Ministry of Electronics and Information Technology

Internship Report

Digital Forensics

Anti-Counterfeit Technology

Author:
Simaran Jaira
Pranshu Dubey

Supervisor:
Mr. Gaurav Gupta

Ministry of Electronics and Information Technology
Government of India

Abstract

Due to consumerism and globalization, there is a rise in the manufacturing sector. Augment that with the evolution of cutting edge technology and the economy stands face to face with the wrath of counterfeit of goods. Counterfeit goods have spread across multiple industries including apparel, accessories, automobile, education, government, banks, music, software, medications, liquor, cigarettes, consumer goods, toys, electronics and much more.It is a parallel industry, and a cheap counterfeit product can do harm because it's made from cheap, substandard and dangerous substitutes.Counterfeits can be extremely dangerous to the safety and health of people. This is where the role of anti-counterfeit technology comes in. This work is a suvery of present anti-counterfeit technology. However, the main contribution is to study and propose a new anti-counterfeit technology which is reliable and cost effective.

Acknowledgement

An understanding of the study like this is never the outcome of the effort of a single person rather, it bears the support of a number of persons who directly or indirectly helped me in completing my project. I would be failing in my duty if I do not say a word of thanks to all those whose sincere advice made my training period a real educative and pleasurable one. I take this opportunity to express my profound sense of gratitude and respect to all those who helped me throughout the duration of the project. I wholeheartedly thank Mr. Gaurav Gupta for his dynamic guidance and for providing me with full information and necessary resources regarding the project. His technical fluency inspired me a lot and I definitely gained more confidence from him. Without him time and guidance the project could not have been completed. I'm also grateful towards the Ministry of Electronics and Information Technology for providing me with the facilities and Mr. Rakesh Maheshwari for giving me this opportunity without which the project would not have been finished.

Contents

Abstract **1**

Acknowledgement **2**

1 Introduction **4**

2 Objective **4**
2.1 Problem Definition 4
2.2 Problem Scope 5

3 Anti-Counterfeit Technologies **5**
3.1 Overt Technologies 5
3.1.1 Lenticular printing 5
3.1.2 Holography 6
3.1.3 Colour Shift 8
3.1.4 KolorOptik 10
3.1.5 M^2 11
3.2 Covert Technologies 13
3.2.1 Security Inks 13
3.2.2 Barcode 14
3.2.3 QR code 15
3.2.4 Void pantograph 16
3.3 Digital Technologies 17
3.3.1 RFID 17

4 Ideas for Anti-Counterfeit Technologies **19**
4.1 Void Pantograph with QR code 19
4.2 Manipulating Image Noise 19
4.2.1 Salt-and-pepper noise 20
4.2.2 Shot noise 21
4.2.3 Periodic noise 22

5 Conclusion **23**

6 Future Enhancement **23**

7 References **23**

1 Introduction

In this era of advancement and cutting edge technology where the manufacturing sector contributes to the majority of GDP in developing nations like India, there is an emerging issue of counterfeiting of goods. In 2013, it was responsible for the employment loss of about two million people. It accounts for the loss of $737B to $898B which is equal to 5% to 7% of world trade which concludes that it impacts globalization.

When we look at the catastrophe that counterfeit of goods might cause it becomes important to come up with security measures against this. In this report, we are gonna cover some major anti-counterfeit technologies in depth.

2 Objective

2.1 Problem Definition

According to International Chamber of Commerce, 1.7 Trillion Rupees is the estimated global economic and social impact of counterfeiting in 2015. There is a 10,000% growth in the problem of counterfeiting in the past two decades says IACC. Counterfeit goods have spread across multiple industries including apparel, accessories, automobile, education, government, banks, music, software, medications, liquor, cigarettes, consumer goods, toys, electronics and much more. Made from cheap, substandard and dangerous substitutes, counterfeits can be extremely dangerous to your safety and health. Owing to the global obsession with online shopping, counterfeits are minting money day and night. Transactions through counterfeit merchants and illegal sites can give a hard hit to your pockets.

Counterfeiting takes away the hard-earned money and reputation of legitimate companies by selling the fake and cheap replicas of their original products.

With counterfeiting making its footprints deeper and marking its presence everywhere, the solutions to combat it have not only become necessary but mandatory. This is where the role of anti-counterfeit technologies comes in. Anti-counterfeit technologies ensure that a given product is genuine or counterfeit. The initial point of automated non-destructive product authentication to prevent counterfeit is to insert a special security feature

into products like a barcode, QR code, serial numbers etc.

2.2 Problem Scope

The scope of this project is to survey the existing anti-counterfeit techniques that are currently in usage and to study them in depth along with their reliability. After the survey and gaining understanding about the requirements of the anti- counterfeit technologies, we will try to come up with a new and cost effective technology. Our main aim is to come up with a solution which is not resource hungry but cost effective.

3 Anti-Counterfeit Technologies

3.1 Overt Technologies

These can be viewed through naked eyes and are meant for fats, easy and on the spot visual authentication. These are features built into labels, documents and packaging and have dynamic visual effects.

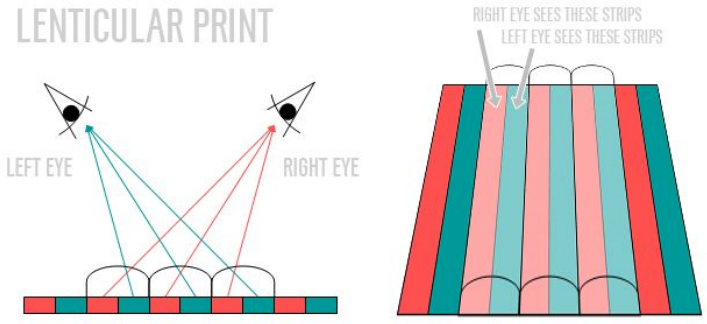
3.1.1 Lenticular printing

Lenticular printing is a technology in which lenticular lenses (a technology that is also used for 3D displays) are used to produce printed images with an illusion of depth, or the ability to change or move as the image is viewed from different angles.

Examples of lenticular printing include flip and animation effects such as winking eyes, and modern advertising graphics that change their message depending on the viewing angle.Colloquial terms for lenticular prints include "flickers", "winkies", "wiggle pictures" and "tilt cards".

How Lenticular Printing works: Lenticular printing is a multi-step process which consists of creating a lenticular image from at least two images, and combining it with a lenticular lens. This process can be used to create various frames of animation (for a motion effect), offsetting the various layers at different increments (for a 3D effect), or simply to show a set of alternate images which may appear to transform into each other. Once the various images are collected, they are flattened into individual, different

frame files, and then digitally combined into a single final file in a process called interlacing. From there the interlaced image can be printed directly to the back (smooth side) of the lens, or it can be printed to a substrate (ideally a synthetic paper) and laminated to the lens. When printing to the backside of the lens, the critical registration of the fine "slices" of interlaced images must be absolutely correct during the lithographic or screen printing process or else "ghosting" and poor imagery might result. Ghosting also occurs on choosing the wrong set of images for flip.



Material used: There are several film processors that will take two or more pictures and create lenticular prints for hobbyists, at a reasonable cost. For slightly more money one can buy the equipment to make lenticular prints at home. This is in addition to the many corporate services that provide high-volume lenticular printing. The newest lenticular technology is manufacturing lenses with flexo, inkjet and screen-printing techniques. The lens material comes in a roll or sheet which is fed through flexo or offset-printing systems at high speed, or printed with UV inkjet machines (usually flat-beds that enable a precise registration). This technology allows high volume 3D lenticular production at low cost.

Reliability: It's effective for anti-counterfeit but can be easily copied or produced and can be put on fake products while making them look authentic and hence resulting in a defeat.

3.1.2 Holography

By definition, a hologram is a three-dimensional image, created with photographic projection. Hologram term is derived from Greek words holos (whole)

and gramma (message). It is a true three-dimensional and free-standing image that does not simulate spatial depth or require a special viewing device.

The theory of holography was developed by Dennis Gabor in 1947. The development of laser technology made holography possible. A photographic technique that records the light scattered from an object, and then presents it in a way that appears three-dimensional is known as Holography.

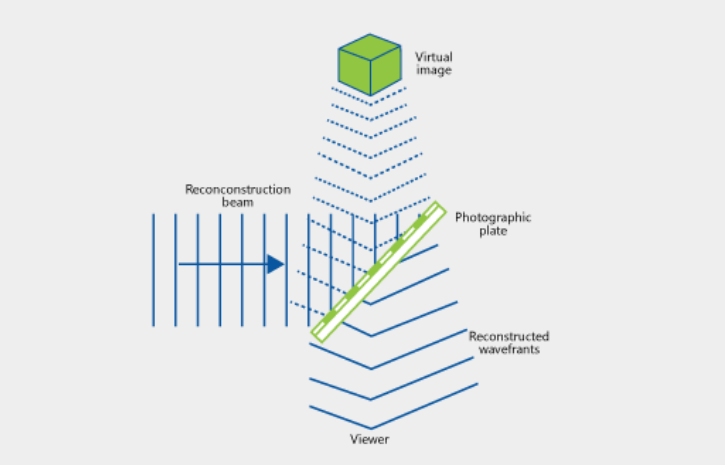
Various types of holograms have been made over the years, including transmission holograms, which allow light to be shined through them and the image to be viewed from the side; and rainbow holograms, which are used for security purposes like credit cards and driver's licenses and other ID's etc.

How holography works: In order to create a hologram, an object is needed that needs to be recorded; a laser beam to fall on the object and the recording medium; a recording medium with the proper materials needed to help clarify the image; and a clear environment to enable the light beams to intersect.

A laser beam splits into two identical beams and redirected by the use of mirrors. One of the split beams, the illumination beam or object beam, is directed at the object. Some of the light is reflected off the object onto the recording medium.

he second beam, known as the reference beam, is directed onto the recording medium. This way, it doesn't conflict with any imagery that comes from the object beam, and coordinates with it to create a more precise image in the hologram location.

The two beams intersect and interfere with each other. The interference pattern is what is imprinted on the recording medium to recreate a virtual image for our eyes to see.



Material used: The recording medium, where the lights converge, can be made up of various materials. One of the most common used with hologram creation is photographic film, with an added amount of light-reactive grains. This enables the resolution to be higher for the two beams, making the image look much more realistic than using the silver halide material from the 1960s.

Reliability: It's effective for anti-counterfeit but can be easily copied or produced and can be put on fake products while making them look authentic and hence resulting in a defeat.

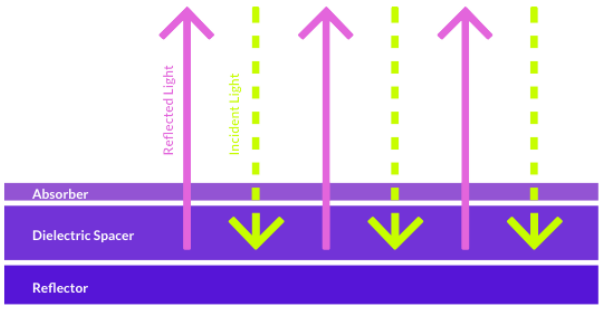
3.1.3 Colour Shift

Colour shifting is when various objects within the external environment shift and change their colour through a continuously repeating cycle that occurs in a fluid motion across the surface of the object.[1] For example, moss on a rock could visibly shift from green to red to blue to any other colour and then back to green again in the style of a smooth and seamless animated loop. This effect is particularly strong and likely to occur if the objects original colour was bright or out of place. Colour shifting is often accompanied by other coinciding effects such as color enhancement and colour replacement. It is most commonly induced under the influence of moderate dosages of psychedelic compounds, such as LSD, psilocybin, and mescaline. However, it can also occur to a lesser extent under the influence of certain stimulants

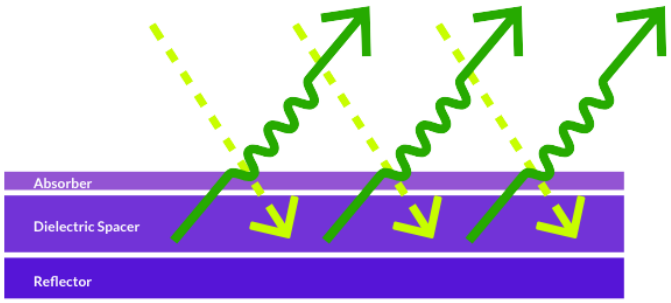
such as MDMA.

How Colour Shift works:

Viewing Position 1: Colour Shift has thin film layers that filters light through. When viewing directly, the light that is reflected back through the thin film produces a colour; in this example magenta.



Viewing Position 2: When Colour Shift is tilted and viewed at an angle, the light that is reflected back produces a second colour; in this example the colour green.



Material used: The Colour Shift optical thin film is 200 nanometres in thickness. This means you need to stack 375 of them to reach the thickness of an average human hair.

Reliability: Colour shifting optical thin film has been the standard for document security for over two decades, and for good reason: it provides the ultimate in security yet is very simple to use. It is also one of the most durable overt security features, with little to no loss in its characteristics when crumpled. Colour Shift is also very difficult to simulate. In addition to involving extremely sophisticated production equipment, the technology is challenging to manufacture and requires deeply specialized knowledge. Apart from all this, it's cost effective too.

3.1.4 KolorOptik

Nanotech's KolourOptik security platform uses advanced nano-optics for the most sophisticated security authentication on the market – it transcends barriers found in conventional holograms. KolourOptik technology is the first nanotechnology to seamlessly integrate into the commercial manufacturing process. It has taken Nanotech's team many years to develop the entire KolourOptik process. This process requires patented algorithms, extremely skilled personnel, sophisticated multi million-dollar equipment and class 1 clean rooms to effectively fabricate master shims while keeping security a priority.

Using light through an image to make colours appear

How KolorOptik works: They start off by designing with a user-centric approach. KolourOptik can be customized to any shape, size or colour, with details that can be viewed with the naked eye or detected via specialized equipment. KolourOptik can be applied on a wide range of materials ranging from metals, plastics, acrylic, cloth, paper substrates and more.

Material used: KolourOptik technology uses patented algorithms coupled with electron and ion beam technology to make hundreds of billions of extremely small holes ("nano-holes") on virtually any material.KolourOptik images are comprised purely of nano-scale holes in refined metals – no dyes or pigments are involved.

Reliability: More than 500,000 DPI and 50,000 PPI produces both large and small images that are ultra-high definition.Once built, an origination wafer can be used to produce a subsequent master shim – suitable for high-speed, large-volume production. The requirements for production and the nano-scale of this technology ensures the shim cannot be reverse engineered, thereby providing the ultimate in security. But it's not cost effective.

3.1.5 M^2

It seamlessly combines programmable movement with colourful iconography without the need for lenses, mirrors or diffractive gratings. M^2 sets a new standard in authentication technology.

Design: M^2 can be customized into any shape, size, and colour. Ultra high definition details can be viewed with the naked eye or detected via specialized equipment.

Movement: M^2 has fast programmable movement controlled with their latest nano-optic technology.

Colour: Customizable high-resolution multi-colour nano-optic images with dramatic inverting effect.

The ship inverts when tilted, fast movement in the border, moving bar inverts the text, colours change on large tilt

How M^2 works: Thickness is indistinguishable from the substrate using our advanced M^2 nano-optic images without the need for lenses, mirrors or diffractive gratings. With their advanced M^2 nano-optic technology, the feature works under virtually any lighting condition with 180-degree viewing.

Material used: M^2 nano-optic images are comprised purely of nanoscale holes – no dyes or pigments are involved. M^2 can be applied to a wide range of materials ranging from metals, plastics, acrylic, cloth or paper substrates and more.

Reliability: The latest M^2 nano-optic technology produces ultra-HD images in an ultra-thin format suitable for integration into stripes and other surface applied features. It defines a new category for authentication. The complex nano-technology behind M^2 ensures the shim cannot be reverse engineered, providing the ultimate level of security.But it's not cost effective at all other than that it's a technology used by banks, nowadays.

3.2 Covert Technologies

To verify their presence and validity, a special reader or a detector is required. These include ultraviolet and infrared inks, micro text unique synthetic tagging etc.

3.2.1 Security Inks

These are used to minimise/curb counterfeiting. The images/text created by security inks are not visible by naked eyes and they can be viewed only with the help of hand-held gadgets like talking pen, taggant reader, UV torch etc.

Following are the different types of security inks used:

1. **UV or invisible ink** – These inks also known as security inks and are used due to their property that when applied they are invisible either on application or soon thereafter, and can later be made visible by UV light.

2. **Fluorescent ink** – This ink is colourless, transparent, or white and can be easily detected under UV light.

3. **Thermochromic ink** – This ink is visible only when given heat.

4. **Photochromic ink** – This ink is visible under sunlight only.

How Security Ink works: After choosing the required ink,it's imprinted on the required material using specific printers.They can be viewed with talking pen, UV torch etc.

Material used: They are extensively used on labels and containers for primary, secondary and tertiary packaging and they are formulated for almost all substrates.

Reliability: These inks are cost-effective, relatively easy to apply, and provide an excellent base for some of the most advanced covert applications such as DNA markers and taggant integration.

3.2.2 Barcode

A barcode is a really simple idea: give every item that you want to classify its own, unique number and then simply print the number on the item so an electronic scanning device can read it. We could simply print the number itself, but the trouble with decimal numbers is that they're easy to confuse (a misprinted eight could look like a three to a computer, while six is identical to nine if you turn it upside down—which could cause all sorts of chaos at the checkout if you scanned your cornflakes the wrong way up). What we really need is a completely reliable way of printing numbers so that they can be read very accurately at high speeds. That's the problem that barcodes solve.

How Barcode works: Once it is run across the scanner, the scanner picks up the barcode. This is done by it reading the bars and spaces between the bars. The numbers at the bottom of a UPC label are for humans only. As the scanner picks up the bars, it then transfers the information to a computer (or register). The computer then finds the record associated with that barcode. The computer records may contain such information as price, number of items available, and other pertinent information like that.

Material used: It is generally printed using normal grade printer on any kind of sheet whatsoever.

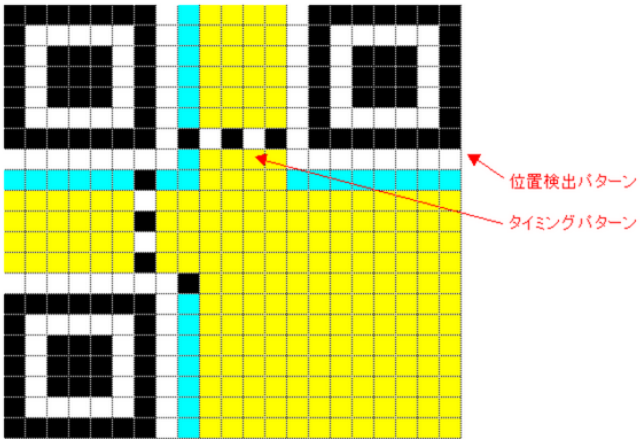
Reliability: A barcode is a unique number or pattern by which items are uniquely coded, either through an alpha/numeric code and those unique codes are stored in a database and scanned at various points throughout the supply chain . When the product travels through the entire chain and scanned at various check points, it results in providing valuable information

about the authenticity of the product. It's so cheap that it can be easily replicated on the product just by copying it.

3.2.3 QR code

QR (Quick Response) code is the trademark name for the two dimensional barcode system. It was originally invented in 1994 by Denso Wave, a Toyota subsidiary, as a way to track vehicles as they were assembled, and to scan components at high speeds. While Denso Wave does hold the patent on the technology, it has granted free licence on it, going so far as to publish the spec online, and allowing anyone to use it.

How QR code works: The conventional one dimensional barcodes used on virtually every consumer product are mechanically scanned. That is, they're read by physically bouncing a narrow beam of light onto the code, which can be interpreted using the pattern of light reflected off the white gaps between the lines.



QR codes can hold 100 times more data than 1D barcodes—they can also be digitally scanned. The block of smaller black and white squares is read by a smart phone's image sensor, then interpreted by the system processor. The three large squares act as alignment targets, while the smaller square in the remaining corner acts to normalize the size and angle of the shot. As you can see from the image on the left, the blue strips near the alignment squares contain formatting information, and the remaining yellow area is the

actual data that's converted into binary code and checked for errors before being displayed. The encoded data can be interpreted as one of four primary modes—numeric, alphanumeric, byte/binary, and Kanji. Other forms of data can also be displayed with the appropriate extensions.

Material used: It is generally printed using normal grade printer on any kind of sheet whatsoever.

Reliability: QR codes are two dimensional, machine readable bar codes that can contain a significant amount of information intended for a specific user in black and white squares. These squares are used for storing URL's and other information. We utilise this capability to securely share secret information between the web site and the user. On scanning the QR code, the user is able to know if the product he has purchased is genuine or not.It's so cheap that it can be easily replicated on the product just by copying it.

3.2.4 Void pantograph

In security printing, void pantograph refers to a method of making copy-evident and tamper-resistant patterns in the background of a document. Normally these are invisible to the eye, but become obvious when the document is photocopied. Typically they spell out "void", "copy", "invalid" or some other indicator message.

How Void pantograph works: Void pantographs work by exploiting the limitations and features of copying equipment. A scanner or photocopier will act as a low-pass filter on the original image, blurring edges slightly. It will also not be perfectly aligned with the directions of the document, causing aliasing. Features smaller than the resolution will also not be reproduced. In addition, human vision is sensitive to luminance contrast ratio. This means that if a grey region consists of a grid of very small dark dots the filtering will produce a lighter grey, while a region of larger dots will be affected differently ("big-dot-little-dot"). This makes it possible to see a pattern that had been invisible.Numerous variations exist, including printing the marks using a raster of lines in one direction on a background of lines in another direction,or using fine line patterns that alias into a visible moire pattern when copied.

Material used: The void pantograph is generally created using pre-press software and requires specific line screens. A printer who specializes in printing the void pantograph would be a good resource - it sounds like it's not something you can create easily in the Adobe application and expect consistent results on any output device. But banks use special VOID paper for this too.

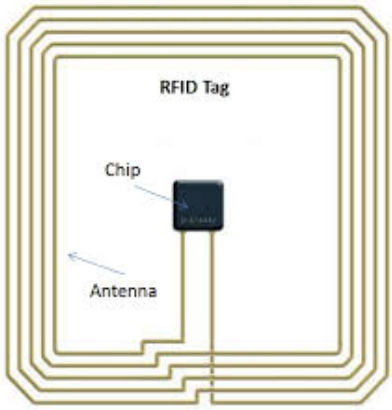
Reliability: It's reliable and difficult to replicate but not impossible and hence it's only limited to the usage in cheque and coupons.

3.3 Digital Technologies

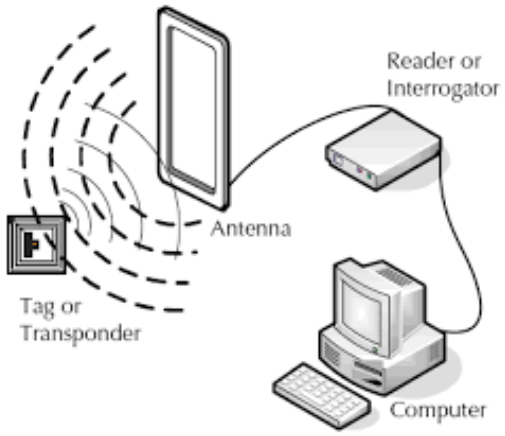
These may be either overt or covert but all require an electronic means for detection and validation. These are mostly associated with RFID tags or with serialised numbers that can be compared to a remote database.

3.3.1 RFID

RFID is an acronym for "radio-frequency identification" and refers to a technology whereby digital data encoded in RFID tags or smart labels (defined below) are captured by a reader via radio waves. RFID is similar to barcoding in that data from a tag or label are captured by a device that stores the data in a database. RFID, however, has several advantages over systems that use barcode asset tracking software. The most notable is that RFID tag data can be read outside the line-of-sight, whereas barcodes must be aligned with an optical scanner.



How RFID works: RFID methods utilize radio waves to accomplish this. At a simple level, RFID systems consist of three components: an RFID tag or smart label, an RFID reader, and an antenna. RFID tags contain an integrated circuit and an antenna, which are used to transmit data to the RFID reader (also called an interrogator). The reader then converts the radio waves to a more usable form of data. Information collected from the tags is then transferred through a communications interface to a host computer system, where the data can be stored in a database and analyzed at a later time.



Material used: As stated above, an RFID tag consists of an integrated circuit and an antenna. The tag is also composed of a protective material that holds the pieces together and shields them from various environmental conditions. The protective material depends on the application. For example, employee ID badges containing RFID tags are typically made from durable plastic, and the tag is embedded between the layers of plastic. RFID tags come in a variety of shapes and sizes and are either passive or active. Passive tags are the most widely used, as they are smaller and less expensive to implement. Passive tags must be "powered up" by the RFID reader before they can transmit data. Unlike passive tags, active RFID tags have an on-board power supply (e.g., a battery), thereby enabling them to transmit data at all times. For a more detailed discussion, refer to this article: Passive RFID Tags vs. Active RFID Tags.

Smart labels differ from RFID tags in that they incorporate both RFID and barcode technologies. They're made of an adhesive label embedded

with an RFID tag inlay, and they may also feature a barcode and/or other printed information. Smart labels can be encoded and printed on-demand using desktop label printers, whereas programming RFID tags is more time consuming and requires more advanced equipment.

Reliability: Recently, nations across the world are embedding RFID tags in passport for enhanced security. But the fact that the effective cost of RFID is too high makes it impossible for it to used in products for authentication.

4 Ideas for Anti-Counterfeit Technologies

4.1 Void Pantograph with QR code

Anyone can copy and make a QR code to put on their respective product making it authentic even though it's a counterfeit. But if we use Void Pantograph with the QR code, it will render the QR code useless if we copy or scan it. The basic requirements for this is Void Pantograph paper and QR code can be generated for respective products. It's also cost effective,so we are gonna experiment and test it further in the coming months.

4.2 Manipulating Image Noise

Image noise is random variation of brightness or color information in images, and is usually an aspect of electronic noise. It can be produced by the sensor and circuitry of a scanner or digital camera. Image noise can also originate in film grain and in the unavoidable shot noise of an ideal photon detector. Image noise is an undesirable by-product of image capture that obscures the desired information.

Noise clearly visible in an image from a digital camera

We can use the following noises to our advantage. We can manipulate the following noises to be inserted into our anti-counterfeit technologies and everytime someone tries to scan or copy it, these noises will be evident.

4.2.1 Salt-and-pepper noise

An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions. This type of noise can be caused by analog-to-digital converter errors, bit errors in transmission, etc. It can be mostly eliminated by using dark frame subtraction, median filtering and interpolating around dark/bright pixels.

Image with salt and pepper noise

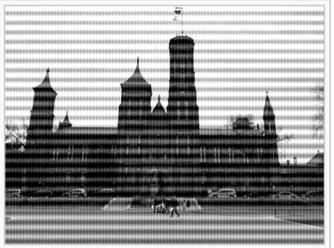
4.2.2 Shot noise

The dominant noise in the darker parts of an image from an image sensor is typically that caused by statistical quantum fluctuations, that is, variation in the number of photons sensed at a given exposure level. This noise is known as photon shot noise.

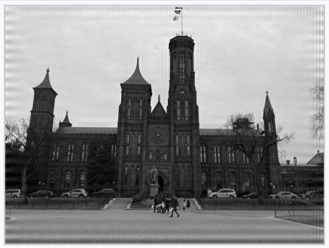
Photon noise simulation. Number of photons per pixel increases from left to right and from upper row to bottom row.

4.2.3 Periodic noise

A common source of periodic noise in an image is from electrical or electromechanical interference during the image capturing process.An image affected by periodic noise will look like a repeating pattern has been added on top of the original image. In the frequency domain this type of noise can be seen as discrete spikes. Significant reduction of this noise can be achieved by applying notch filters in the frequency domain.The following images illustrate an image affected by periodic noise, and the result of reducing the noise using frequency domain filtering. Note that the filtered image still has some noise on the borders.



An image injected with periodic noise.



Application of frequency domain notch filters.

5 Conclusion

We successfully surveyed the major existing anti-counterfeit technologies with respect to their reliability and cost. We also studied and proposed some new ideas for anti-counterfeit techniques that can be used to tackle the existing scenario.

6 Future Enhancement

The proposed ideas for new anti-counterfeit technologies will be designed, tested and experimented in the upcoming months to come up with a reliable, cost effective and clever approach.

7 References

1. C. N. Chong, D. Jiang, J. Zhang, L. Guo, "Anti-counterfeiting with a Random Pattern", Emerging Security Information, Systems and Technologies, 2008. SECURWARE '08. Second International Conference on , vol., No., pp. 146-153, 2008.

2. Y.-C. Chen, W.-L. Wang, and M.-S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection," in Proceedings of the 9th International Conference on Advanced Communication Technology, vol. 1. IEEE, February 2007, pp. 255-259.

3. A. Worsdall and A. Clark, Anti-Counterfeiting: A Practical Guide. Jordans, August 1998.

4. https://patents.google.com/patent/US8105677B2/en

5. https://patents.google.com/patent/US6390362B1/en

6. https://en.wikipedia.org/wiki/Image_noise

7. https://www.nanosecurity.ca/

8. https://holostik.com/