Common Pitfalls in Selecting Anti-Counterfeiting Technologies

by Deepak, Professor
National Center for Flexible Electronics, IIT Kanpur
Email: saboo@iitk.ac.in

It is difficult to call out a start date for modern printing. But, if we regard invention of Gutenberg's printing press in 1450 AD as that, introduction of anti-counterfeiting technologies on printed packages is similarly dated soon after. Yet, counterfeiting grows year-on-year. That suggests a need to take a pause and re-evaluate the approach to addressing the issue of counterfeiting. To be clear, we are referring to counterfeiting as the one where a buyer is duped into buying a counterfeit; in contrast, where the buyer is aware and still buys a knockdown or grey market product knowingly, is excluded in this discussion although that may also be a concern in some ways e.g., brand erosion if not direct revenue loss. Also, excluded are non-consumer facing products, such as Passports, where authentication is done by specialized personnel.

Consider the following aspects to establish the right approach to select anti-counterfeiting technology for consumer products.

1. **"Consumer" vs "Thief" as the focus while selecting anti-counterfeiting technology.** Brands always keep consumers at the center of everything they design, not just the product but also when they select anti-counterfeiting technology. Regarding anti-counterfeiting technology they work on the premise that the consumers will go by the manual and religiously use the provided technology in big numbers to verify authenticity of their products and blow the whistle when they come across fakes. The fact of the matter is that consumer behavior is not to do this, irrespective of industry or strata of society or any other segment of people one can think of. To validate this assertion, observe our own and behavior of those around us, whether as a consumer we scan/scrutinize a product to establish authenticity before buying. When asked this question, the answer we found is that we rarely scan for authenticity. This suggests a very simple change of our design approach then. Rather than focusing on end consumer to design an anti-counterfeiting technology, address the source of the counterfeit sale – a dishonest retailer/distributer/wholesaler, as the case maybe and hence forth called "*Thief Retailer*". And there is a difference in approach when we do that, as illustrated below.

   When designing a product, obviously with consumer focus and one that sells, based on the consumer segment, market and other factors one could follow a Design-To-Cost approach by trimming down or upscaling features, suitable ergonomics and what not. Unlike product design, anti-counterfeiting technology design has to have a black or white outcome, no shades of grey are permissible. This is very similar to the example - when you leave your house having four doors, is it prudent to lock three doors and leave one open and be content that you are 75% secure? Indeed, we lock all the doors. **This is a difference in consumer and thief-focused thinking, that is, you cannot lower the standards when protecting a product and protection strategy is directed at thief**.

   Suggestion: In selecting anti-counterfeiting technology think of protection from Thief Retailer, not convenience of the consumer. This has critical implications. For example, a technology may require an App, which we already know few people download, and hence may be rejected on account of consumer-focused thinking. But that we will show will be a mistake, when one thinks like a thief.

2. **Fear in *Thief-Retailer* as a means for preventing counterfeits.** We have asserted, as consumers, even when a brand provides a means of authentication of its product, we rarely check. Hence, ad nauseum (yes, that is what has been happening) thinking of consumer as a defense against counterfeit is a mistake. Instead examine the psychology of the *Thief Retailer*. Would he sell fakes if he fears getting caught? Answer is no. Do most technologies prevalent in market capable of making a *Thief Retailer* fear? Answer is no, as we show in the Table after establishing the parameters necessary to evaluate a technology. This is because with most of the existing technologies, a *Thief Retailer* has an escape route when caught selling a fake product. As long as a *Thief Retailer* is able to feign ignorance and himself claim to be a victim at the hands of from who he has bought, he has an escape route. This implies, the solution to prevent or deter the "Thief Retailer" from brazenly selling counterfeit products would be to design anti-counterfeiting technology that increases the risk of getting caught. We emphasize the same via the following real example.

   Theft is reported on a factory floor of a manufacturing unit. Floor Manager deploys a large number of cameras for surveillance with a pamphlet pasted in bold below each of them - "you are under the camera surveillance". Irrespective of whether the cameras are functional or not, guess what? no more theft is reported. Why did this happen? By merely instilling a fear in the minds of thief – of increased probability of getting caught red handed. This is a real story narrated by a factory owner, where only a few cameras were in a working condition.

   Suggestion: It is not necessary that consumer (and others) check authenticity of a product, the threat of ability of consumer, retailer, brand inspector or anybody to be able to unambiguously check the authenticity is sufficient. If technology is such that it can establish complicity of Thief Retailer with certainty, and one that can be used to obtain conviction, then it would deter Thief Retailer even more. This we believe is a new approach to anti-counterfeiting.

3. **Can hidden features, scratch codes, or complicated technologies requiring specialized equipment for authentication protect consumer goods?** Answer is clearly no**.** All these options do not allow the retailer to authenticate. If the *Thief Retailer* and consumers are excluded from ability to authenticate, then seller of fakes would have ready excuse for not being able to recognize a fake, and he is able to get away as a "victim" rather than a thief. Hence, only **overt technology** which can be authenticated by any retailer or consumer are proper technologies.

   Suggestion: Ability to authenticate must have a characteristic that it can be accurately authenticated by <u>anyone, anywhere, anytime</u>. This also implies that the security feature/tag must be overt. In short, complete democratization of the power and means to authenticate is required.

4. **Is Web/URL, SMS or WhatsApp based authentication reliable?** As elaborated in point 2, the pathway to preventing counterfeit is to instill fear of getting caught in *Thief Retailer*. If a counterfeit product also has equivalent fake or misdirected website (phishing/script spoofing), SMS or WhatsApp number included with the product and the authentication is devised to always confirm genuineness, the *Thief Retailer* gains the ability to deny his

involvement, that is, he claims how could he have known that the product was fake. Therefore, if authentication is to be done by accessing internet/data transfer, it should always be through an App which is to be downloaded only from Play store or Appstore. These Apps prevent misdirection. A Consumer-based thinking may regard an App download as a negative, but as elucidated in point 1, for protection of a product, the thinking needs to be *Thief-Retailer*- focused in order to create fear, as explained in point 2. Taking away the option of deniability by *Thief Retailer* works to create the fear, which as explained here would only be available through an App. The actual download of App and subsequent check of authenticity by consumer is not necessary, it is the **threat of** ability of consumer and retailer to download the App and check for authenticity that creates fear in the minds of *Thief Retailer*; in any case, he does not know which consumer will download an App and check. Nonetheless, this is a classic example where in empathy with the customer/consumer rather than threatening the *Thief Retailer*, brands often make an error in selecting a technology, for example, Web/URL instead of an App, despite knowing the fact few consumers actually check for authenticity irrespective of whether it by an App or not.

Suggestion: Rely on App on a mobile-phones for authentication. Ease for consumer who rarely checks for authenticity is not a priority. The availability of App works as the presence of caution "you are under the camera surveillance". Whether or not App will be downloaded is not important, reliability is and seller of fakes does not know which consumer may end up downloading an App. Web/SMS/WhatsApp are open to abuse, hence unreliable. In short, the threat has to be reliable also.

5. **Can technology be two-dimensional if authentication is with a smart mobile/cell phone?** All two-dimensional overt features can be copied to the scale that a mobile phone camera *sees*. The design of any anti-counterfeiting technology that uses a mobile/cell phones in the hands of consumers has to be designed for phones of lowest camera standards. Moreover, some users have more shaky hands than others, yet technology should work for all users. In other words, some level of focus and motion blurs are common in the pictures taken by users. That limits the size of features in the image that are to be used for authentication. If a technology provider uses very small features to prevent copying, then the genuine product also faces great deal of problems in authentication due to the small sizes involved. And if feature sizes are of scale that are easily seen in the picture taken by a mobile phone even when the picture is a bit blur, then at that level making a copy of two-dimensional picture is easy. In some cases, mere photocopy will do. For more sophisticated designs, it is simple enough to take a professional quality picture of a genuine tag, perhaps using a macro lens or even a microscope and then editing the picture until the print of picture mimics the original.

   Suggestion: The overt security features in a tag should always be three-dimensional.

6. **Role of advertisement of available anti-counterfeiting technology on a product.** It is important to also advertise the technology that is available to ascertain genuineness of a product. First purpose it serves is that fake products without security features are not sold. The other purpose is to create a fear in the minds of *Thief Retailer*. Normally, advertising to reach consumers is a tough and expensive task. But, here only pretensions of reaching out to consumer are sufficient. In other words, ostensibly the target of advertisement is the consumer, but we are targeting the Thief Retailer, who when notices such advertisement perceives further risk of getting caught.

Suggestion: Based on scan reports, identify the regions where more counterfeits of a product are sold. Advertise in that region, so that Thief Retailer perceives greater risk of App downloads and checks by the consumers.

In conclusion selecting a proper anti-counterfeiting technology hinge on two aspects/criteria.

1. **The authentication should be reliable and available to anyone, anywhere and anytime**, implicitly meaning that a *Thief Retailer* should also have ability to authenticate. This, so that he can't claim that he did not know that product is fake. This is important to increase the risk perception of getting caught in a *Thief Retailer*, leading to dissuading him to sell fake products. A corollary of his approach is that, for example if mobile phone is being used, then App be used in favor of Web/URL, SMS or WhatsApp based authentication, regardless of number of App downloads.
2. **The physical tag that is attached to the product and used for authentication is unclonable.** Otherwise, if the tag gets cloned, then however good is authentication, the response always will be genuine even for a fake/copied tag. Also, important is to clearly define what is meant by unclonable tag. Only the tags made by nature, implying random features (not numbers), similar to human finger print, can be unclonable. Any tag that is engineered and made by people, implies those making it will be able to make it again and again, which automatically violates the definition of un-clonability. Often, difficult to make tags, for example advanced holograms or two-dimensional tags with hidden or copy detection patterns, are pushed as unclonable, which they are not. In short, unclonable tags are those which even the manufacturer of the tag cannot make it again, implying the features of tag must emerge by some natural processes, such as human finger-print. This also implies, if a smart phone is being used for authentication, then two-dimensional features will not work, requirement will be a three-dimensional tag with features of sizes that can't be printed by even a 3D printer; in any case, 3D printers are too slow for any mass production.

We also comment on digital protection, such as blockchains. First, it should be clear, any physical product that is to be protected would have to have a physical identifier that triggers the blockchain response. So, while the blockchain may be very secure, if the physical identifier is copied, then blockchain would return the same answer for both genuine and fake products. And if the physical tag is made unclonable, there is limited justification for using blockchains for authentication.

In closing, if either of these two criteria are violated, the anti-counterfeiting technology is no good. Measured against these two criteria of technology selection, in the Table we provide how most available technologies fail. Often even when any of these technologies are adopted, for a short period, it shows good results, but only because the counterfeiters are taking few months to adapt to the change. As has been the experience, after few months, the counterfeit products are back again in the market and brands seek yet another technology. Hence, we recommend that rather than constantly changing the technology, it is much better to delve into strategy of anti-counterfeiting and then select the technology accordingly. The strategy and consequent parameters on which technology should be measured is provided here.

Technology	Working	Unclonability	Reliable Authentication	Comment
Hologram	3D images created by interference of light waves. Essentially a visual object that changes color on tilting	X	X	1. Holograms could be difficult to replicate, but supplier makes identical copies again and again, meaning it is clonable; 2. Authentication is visual, specifically a changing of color upon tilting. So any hologram does the job, allowing counterfeit seller to deny his involvement by affixing an approximate hologram
QR Code	Standard 2D barcodes that store information such as URLs or other data. It is only a machine readable script/form	X	X	1. Any photocopy would work to make a clone; 2. Once QR code is cloned/copied, the response of authentication is the same for both genuine and fake product, allowing counterfeiter to deny his involvement under a plea that his authentication yielded genuine result
QR code with Web, SMS or WhatsApp authentication	The authentication is through a website, SMS, or WhatsApp number	X	X	1. QR code is anyways clonable; 2. On top of it, authentication is by directing to a website, SMS or whatsapp number. A fake site or phone number of counterfeiter always authenticates the product. This allows counterfeiter to deny his involvement under a plea that his authentication yielded genuine result.
Encrypted or Dynamic QR codes	In one case, the content that is in the QR code is encrypted. For dynamic QR code URL (website) is a fixed address, but the user is redirected from this site to some other site which can be changed in time, making it dynamic	X	X	This has no direct relation to authentication and security; for example, encrypted or not, once QR code is copied it behaves like a genuine QR code. These are backend technologies, used for other conveniences, nothing to do with establishing product genuinity.

Technology	Working	Unclonability	Reliable Authentication	Comment
QR Code based Track and Trace	QR code is for machine reading and product is traced through the supply chain	X	X	1. QR code can be copied; 2. Once QR code is copied the response of Track and Trace system is same as that for genuine product. Strategies such as the first scan of a QR code will be regarded as genuine and second one as fake are ingenuous, as genuine product may be scanned multiple times. Brands that adopt this technology start receiving complaints and as a consequence they quickly turn off the customer facing response
Hologram+QR code	Two independent technologies offered together	X	X	Comments both for Holograms and QR codes apply here
Copy Detection Patterns with or without QR codes	A known random pattern gets distorted or there is dot gain effect when photocopied. The distorted pattern is authenticated/caught by an algorithm on App, or a server where picture is sent through a weblink. A variant is to impose a random pattern/distribution on a QR code, making reading of QR code difficult. But during authentication an algorithm removes distribution and hence QR code can be read	X	Y	1. As a principle, any 2D graphics can be copied intelligently; 2. This technology only protects against common photocopy. But an experienced counterfeiter would take a high optical resolution picture with a macro lens/microscope, edit out distortion, if any, and then print to clone; 3. Authentication can be reliable if done by App, website based authentication is always prone to misdirection, providing option of excuse to the seller of counterfeits.

Technology	Working	Unclonability	Reliable Authentication	Comment
Embedded image in package artwork (microdots, hidden patterns, encrypted)	There is an image in package artwork. Claims are of included microdot, hidden patterns, encryption (which are all irrelevant in making copies of an artwork image)	X	X	1. Readily copied, since it is only 2D; 2. Those selling this technology use web based authentication, which is not reliable
Multiple small images with orientation relationship	Small images are used, and together arranged in a pattern with fixed orientation relationship	X	X	1. All 2D patterns to be verified as picture from a mobile phone are readily copied; 2. Web based authentication is unreliable
Scratch Code	A part, for example a long number, is covered under a scratch code, and the random number completes only when consumer scratches the code	Y	X	1. As long as the number is covered, the technology is unclonable; 2. Authentication does not meet the criteria of anyone, anywhere, anytime. Since it excludes the retailer, the retailer has the excuse to feign ignorance
Passive RFID	RFID tag that is authenticated by a specialized device that also powers the tag	X	X	1. Passive tags can be programmed to return the same values as a genuine tag and hence can be copied 2. Authentication is by a specialized device, hence the seller of fakes does not have ability to validate, allowing him to feign ignorance.
Active RFID	RFID tag has its own power to emit radiation and authenticated by a specialized device	Y	X	1. Active RFID tag can have embedded encryption in silicon chip itself and hence unclonable; 2. Authentication is by a specialized device, hence the seller of fakes does not have ability to validate, allowing him to feign ignorance.

3D Self Generated Random Patterns (Checko)	The patterns are generated in 3D form by cracking of ink. Authentication is by an App that matches the pattern and recognizes 3D structure	Y	Y	1. Since the tag is formed by natural process and is 3D, it is unclonable; 2. Authentication is by algorithms, AI and mathematics, offered through an App and available to anyone, anywhere and anytime, aking is reliable.