NANOTECH

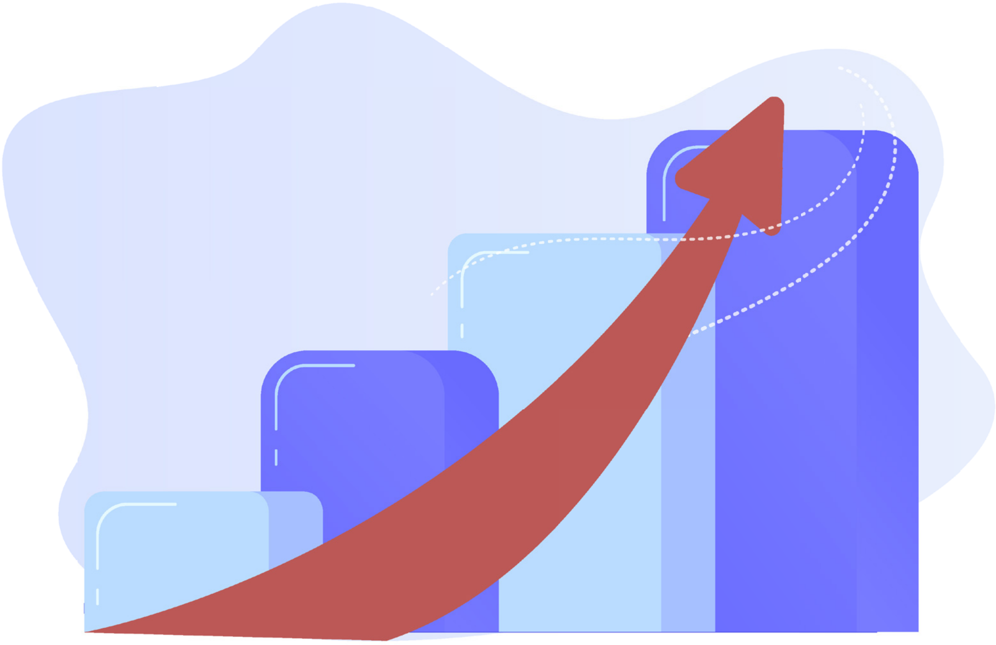
INDUSTRY INSIGHT

Designing Security Features

The best practices on designing security features with a user-centric approach

Overview

The global counterfeit market grew ~50% to USD 1.82 trillion in 2020, and bogus goods are a growing and global concern. Fake substandard products have become a major problem for companies that are trying to build and protect their brand authenticity and revenue. There are numerous contributors as to why this is a persistent global problem. Ambiguous security features on the market and a lack of next-gen technology to validate the authenticity of products are key contributors. In order to create a truly differentiated and useful security feature that can protect brands and their products the design process of the feature must be user-centric. We must pay close attention to how well the security product is received by those that will be using it. Is the security feature obvious and easy to use? Is it memorable? Does it actually provide authenticity protection? All these questions can be answered through rigorous design practices coupled with strong visual elements.



Phase one:

Research and Define

First, we must define our target audience. The audience can be divided into two major groups within the brand protection industry: brands that want to protect their products and consumers that want to purchase genuine products. Nanotech's research results show that most of the security features in the current brand protection market are easily replicated with traditional holographic technology.

Next, we have to identify the opportunity with current offerings available in the market. What security features are performing well, and what needs further improvements. Differentiation is crucial in introducing new products into the market, especially where the current solutions are lacking. feature and consumers end up having a difficult time validating the product efficiently.

To compensate for the lack of advancement in technology, manufacturers have been known to layer on multiple effects to enhance and dazzle their security features in hopes of creating a more secure product. With a complicated visual element presented in one single hologram, the result is often complex and confusing, breaking our goals of obvious, easy to use, and memorable. With complicated features, companies will have a hard time educating consumers on feature transitions and effects, and consumers end up having a difficult time validating the product.

Phase two:

Ideate

Even with the most innovative product in the market, if there is no resonance with the target audience, it will ultimately fail. Donald Miller, CEO of StoryBrand and brand expert once said: “People don’t buy the best products; they buy the products they understand the fastest”. The end goal is to deter counterfeit products by sending the right message to end-users in the easiest and most intuitive way possible, thus avoiding the need for significant user education. A great design should be intentional in every aspect and it should be evident that every element serves a purpose in reaching that goal.

At this stage, brainstorm ideas from multiple sources, collect data from market research, user feedback (the target audience) and be willing to iterate on designs and deploy new technology that can offer true security. Any ideas should be welcome at this stage as certain impractical concepts may lead to other great ideas during the brainstorming. To spark creative thinking, generate as many ideas as possible, and then converge once there is a clear direction to move towards.

Phase three:

Find the Right Solutions

With all the project requirements in mind, now move to the sketching phase. We want to create security features that are intuitive and memorable. There are many ways to achieve this. Below are some of the design tips that can aid the process:

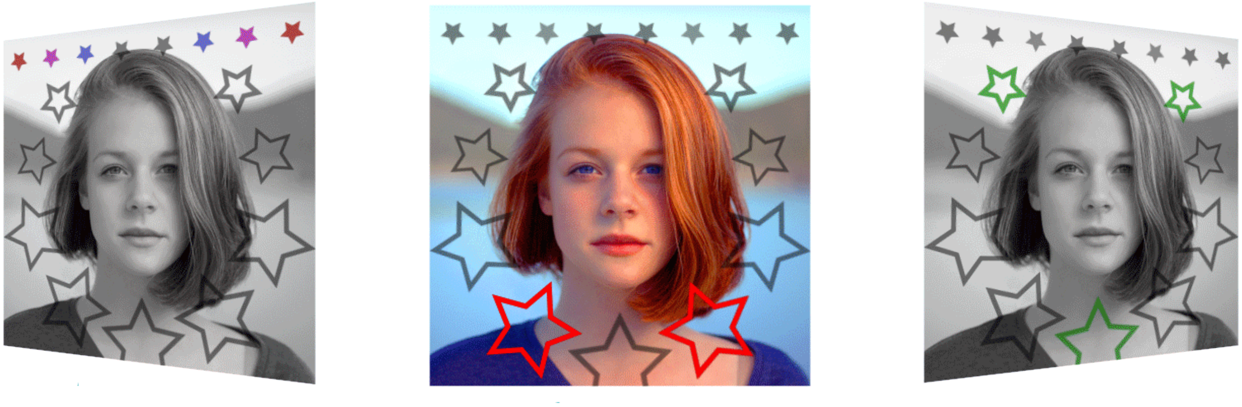


Figure 1: An example of our LivePortrait feature demonstrating our full RGB high-resolution ability

The Visceral Effect

The Visceral effect in design is the most primal feeling one gets when looking at something for the first time, also known as "love at first sight". People are more willing to learn and adapt to new things if the appearances are pleasing to the eye or have unique effects that the brain can quickly understand.

Nanotech's LivePortrait product is an example of the visceral effect in practice. With the combination of our patented nano-optics and our state-of-the-art electron beam lithography machine, we delivered something quite differentiated from traditional holography and its chaotic rainbowing effect and created something unique, memorable, and secure with features like 12,700 ppi resolution, true colour RGB, and photorealistic images. The end result is the potential to create a bond between the brand, its products, and the consumer. The security feature is easily recognizable and allows consumers to intuitively authenticate the product by noticing features like the "true red lips", "blue eyes", and "red to gold colour shifting hair".

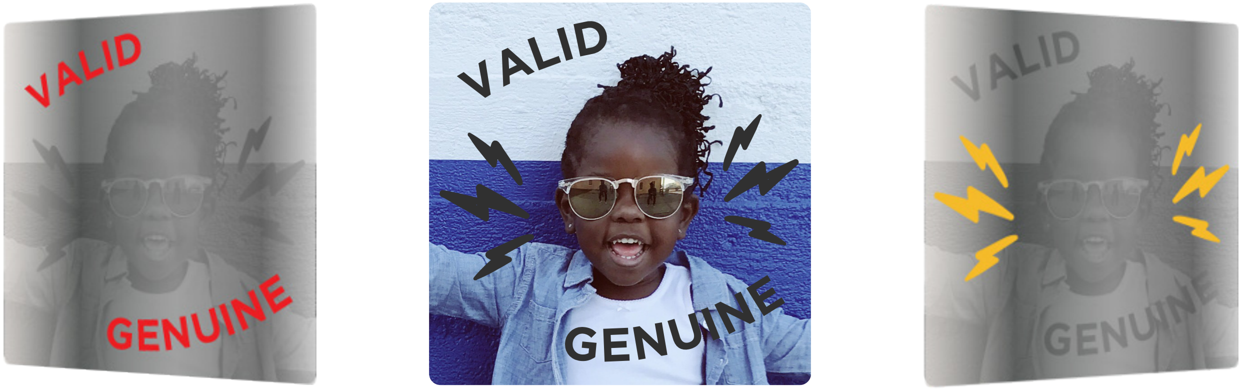


Figure 2: An example of our LivePortrait feature demonstrating our full RGB high-resolution ability

The Von Restorff Effect

When we are designing an image-switch effect, we want the end-users to be able to identify the authentication markers immediately and this is where the Von Restorff effect comes into play. The Von Restorff effect is when an item that stands out from its surroundings is perceived to be more memorable. With this in mind, we want to put changing visual elements at specific locations that are pleasing to the eye. Utilizing photography "rule of thirds" is one method to achieve this. In addition, toning down the remaining visual elements helps the user easily notice an image transition, ultimately grabbing the user's attention.

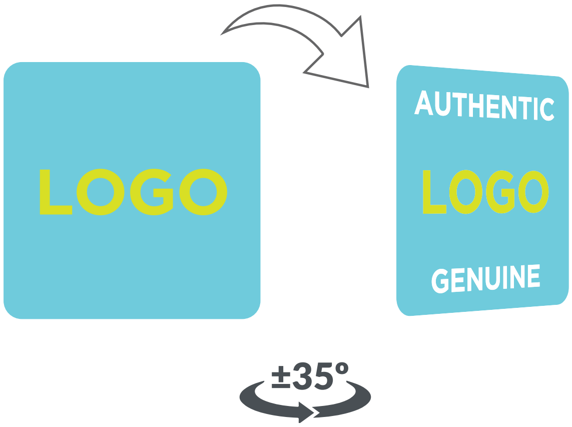


Figure 3: Easy activation simply by tilting the feature

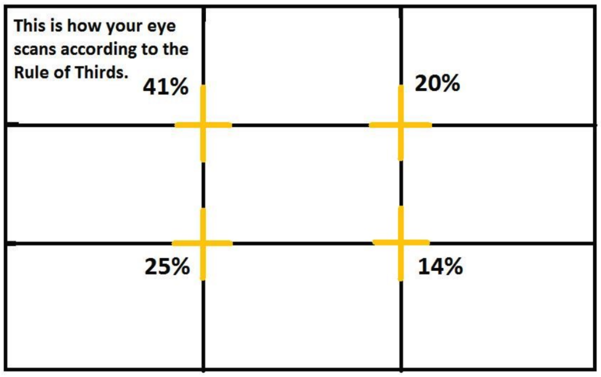


Figure 3.2: Rule of Thirds in composition

The Behavioral Effect or Usability

The behavioral effect is the product experience that we create for the users. The less effort required by users to notice an effect the higher chance for them to have a positive experience. Positive experiences promote engagement; users should be able to interact with and understand a security product with minimum effort. Is the product easy to use? Is it memorable? Is large movement of the security label required to get the maximum movement within the label? Is the location for authentication markers in the prime areas? Is the text legible? Is the contrast noticeable? These are some of the questions we need to answer when we create a security feature. Think from the user standpoint and what can be done to enhance their experience. For instance, when users are tilting the security feature, they would expect to see a strong transition effect or crisp change as advertised by the original manufacturer rather than a slight change that is hard to notice. If the behavioral effect is complicated or poor, it can end up creating a negative user experience. In contrast, a strong behavioral effect, will increase usability of a security feature and help users detect genuine products and protect them from counterfeits.

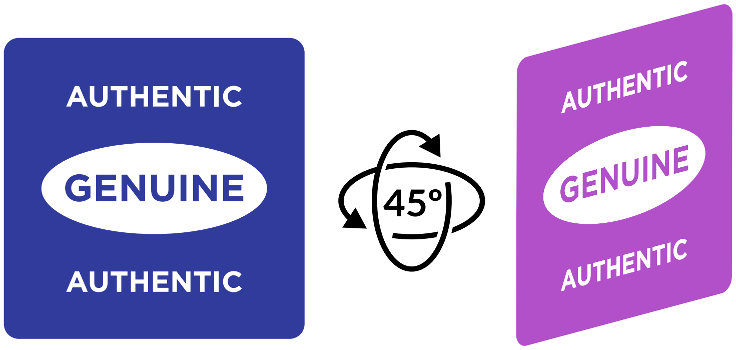


Figure 4: Nanotech's LumaChrome PSA label has a vibrant colour shifting effect regardless of the direction of tilt

Hick's Law

People may have heard the terms, KISS for "Keep it simple, silly", or "less is more". By lowering the user's cognitive load, it will increase the overall usability and effectiveness. When designing a security product, keep the design elements that are essential and eliminate elements that do not clearly serve a purpose. Users are constantly bombarded with information and the simpler the security product is the more memorable it will be.

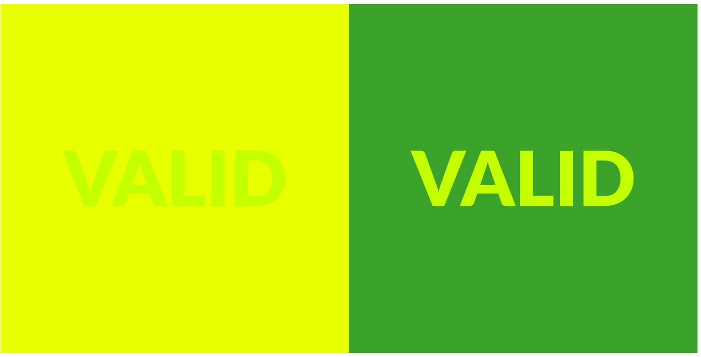


Figure 5: Both 'VALID' words have the same colour values but the right side is more prominent than the left due to higher contrast

Contrast and Colour

Contrast creates focal points and can grab a user's attention. Contrast is created by the use of varying colours, textures, sizes, and shapes. With contrast, designers can direct users on what and where they want them to focus. When we are designing security features, we want to create an instant "wow effect" because users tend to quickly make an assessment on the security feature and thus are quickly validating the product. Users need to immediately know if the product they are going to purchase is either genuine or not. The security feature designer's role is to perfect the contrast, colour, and other previously noted design elements to deliver a fast authentication experience. Bright colours stimulate the eyes, and the eye is also more sensitive to certain colours than others. We also need to consider colour theory, brand colours, and colour psychology since they are all client-specific and can be used as needed.

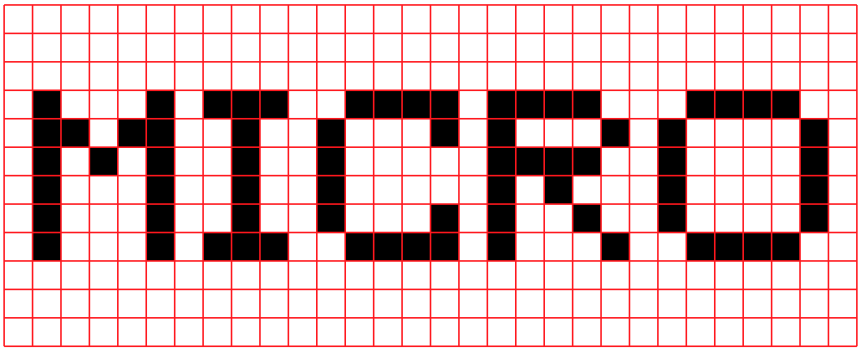


Figure 6: San serif renders more clearly in small pixel grid

Typography

The most common categories for typeface are serif and san-serif. The easiest way to distinguish the two is to look for the ornamental ‘feet’ or the serif. Selecting the right typeface is extremely important in our design. The main purpose of our products is to communicate with end-users in the most effective manner. San serif is considered more approachable which allows the brain to relax and function more efficiently. Security feature product sizes vary and selection of a typeface like san-serif ensure legibility even at small sizes. Other elements to consider for typeface are legibility, compatibility with brands and logos, and whether the typeface is pleasing to the eye.

Phase four:

Prototype, Iterate, Manufacture

Once we have selected the most effective solutions to protect our product, we want to produce working prototypes so that we may optimize the security feature itself and the manufacturing processes. Creating samples, gathering target customer feedback, and iterating on the design is critical to validate the success of the product before product launch. When all stakeholders are satisfied with the security feature design and pre-production samples, we are ready for volume manufacturing.

Conclusion

Security feature design is an iterative process that requires multiple stakeholders, with varying expertise, to deliver a successful authentication product. Overall, there are many key design methods used in reaching the goal of designing a security product that users can and will use to validate their potential product purchases. The most important aspect of a great feature is to always think about the relationship and interaction between the end- user, the security feature, and the end product. Simple and memorable security products with unique effects that are differentiated from the easy to copy, generic solutions on the market today will help users and brands meet their authentication needs and stay a step ahead of the growing global counterfeiting industry.