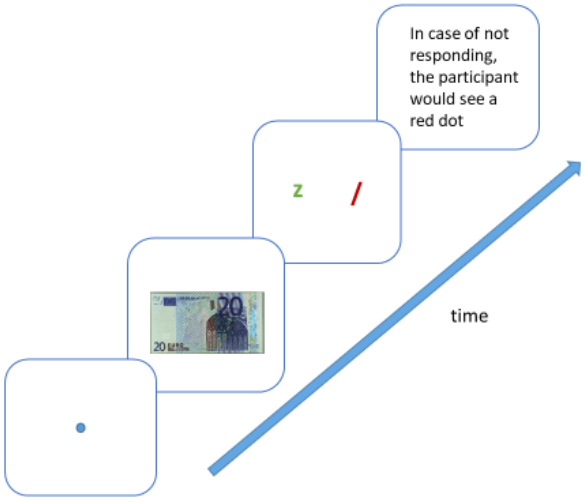

Figure 3. Example of a trial. Each trial started with a fixation dot in the center, for 500 ms, followed by a banknote (either EUR 20 or EUR 50, either genuine or counterfeit, either with a cue or not). The display duration was 1,000 ms. The information regarding the ratio of counterfeits was varied between blocks. If participants failed to press a key within 4,000 ms from stimulus onset, the trial was logged as a time out trial.

3. Results

All trials with a time-out were removed. In case this resulted in removing more than a third of a participant’s trials, the data of this participant was removed altogether, as this indicates that the participant was not able to perform the task properly. In total 29 participants were removed, constituting 9,1% of the data. The results of the remaining 422 participants were used.

To reiterate, the experiment included the following factors: Cue Validity (*valid* vs. *invalid cues*) and Trust (*low, mid-* and *high* levels of trust). These variables allowed us to rely, in part, on measures derived from Signal Detection Theory (SDT). The ability to discriminate genuine banknotes from manipulated banknotes is called sensitivity (d'), which can be estimated by deducting the z-transformed probability of false alarms (i.e., incorrectly classifying a genuine banknote as being counterfeit) from the z-transformed probability of hits. A d'-score of 0 corresponds to a complete inability to distinguish genuine banknotes from counterfeits. According to Raymond (2017), a d' of 1.25 represents decent sensitivity in banknote authentication. The maximum d'-score that can be obtained in this study is 3.92.

Importantly, while d' can be calculated when inspecting main effects of Trust (i.e., irrespective of cueing condition), this is not the case when inspecting main effects of Cue Validity (i.e., irrespective of level of trust). This is because the cue valid and invalid conditions solely contain counterfeit banknote trials (indeed, consider that there is no such thing as a validly cued genuine banknote), and therefore one cannot conjure a false alarm rate required for the calculation of d'. Hence, in all analyses that involved the Cue Validity factor, we simply relied on accuracy (the SDT-equivalent of which would be the hit rate, retrieved from counterfeit banknote trials). Our central analysis (reported in Section 3.2) was thus a 2 x 3 repeated measures analysis of variance (ANOVA) with Cue Validity and Trust as factors, and accuracy as dependent variable.

We nonetheless also analyzed Trust in isolation (Section 3.1), as we could retrieve not only d', but also the response bias (i.e. the extent to which one response is more likely to be given than another), or β, when inspecting this variable separately. The β measure, calculated by dividing the z-transformed probability of hits by the z-transformed probability of false alarms, provides an important verification of the effectiveness of our Trust manipulation. That is, if participants took the block instructions to heart, we expected them to have marked a larger portion of genuine banknotes as counterfeit upon being warned for a high counterfeit prevalence. At the same time, we may expect them to mark a low number of counterfeits as being genuine. Upon being warned for a low counterfeit prevalence, we would expect these patterns to be inversed. In short, if our Trust manipulation was indeed effective, we expect that β would be higher (i.e., more conservative) in the high-trust than in the low-trust condition.

3.1 Verifying the manipulation of Trust

Repeated measures ANOVAs were used to analyze main effects of Trust on d' and β. Overall, sensitivity did not increase linearly with a decrease in Trust ($F(2,421)=2.131, p=.119$). We did, on the other hand, observe a marginally significant effect of Trust on the response bias ($F(2,421)=2.437$, $p= .088$), with a more conservative response strategy in the high-trust than in the low-trust condition: that is that lower levels of trust aided counterfeit detection, but, at the same time, caused a higher proportion of false alarms. From these results we conclude that the way in which we manipulated trust was effective.

3.2 Central analyses

A Generalized Linear Model was run with Cue Validity and Trust as factors and accuracy as dependent variable. In line with our hypotheses, valid cues led to better accuracy than invalid cues: $F(1,421)=9.230$, $p=.003$. Again, we also observed a main effect of Trust, with better counterfeit detection at lower levels of trust; (however, given the absence of effects

in d' and the reversed effect for genuine banknotes, as reported in Section 3.1, it can be argued that this particular effect reflects a shift in β, rather than a change in overall performance). Trust did not modulate the effect of Cue Validity: F(2,421)=0.098,p=.907. Figure 4 shows the average scores for the six conditions.

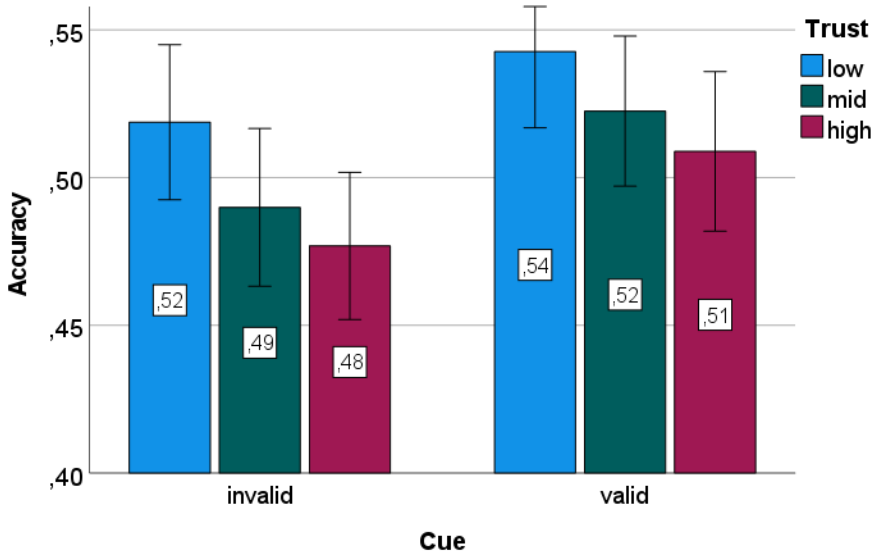

Figure 4. Average accuracy per level of trust (low, mid, high) and per valid or invalid cueing condition. Both a low trust in the authenticity (i.e. a high expectation on the number of counterfeits) and valid cueing led to better performance. Error bars depict 95% confidence intervals.

Evidently, overall authentication performance was quite poor in this population sample. In order to determine whether the task was too difficult, we calculated the average sensitivity scores in the no-cue condition, since this condition provides a baseline (without novel design elements) and as such can be compared to the study of van der Horst et al. (2020). We observed a sensitivity of d' = .386, which is indeed decidedly lower than the sensitivity d' = 1.05 observed in the study of van der Horst et al. (2020). This suggests that the task at hand was indeed rather difficult. However, it was significantly above chance-level (t(421)=11.274,p<=.001). We reckon that recognizing a single fake element in an image of a banknote that is exposed for only one second might be too difficult for non-trained members of the general public.

For this reason we decided to run the same experiment with a group of 66 psychology students and this time presenting the images of the banknotes until response. The results of this replication experiment are presented in the Appendix. Importantly, while the overall performance in this population sample was indeed better, we replicated all effects of interest (the bias of participants increased with a lower trust in the authenticity of banknotes: F(2,66)=3.684,p=.028. Main effects for accuracy per cueing validity (F(1,66)=5.690,p=.020) and trust (F(2,66)=5.621,p=0.005) and no interaction between these factors: F(2,66)=.899,p=.401.). In addition trust affected sensitivity scores adversely: F(2,66)=4.103,p=0.019.

General Discussion

The goal of this study was to investigate whether salient design elements, intended to direct attention to the location of security features, would aid banknote authentication accuracy. In our experiments, pink frames around a counterfeited security feature were expected to act as a cue, akin to attentional cues in classic tasks such as Posner's cueing paradigm (1980). Similarly, a pink frame around a genuine security feature, when at the opposite side a counterfeited security feature was present, was expected to act as an invalid attentional cue. Across two experiments we confirmed these expectations. Banknotes with a salient element around the counterfeited feature location yielded better detection than banknotes with an invalid cue. These results provide a proof-of-concept that bottom-up attentional salient cues can aid banknote authentication.

We also found that lower levels of trust aided counterfeit detection, but, at the same time, caused a higher proportion of false alarms (Section 3.1). It is worth considering that although high counterfeit detection rates are undoubtedly beneficial, effectuating these by means of lowering trust would imply extensive examination processes (i.e. more false alarms) and likely less smooth functioning of the cash payments system. Central banks may want to weigh this particular finding when they issue press releases informing the public about counterfeit prevalence. In relation to this, Lau and Huang (2010) have argued that instructions alone might not be very effective in reducing error rates in real-life low-prevalence contexts, such as airport baggage screening or counterfeit banknote detection. Instead these authors have argued for randomly distributing 'pseudo-targets'. This would imply an artificial increase in prevalence, and the experience gained with such pseudo-targets would reduce the chance of missing actual targets. Applying this idea to the realm of banknote authentication, central banks might consider purposefully bringing counterfeits into circulation, which, upon being spotted and reported, would yield a reward. Naturally, discussions of the legal constraints surrounding such operationalizations of trust and prevalence are beyond the scope of this paper.

The average sensitivity or d' in the no-cue (baseline) condition in the present experiment was .386. A d' of 0 corresponds to a complete inability to distinguish genuine banknotes from manipulated banknotes; and, according to Raymond (2017), a d' of 1.25 represents decent authentication sensitivity. Previous research (Van der Horst et al., 2020) showed a higher average sensitivity (d'=1.05) for the general public in a task similar to the present one (i.e., participants had to detect counterfeit banknotes that were presented for one second on a screen). There are however also important differences between the two experiments. Firstly, participants encountered novel design elements in the present study, which they ought to treat as being non-informative about the banknote's authenticity. Secondly, in the present study counterfeited banknotes contained only one counterfeited element, the emerald number or the hologram, which likely made the distinction between genuine and counterfeit banknotes smaller than in the study of van der Horst et al. (2020).

In our replication experiment with psychology students (N=66) that saw the stimulus until response, overall performance was decidedly better (d' = 1.73 in the baseline condition). The pattern of positive effects on counterfeit detection by validly cueing and low trust was also found in this replication experiment.

Bearing the ultimate goal of this line of research - improving banknote authentication - in mind, one factor worth considering is the extent to which participants in our follow-up experiment were helped by a prolonged viewing time. With respect to viewing time, it must be noted that in the study of van der Horst et al. (2020), visual information did

not help authentication much beyond the first second. With these considerations in mind we compared the average response times in the experiments. Participants needed on average 1.1 seconds in the first experiment for a correct response. In the replication experiment this was 1.6 seconds. Apart from the fact that in the replication experiment the participants were students, and did not represent the Dutch public, this particular finding suggests that a longer viewing time could be helpful. On the basis of this, central banks may want to communicate to the public that it helps to examine a banknote just a bit longer.

The present findings demonstrate a possible role for bottom-up saliency to aid banknote authentication. In this experiment, the manipulation of the banknotes involved the use of a pink frame around a security feature, but other design choices can be made. Future research should focus on the best way to present salient elements on banknotes. One could think of choices on colour, orientation, size and even motion which are generally considered to be guiding attention (Wolfe & Horowitz, 2017). Saliency should not negatively affect the esthetics of banknotes, so it would be useful to involve banknote designers in future research. Furthermore, while saliency should help in finding the security features, what to do next - i.e., how to use these security features for successful authentication - remains a challenge. Further research on making the security features more intuitive may thus be beneficial for counterfeit detection.

In conclusion, the present findings suggest that salient design elements may aid counterfeit detection. This cueing effect is also shown for perceptual sensitivity measures such as accuracy and d' (Bashinski & Bacharach, 1980; Theeuwes & Van der Burg, 2007). Invalid cues led to worse performance, so it is important that the salient design elements are solely at the location of security features. Additionally, as low levels of trust positively impacted authentication, we posit that the general public would benefit from increased awareness about the existence of counterfeited banknotes.

References

Bashinkski, H.S., & Bacharach, V.R. (1980). *Enhancement of perceptual sensitivity as the result of selectively attending to spatial locations*. Perception & Psychophysics, 28 (3), 241-248.

De Heij (2017). *A Model for Use-centered Design of Payment Instruments Applied to Banknotes: Upid-Model*. Thesis. Tilburg University.

De Nederlandsche Bank (2020). *Echt of vals?* Consulted on 5 January 2021. Retrieved from www.dnb.nl/echtofvals.

De Nederlandsche Bank (2021). *Daling aantal valse eurobiljetten*. Press release 22 January 2021. Retrieved from https://www.dnb.nl/actueel/algemeen-nieuws/persberichten-2021/daling-aantal-valse-eurobiljetten/.

Deutsche Bundesbank (2020). *Significant rise in number of counterfeit banknotes.* Press release 7 August 2020. Retrieved from Significant rise in number of counterfeit banknotes | Deutsche Bundesbank.

Drelie Gelasca, E., Tomasic, D., & Ebrahimini, T. (2005). *Which colors best catch your eyes: a subjective study of color saliency.* First International Workshop on Video Processing and Quality Metrics for Consumer Electronics, Scottsdale, Arizona, USA. Retrieved from: https://infoscience.epfl.ch/record/87215.

Egeth, H.E., & Yantis, S. (1997). V*isual Attention: Control, Representation, and Time Course.* Annual Review Psychology (48), 269-97.

European Central Bank (2019). *Annual Report 2019*. Retrieved from Annual Report 2019 (europa.eu)

Godwin, H.J., Menneer, T.,Riggs, C.A.,Taunton, M., Cave, K.R., & Donnel, N. (2016). *Understanding the contribution of target repetition and target expectation to the emergence of the prevalence effect in visual search.* Psychonomic Bulletin Review (23), 809–816. DOI 10.3758/s13423-015-0970-9

Klöne, E-J, Vrakking, T., & Zondervan, I. (2019). *A biennial study about knowledge and appreciation of euro banknotes among the Dutch*. Prepared for De Nederlandsche Bank by Motivaction. www.dnb.nl.

Kuzmova, Y., Wolfe, J., Rich, A., Brown, A., Lindsey, D., & Reijnen, E. (2008). *PINK: the most colorful mystery in visual search*. Journal of Vision, 8(6):382, 382a, http://journalofvision.org/8/6/382/, doi:10.1167/8.6.382.

Lau, J.S., & Huang, L. (2010). *The prevalence effect is determined by past experience, not future prospects*. Vision Research. 2010(50), 1469-74. doi: 10.1016/j.visres.2010.04.020.

Nanotech. (2021). *Banknote security and authentication*. Consulted on 16 November 2020, Retrieved from Banknotes | Nanotech (nanosecurity.ca).

Nocum, D., Brennan, P., Huang, R., & Reed, W. (2013). *The effect of abnormality-prevalence expectation on naïve observer performance and visual search.* Radiography. 19, 196–199. 10.1016/j.radi.2013.04.004.

Posner, I. (1980). *Orienting of attention*. Quarterly Journal of Experimental Psychology. 32 (1): 3–25. doi:10.1080/00335558008248231. PMID 7367577.

Raymond, J. (2017). *The Importance of Intaglio in the Authentication of Banknotes by the General Public.* Prepared by Secure Perception Research for International Banknote Designers Association. Birmingham.

Theeuwes, J., De Vries, G.J., & Godijn, R. (2003). *Attentional and oculomotor capture with static singletons*. Percept Psychophys. 2003 Jul;65(5):735-46. doi: 10.3758/bf03194810. PMID: 12956581.

Theeuwes, J., & van der Burg, E. (2007). *The role of spatial and nonspatial information in visual selection*. Journal of Experimental Psychology: Human Perception and Performance, 33(6), 1335–1351. https://doi.org/10.1037/0096-1523.33.6.1335.

Theeuwes, J. (2010). *Top-down and bottom-up control of visual selection*. Acta Psychologica, 135(2):77-99. DOI: 10.1016/j.actpsy.2010.02.006.

Theeuwes, J. (2019). Goal-Driven, Stimulus-Driven and History-Driven selection. Current Opinion in Psychology, 29, 97-101.

Van der Horst, F., & Matthijsen, E. (2013). *The irrationality of payment behavior*. DNB Occasional Studies 11(4).

Van der Horst, F., De Heij, H., Miedema, J., & Van der Woude, M. (2017). *Perception of public security features on euro banknotes.* A Qualitative survey on Confidence and Authenticity. IBDA INSIGHT 13, 53-55.

Van der Horst, F., Miedema, J., Snell, J. & Theeuwes, J. (2020). *Banknote verification, relies on vision, feel and a single second*. DNB Working Paper No. 680.

Van der Horst, F., Snell, J. & Theeuwes, J. (2020). *Finding counterfeit banknotes: the roles of vision and touch.* Cognitive Research: Principles and Implications 5(40).

Wang, B., & Theeuwes, J. (2020). *Salience determines attentional orienting in visual selection.* Journal of Experimental Psychology Human Perception & Performance · August 2020. DOI: 10.1037/xhp0000796

Wolfe, J. M., Butcher, S. J., Lee, C., & Hyle, M. (2003). *Changing your mind: On the contributions of top-down and bottom-up guidance in visual search for feature singletons.*

Journal of Experimental Psychology: Human Perception and Performance, 29(2), 483–502. https://doi.org/10.1037/0096-1523.29.2.483

Wolfe, J., & Van Wert, M. (2010). *Varying Target Prevalence Reveals Two Dissociable Decision Criteria in Visual Search*. Current Biology 20, 121-124.

Wolfe, J.M., & Horowitz, T.S. (2017). *Five factors that guide attention in visual search*. Nature Human Behaviour, 1, p.58.

Appendix

Replication experiment, presentation time increased

In line with our expectations, the 66 students, who were granted a longer presentation time, performed better than the panel. The average sensitivity for the no cue condition was 1.734, definitely higher than the sensitivity score for the CenTErdata panel of Dutch participants (0.386). This score is also considerably higher than a sensitivity score of 1.25, which is the norm that Raymond (2017) proposed for representing a reasonably good performance.

The influence of trust on the authenticity of banknotes was calculated with a GLM repeated measures. In this experiment higher trust influenced sensitivity scores negatively: $F(2,66)=4.103, p=.019$ (Figure 5).

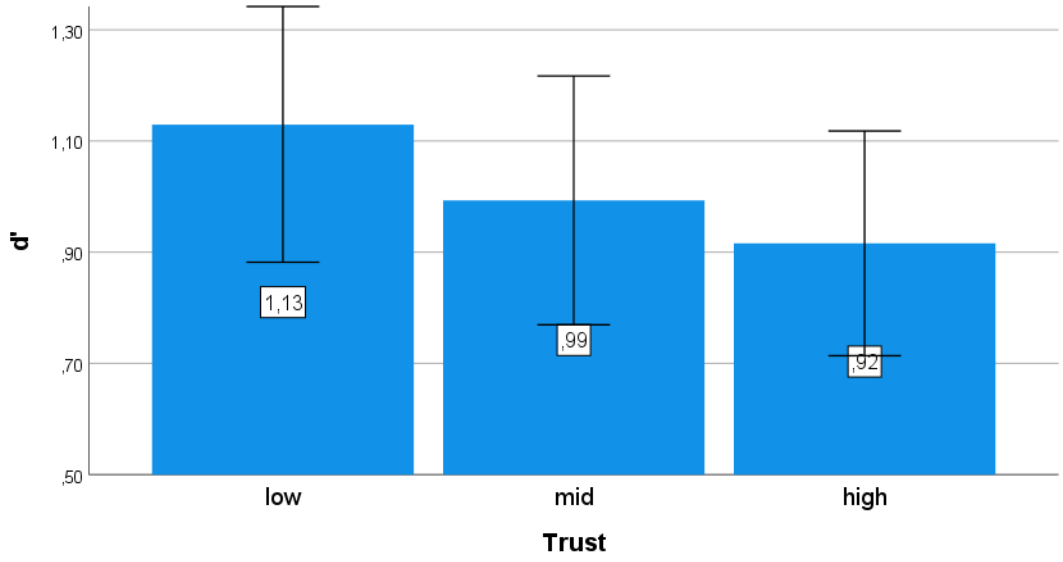

Figure 5. Average authentication sensitivity scores per condition of trust in the authenticity of a banknote (low, mid, high). Presentation time is until response. The sensitivity scores of participants significantly changed when the expectation of the ratio of counterfeits was varied. Error bars depict 95% confidence intervals.

The bias of participants increased with a lower trust in the authenticity of banknotes: $F(2,66)=3.684, p=.028$. This means that when the participants have low trust and expect a high ratio of counterfeits the criterion is also high. Such a bias is called conservative, i.e. not willing to make that much false alarms and taking the chance of lower hits. Conversely, a low expectation on the number of counterfeits leads to a more liberal criterion, i.e. that participants made both more hits and false alarms. See Figure 6.

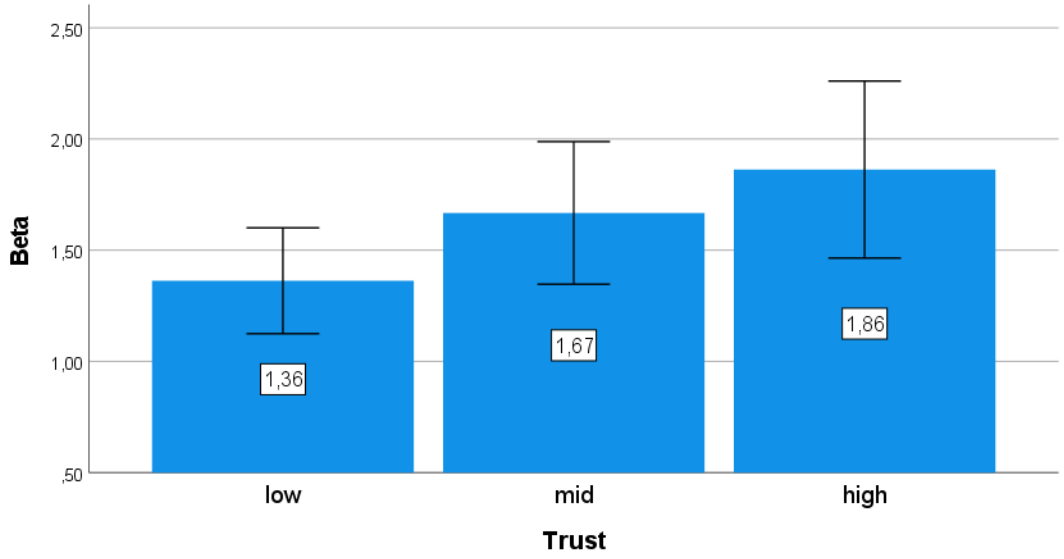

Figure 6. Average bias scores per level of trust in the authenticity of a banknote. When images were presented until response, a high trust has led to a more conservative bias, i.e. a lower tendency to declare a banknote a counterfeit. Error bars depict 95% confidence intervals.

Just like the experiment with participants from the CenTErdata panel, we found main effects for accuracy per cueing validity (F(1,66)=5.690,p=.020) and trust (F(2,66)=5.621,p=.005) and no interaction between these factors: F(2,66)=0.899,p=.401.

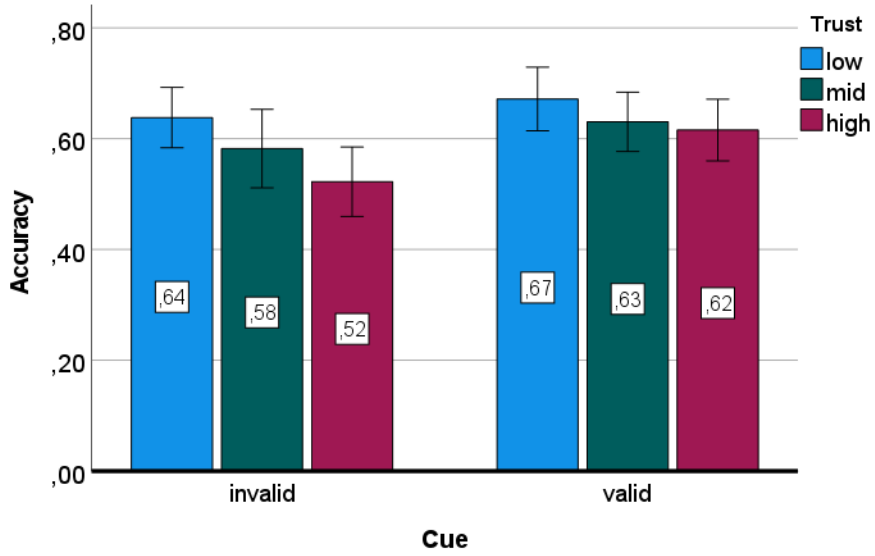

Figure 7. Average accuracy per level of trust (low, mid, high) and per valid or invalid cueing condition. Presentation time is until response. Both a low trust in the authenticity (i.e. a high expectation on the number of counterfeits) and valid cueing led to better performance. Error bars depict 95% confidence intervals.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl