

Can Cell Phones And Cryptography Combine To Check Counterfeiting?

Counterfeit currency is fast becoming a major problem in our country. Although currency forgers have a number of technologies at their disposal, we could trip them up by just using our cell phones and some cryptography.

Abhijit Bhattacharjee

The author is founder and product manager, myMobilephone. In—a company that aspires to build technologies, applications and services for the common people of India, which are accessible on their mobile phones. His firm has developed an application to generate QR codes in Hindi and other regional languages, which is freely usable on the company website.



This Diwali, when I demonstrated a QR (quick reaction) code application to my father, he asked if it was possible to detect fake currency notes using a mobile phone camera. I had been gathering ideas for over two years on Mobile ICT (information and communication technology) and its potential role in the life of the common person, and this was the most valuable and relevant input of the lot.

I told my father that QR codes couldn't help much in this case because it would be easy for a counterfeiter also to reproduce them. However, it

might be possible to machine-analyse the note through a phone camera and detect those intricacies of the lithograph (for instance, a particular mark on Gandhiji's nose) that are difficult to spot for a common person but are easy for a machine to close in on several parameters. The photograph could be taken in any orientation. I experimented right away with my phone camera but found that without the close-up mode (available in many phone cameras), it was impossible to get images with the resolution and clarity that could serve the purpose. Perhaps it could be done with a lens adapter fitted to the phone camera.

The power of cryptography

I read up what I could find about fake currency notes in India, and was shocked to discover the extent of the menace and the problems it has caused to innocent people. A CBI (Central Bureau of Investigation) director stated in 2006 that 1.7 trillion rupees of fake currency notes are in circulation. Such is the fear of counterfeit currency that there are parts of the country and Nepal where no one will accept a Rs 500 note—it is even feared that ATM machines are disbursing fake

currency notes. A conservative estimate puts the total counterfeit currency in circulation in this country at Rs 1500 crores.

We have so far not been able to do much about this menace, but there is now a possibility of tackling the issue head on.

What if we insert a cryptographic code (a short number) along with a serial number in every printed currency note of higher denomination? Cryptographic codes (hash codes, etc) are a unique mathematical invention, the nature of which makes it impossible for anyone to tamper with them. They are used in many security applications such as digital certificates, specifically for this reason. Cryptographic codes are available in many schemes and algorithms, and are used depending on the nature of the application. Cryptographic codes involve computations and hence can be verified only electronically. That is why no one would ordinarily think of inserting cryptography codes into currency notes to certify their authenticity.

But with one in every two adult Indians equipped with a mobile phone today, everybody can just pick up their phones and SMS the serial number of a currency note to a toll-free number. A calculated cryptographic code and the currency denomination can then be sent back to them instantly over SMS. If the code matches what is on the note, the note is genuine. If the note is fake, a wrong serial number will be revealed to the system, and the currency holders can be advised about their next course of action.

Benefits galore

This approach has several benefits. If too many fake notes start turning up from a particular part of the country, that would serve as an instant alert for the economic offences team to swing into action in that province.

If the counterfeiter makes a note of the codes as seen on real notes and prints them, the duplicate serial numbers will show up from unlikely geographically distant parts of the

What if we insert a cryptographic code (a short number) along with a serial number in every printed currency note of higher denomination? Cryptographic codes (hash codes, etc) are a unique mathematical invention, the nature of which makes it impossible for anyone to tamper with them.

country within a time window, raising an alert in the system.

The best part is that the holder is always traceable, as the government also has the identity documents of phone owners. The service can be used by just about anyone as most people either have a mobile phone or have access to someone who does.

The service should be toll free. The cost of an SMS when sent in bulk, as in this case, is less than one paisa. The

printing cost of a 500-rupee note must be a few tens of rupees. Surely, that is an acceptable cost for a nation unsure of its currency notes. And, surely, it is cheaper than manually detecting a note's authenticity. Besides, one can cut down the accompanied risk in every transaction, not to mention the need to regularly introduce innovative and complex printing techniques to beat the counterfeiters.

Putting the system into place

The load for this system can be handled by an array of a few dozen servers—a distributed system. It is a moderate computational load comparable to a popular website. There are asymmetrical cryptographic codes that are by design far simpler to verify than to generate. There could also be a lookup table implementation, which can also be checked over the Internet for those with access to it. And batch processing should be allowed. Many commercial websites will be happy to offer this function because it generates traffic. The data can be deposited to the central servers. Telecom companies will love this additional revenue generated from large volumes of VAS (value added services). But more importantly, being a mainstream application, it will open the public's mind towards VAS applications, their usage, acceptability and their many possibilities.

The system will also provide us with a scientific basis of estimating the size of the problem of counterfeiting at any given time and the territories where it is more prevalent. The conduit points could be easily identified from the growing

diffusion of reports. And can alert the system when new diffusions show up.

Generating a large number of codes in certain types of cryptography can be a mathematical challenge but this can be solved by diluting the mathematical standards that are enforced for commercial security applications (e-commerce transactions). The dilution may not hurt an application of this nature. A clever optimal choice of feasibility, usability, short codes, etc, should determine the choice of scheme. What we need here is the mathematical impossibility for the counterfeiter to come up with a serial number and code that fit each other, possibly a trapdoor function. The application can also choose a subset of the serial number (not the entire number, for simplicity of implementation). As matters stand, may be sending the serial number itself (with its several existing check digits) is a sufficient token to establish authenticity.

The software to verify the hash codes (or any other) could also be released into the public domain and could even run on mobile phones that are advanced enough to support applications, saving the user from the trouble of even sending an SMS. The application will, of course, easily run on any PC. The beauty of strong cryptographic algorithms is that they cannot be reverse engineered even if the software to decode them is released freely. That, in fact, is the practice for all authentication technologies, the source codes of which are all in the public domain and open to hackers.

Using optical character recognition technologies, banks can easily have

automated systems that can check the authenticity of bank notes in large numbers instead of doing it manually. ATM machines can supply a printout of the serial numbers of banknotes disbursed and the docket reports of their authenticity.

Using optical character recognition technologies, banks can easily have automated systems that can check the authenticity of bank notes in large numbers instead of doing it manually.

A treasure trove of data... and peace of mind

The large amount of data that this service will throw up will be a veritable gold mine for economists. This data can be mined to produce extremely useful statistical correlation and reports on the flow and circulation of money, and the velocity of M1 money supply. This will reveal patterns of how money flows through services, trades and provinces. It could detect and track money laundering, its exit and entry into the country, and the extent of black money, as well as money that flows from and into clandestine activities like terrorism, drugs and illegal arms supply. For example, if there is an unlikely coincidence

between notes in Tamil Nadu and those that consistently show up in markets of Manipur, it will be easier to arrive at the role of the North East as a conduit for arms supply to a particular terrorist group.

Authorities can even deliberately introduce a series of bank notes into a particular economic system, and watch where they show up and how quickly. For example, we could trace money said to have been disbursed in the name of rural developmental aid. There will be many applications that will become apparent when we get to look at the data, some of which we cannot even conceive now.

Most importantly, the common man would now be confident, armed with a handy means to verify the authenticity of a note. The receivers of a large number of notes can demand that the givers first authenticate the notes in their presence before receiving the amount. And in case the authorities find more than one fake note being verified from a particular phone in a week, they would know what to do. If such a system is put in place, fake notes should disappear fast from circulation.

If all this sounds too fantastic to be true then throw your mind back to the case of the child of Charles Lindbergh who was kidnapped and subsequently murdered in 1934. It is said that the kidnapper could be traced to a particular city block by correlating the appearance of the marked banknotes of the ransom in neighbouring shops and establishments. If that could have been done in 1934, imagine what we could do now. **IT**