Understanding Anti-Counterfeiting

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

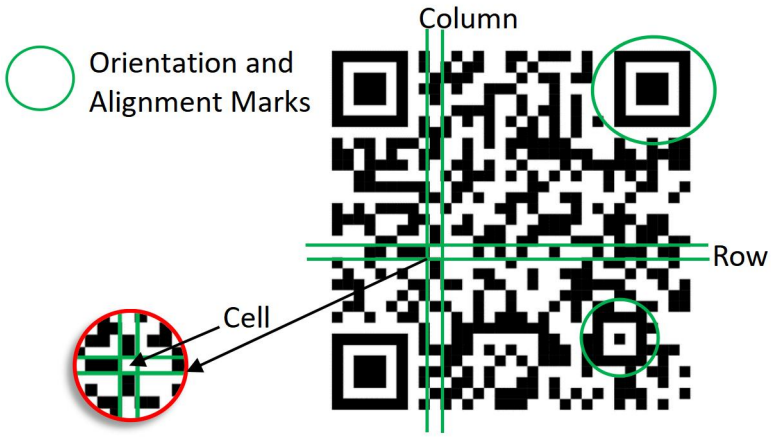
Starting with Watermarks, anti-counterfeiting technologies have been around for more than 300 years, why does counterfeiting still happens?

Security features that set the basis for authentication in past primarily relied on a combination of overt and covert features, such as latent images, watermarks, color changing inks, fluorescent inks, guilloche patterns, micro dot, etc. Most of these were known only to brand owners to be able to inspect and identify fake products. This poses a limitation, because the person selling fake product upon getting caught would be able to feign ignorance and claim to be a victim himself. And to establish veracity of the feigned ignorance, police or judicial action is time consuming and rare to make a dent in anti-counterfeiting. Alternatives are overt features observable to a consumer such as holograms, visible to the eye. But these can be copied, and more importantly, purveyor of fake products need not even make an exact copy, because a consumer observes only a shiny and changing pattern upon tilting and does not know exactly what pattern to observe.

However, with the advent and proliferation of smartphones in the hands of consumers, the focus has shifted to inserting hidden features in the artwork. Earlier, these hidden features could only be detected by experts, but now the same expertise is being automated through imaging with smartphone cameras and algorithms implemented on servers or smartphones of the consumers. But technologies in this class have serious flaws. Bottom line, you only need to copy what a phone camera will see. And that is easy to copy, hidden features or not.

But, so many companies are providing QR code that either provides the product information or it takes to a website where all the necessary information is available. What are they?

To answer this, we need to understand QR codes themselves. The advent and proliferation of Smart Mobile Phones has made the presence of “QR” or Quick Response code ubiquitous. Although, technically, QR code is a specific type of data representation among two-dimensional bar codes, its popularity in common parlance includes other forms, such as Data Matrix and Aztec. A QR code is a square image, internally divided in a matrix of rows and columns, forming a collection of cells, just like those in Microsoft Excel. QR code also has few large features in it, as indicated below, which are used to determine orientation and alignment of the QR code. The data in a QR code is represented by filling each cell with either black or white color (or two well contrasted colors). These two color indicators are interpreted as 0 or 1, in computer’s script (yes, a smartphone is also a handheld computer!). Effectively, just as we could translate written text from one language to another, a QR code is simply a text translated, most commonly from English to a script that computers can reliably interpret.



It is pertinent to note at this point, had a computer been made to interpret an *image* containing English/Latin script (or any other language), it would have used Optical Character Recognition (OCR), which is often unreliable – thus the motivation to use a reliable QR code instead.

For reading back the QR code, the phone's camera captures the image and an App (Application), often pre-integrated with the camera of a smartphone, performs a reverse translation back to English and displays the text on the screen. As an incremental feature of the App, when it sees the text to contain a URL, the App also opens the website on the browser. In short, reverse translation and redirection to a website are features of the computer program that resides on the smartphone, whereas a QR code is merely a translation of human readable script, for example, English, into a script of 0 and 1 or black and white. That also implies that intelligence lies in the App on the mobile phone, and not in the QR code. Hence, QR code is mindless but together with App it appears intelligent.

And why can't they provide authentication or anti-counterfeiting function?

Lack of intelligence in QR code makes it pointless for authentication/detection of counterfeit goods; the same data as in the original when first read, reprinted, and then repasted on a fake good, will return the same text/message as the original. That is, the QR code is cloned while the intelligent part of the solution continues to respond as it would for the original. Furthermore, it is also open to phishing attack, that a minor change in URL link (web address) embedded in the QR code takes to a counterfeiter's website! For example, can you spot the difference between https://checko.ai and https://checko.ai/? They are two different websites, first having ordinary (ASCII) 'e' and other having Cyrillic 'e', indistinguishable by human eye; some browsers will even warn for the second version.

But, then there are Cryptographic/Encrypted and Dynamic QR codes. Can't they work?

This is another misrepresentation of QR codes through this misleading terminology, which refers to backend operations. There is nothing dynamic about the QR code, once printed the QR code remains the same temporally. Dynamic QR code also send users on to specific web pages, just that what makes them "dynamic" is that the URL encoded in them redirects to a second URL that can be changed on demand, even after a code is printed. So a fake "dynamic" QR code will perform as the original. Similarly, encrypted QR codes are not much different. It is the data represented in the QR

code that is encrypted and then it is the App that interprets it back after decrypting. Hence, neither Dynamic nor Encrypted QR codes can provide any security against duplication of QR code itself.

However, QR codes are good for automation in track and trace or traceability, where honesty is assumed, whereas no authentication is possible, which deals with dishonesty.

So what is the difference between Traceability and Authentication?

Traceability of goods moving through a supply chain is about recording the events/movements during the journey at every stage and later recalling it when needed. It plays a vital role in managing the supply chain, for example, monitoring inventories in real-time, sales in geographical locations and months of the year, managing quality control, returns, regulatory compliances, etc. Traceability assumes honesty that the item that is being tracked is a genuine product. Authentication, on the other hand is a means to establish genuineness. Hence, these two are different functionalities to serve independent purposes.

(There is yet another term called Identification, as opposed to Authentication. Without going into details, the difference can be understood from an example. In Aadhaar system, I present myself with my fingerprint and Aadhaar number and ask to be validated that I am who I am claiming to be; that is authentication. For identification, a fingerprint is lifted from a crime scene, and now the job will be to identify who the person is, a far more laborious task.)

Then, how do we do authentication to protect the consumers and brands alike?

Technology comes later. First we have to be clear what the strategy for anti-counterfeiting will be. The people who make fake products are illegitimate businessmen engaged in illegal business. But, they remains hidden, and we get to know of them occasionally when reports of some raids appear in newspapers. That hardly make a dent to counterfeiting. Nonetheless, this counterfeiter has to sell his goods. To do so, he must make a deal with the retailer who has consumer connect. The retailer is a legitimate business owner, sitting in market place, facing the consumers, brand agencies and law enforcers. Then, why does he assumes the risk of selling fakes. Remember the first principle of financial crime. It is committed only when one assesses risk of getting caught to be low. So, that tells you, that retailer does not fear the existing technologies, for he has deniability. The fake product also having QR code as the original or a hologram, which may even be approximate, allows retailer to feign ignorance, as to how would he know that product is fake. So we need to close this loophole and technology needs to ensure that retailer knows, once caught, option of deniability, feigning ignorance or pleading that he himself is victim is not possible.

What would be necessary features of such a technology?

Think of humans also as physical object and we do authenticate them. For example, fingerprint, IRIS scan or facial scan serve that purpose because they are unique and unclonable. For example, fingerprints are good means to authenticate a person and are commonly used. The same ought to be done for products too. We need a copy-proof or unclonable identifier on each product that is to

be authenticated. And we need a reliable means for validating that fingerprint anywhere, anytime by anybody.

Since mobile phones are carried by everyone, perhaps, using camera for imaging and computing power of the phones unleashed through algorithms in form of Apps is the way to go.

But, in the opening it was said, technologies using mobile phone to detect hidden features are having flaws.

That is correct. Not doing it right is problematic. We will refer *tag* to the label affixed on the product, having a set of unclonable features in it, which is used as identifier or means to establish genuineness of a product. When an original tag is scanned and reprinted after high quality scan and subsequent printing, the pattern on the tag is reproduced. However, no reproduction is ever exact, there are aberrations from the original. The objective of inserting hidden features in artwork and then their detection with a smartphone is to catch these aberrations in a copy.

A counterfeiter need not reproduce a tag identically. He only needs to reproduce the image that passes the detection system, such as mobile phone. Hence, the relevant question here is at what scale these aberrations happen and is the smartphone imaging them capable of capturing these aberrations. Else, such technologies are meaningless.

Note that even the commercially available reproduction systems allow aberrations only at 10-100 micrometer size levels; larger sized features of the original are well reproduced. Further, we would require authentication system to work with all types of smartphones, including low-end camera phones in the market. First these low-end phone cameras are incapable of capturing aberrations of such small sizes. Also, we all have noticed many-a-times pictures that we take show blur due to lack of focus or motion blur due to shaking of hands. The latter makes even high-end cameras inconsistent in capturing an image that reveals the needed aberrations from the original. Hence, a fake also gets detected as genuine. Most certainly, when also accounting for the user casualness in taking pictures, that is, tilting of camera, poor alignment and shaking of hands, usage in variety of lighting conditions or partial shadows on the tag, this approach of inserting hidden features in artwork miserably fails.

This explains the unviability of 2-D images with hidden patterns for anti-counterfeiting. But additional options from traditional technologies are also prevalent, which we explain by another example along with a warning that each of them can also be readily duplicated, as in this example. A set of closely spaced curved lines or even Guilloche pattern (Spirograph-like curves) generated algorithmically are seen on currency notes or passports as additional visible security features; sometimes even deliberate ‘mistakes’ are inserted in the design. When these patterns are scanned, Moire patterns or, in general, interference pattern from reflected light, distort the scanned image. Even certain copiers are designed to refuse to copy such features as a matter of country specific regulation. Strong legislation, laws enforced scrupulously by State’s security agency and control over equipment and inks can protect, for example, currency in a jurisdiction. But, then outside the jurisdiction, fake currency is printed. The point here is, technically, it is not impossible to reproduce the same pattern. And with no equivalent level of protection available for commercial products, such technologies fail to provide protection against fakes. We will not get into how a duplicate pattern will be made, except merely to say commercial software is available to remove the

distortions caused during scanning of the original; note minute features are routinely made using such software in lithography masks for production of semiconductor chips. In another instance, what is offered is appearance of text such as 'void' when a copy is made. But even these can be removed through the same software before reprinting.

That sets the requirement on the nature of the fingerprint that is to be used as identifier through which authentication is to be done. Authentication by smartphones of tags having two-dimensional artwork is not possible or, at least, not reliable. This necessitates having a three-dimensional pattern and, equally, a requirement of having capability to detect it by a smartphone through an App.

How would be a tag/identifier linked to the product be made copy-proof or unclonable?

It is clear that the tag should be three dimensional, because any 2D feature set can be copied. Further the three-dimensional pattern itself should be unclonable, otherwise obviously a counterfeiter would also make similar tags. In this regard, it is also important to define what is unclonable. In the scientific literature such unclonable features are known as Physically Unclonable Functions (PUFs). Since these cannot be duplicated, the features serve as unique identity (or call it fingerprint) for each unit sent to the market. The person wanting to sell fakes will not be able to have it. But how do we know if the features are PUF or not?

1) Ask the question, whether a manufacturer of anti-counterfeiting tag can make the same features/tag again. If answer is yes, the technology does not lead to PUF.

   Example 1: A manufacturer of holograms makes identical pieces of holograms in billions.
   Example 2: A QR code, identically, can be printed as many times as needed.

   Hence, neither of the two are PUF. **In short, any tag which is designed and engineered by humans, will get repeatedly made, implying duplication. Only suitable tags are ones which are <u>NOT</u> made by humans, which implies that they are made by nature or natural processes.** Exactly for this reason, for example, patterns in human fingerprint/face/Iris that are formed by nature are appropriately used to authenticate human identity.

2) It may not be possible by the manufacturer of anti-counterfeiting tags to replicate it by his process, so also ask the question, can the same features of the tag be made by some other method. Again, if answer is yes, the technology does not lead to PUF.

   Example: Blow or spray 2-3 colors on a piece of paper to generate a random color pattern. If you repeat the same process, the pattern next time will not be the same. However, person wanting to make fake will simply make a color copy of the original and thus clone. Hence, this technology will also not lead to PUF.

There are companies selling anti-counterfeiting technologies along with a mobile phone based authentication on 2D features and calling them unclonable.

In name of un-clonability, several technologies based on hidden features or those bit difficult to copy are being promoted as unclonable, along with App for verification of that hidden feature. This is simply a misrepresentation. These are just old technologies, re-packaged, such as hidden inks or

features included in artwork of packages, along with a new APP! All these have been tried approaches and failed after few months as they get copied shortly once the details of hidden feature leaks out or copied by an expert.

Unclonable means, even technology provider cannot copy himself!

Consumers don't download Apps on their phones. Why not then do web based authentication?

As the current trend is to use smartphones for authentication, two options are available, either through a downloadable App or a QR code redirecting the user to a website. So, which one to use. The answer here is counter intuitive. Few people download Apps, so it would appear using inbuilt App for scanning QR code and getting redirected to a URL for authentication has more likelihood of use. However, ask a question, when a QR code is provided for authentication, how many of us have used it. Answer is most people have not. Hence, scanning for authentication, or lack of it, is a matter of consumer behavior, irrespective of whether authentication requires App download or not. This implies the question from download/use point of view is not that relevant; instead it should be assumed that few consumers will authenticate and given that what is the best way forward.

We suggest, only an App for authentication based on algorithms along with unclonable (fingerprint type) tags be used. First, it is because, website URLs are character sensitive and exact. All a counterfeiter has to do is just change or insert one additional character in the URL address, and then smartphone browser is redirected to a fake website which the counterfeiter controls. This is commonly known as phishing attack. So, URL based authentication cannot be used. We recall the example of two following sites looking similar, but being different because of change in character 'e' in them: https://checko.ai and https://checko.ai/.

Question remains, when consumer is unlikely to scan, how will authentication take place even with an App. The answer lies in the fact, that to catch a thief, you need to catch him only once, while he carries out multiple thefts. But the thief upon getting caught should have no possibility of plausible deniability. As discussed before, cloned QR codes, holograms, or hidden features, having the limitations explained earlier, allow a counterfeiter to feign ignorance. Also, note that unlike crime of passion which is an irrational crime carried out in heat of moment, any financial crime like counterfeiting is a rational crime, engaged-in only when the seller of fake product has determined that the possibility of getting caught is negligible.

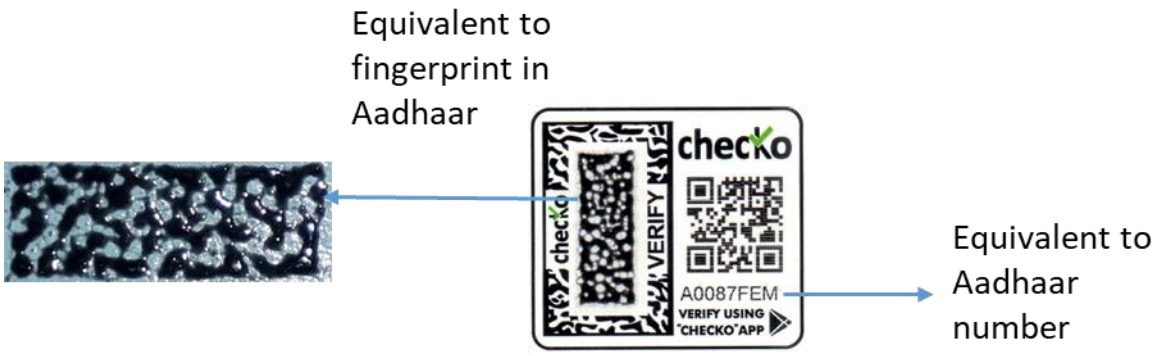
Hence, the technology needed is one which has near certainty of catching a seller of fake goods, taking away his option of plausible deniability. A unclonable tag together with ultra-reliable authentication by an App can provide the anti-counterfeiting function.

It is not the number of App downloads or number of scans, but surety of catching a counterfeit seller that provides protection against fakes.

Is there such a dream technology available?

The **Checko** anti-counterfeiting technology developed at the National Center for Flexible Electronics (FlexE) in IIT Kanpur satisfies all the requirements for a suitable tag for anti-counterfeiting. The

technology is based on providing an **unclonable** ID to any product (i.e., a fingerprint just like Aadhaar uses one for humans), allowing it to be verified in the field by the end buyer or government agency alike, using an algorithm implemented on a mobile phone. The technology is backed by two patents granted both in India and USA and third patent filed in India.



As shown above, the Checko tag consists of an unclonable naturally formed 3D random pattern of black material on white background. The pattern is produced by a natural process, akin to cracks that naturally form when farmland dries up under summer sun. This implies that even the team that invented the technology cannot make the same tag again!! The pattern constitutes equivalent of fingerprint in Aadhaar authentication. The tag is linked to a unique identification number, which is equivalent to the Aadhaar number. Any data related to product on which this tag is affixed is linked to this identification number and thus visible upon scan of the Checko tag.