2014

Ubiquitous Consumer-Centric System to Combating Product Counterfeiting and Boosting Entrepreneurship in Developing Economies

Kingsley C. Nwosu
Saint Leo University

Follow this and additional works at: http://digitalcommons.unl.edu/jade

Part of the Econometrics Commons, Growth and Development Commons, International Economics Commons, Political Economy Commons, Public Economics Commons, and the Regional Economics Commons

http://digitalcommons.unl.edu/jade/6

This Article is brought to you for free and open access by the Economics Department at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in Journal for the Advancement of Developing Economies by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.
Ubiquitous Consumer-Centric System to Combating Product Counterfeiting and Boosting Entrepreneurship in Developing Economies

By

Kingsley C. Nwosu, Ph.D.
Dept. of Computer Science and Information Systems,
Donald R. Tapia School of Business,
Saint Leo University,
Virginia Peninsula Center,
Newport News, Virginia, USA.

Abstract

Counterfeiting has been a menacing problem to global economies; however, it has been more devastating to developing and under-developed countries as a result of its impacts on various aspects of the economic development and health conditions of those countries. The consequences are abundantly documented, evidential and troubling. In addition to the fact that counterfeiting results in distribution of fake, cheap, and substandard products, it has very dissuasive effects on the entrepreneurial fabrics of a society. As various governments and agencies attempt to combat the menace and mitigate the consequences, the perpetrators are becoming even more sophisticated and resolute – encouraged and motivated by the current technological terrains. Most current methods and techniques utilized in combating product counterfeiting usually tend to concentrate on the “detect, catch and prosecute” approach by those governments and agencies. Besides the resource extensiveness of this approach, which is mostly unattainable, the “detect or catch” part may happen, but the “prosecute” part has always been greatly marred by the corruptive environments that are usually endemic in those societies. When technology-based approaches are used in the war against counterfeiting to empower the consumers, either it’s non-ubiquitous, easily compromised by counterfeiters, difficult to use or not cost-effective to the consumers. As a result, what is needed is a technology and consumer-centric, ubiquitous, secure, easy-to-use, and cost-effective system to greatly alleviate this nuisance.

Keywords: counterfeiting, economic development, developing economies, piracy, ubiquitous, entrepreneurship
1.0 Introduction

Fraudulent business activities contribute immensely to the retrogressive stagnation and deterioration of the economies of developing and under-developed countries. One such activity is the prevalence of product counterfeiting or piracy in these countries as reported in OECD (2008), WIPO (2010), and GAO (2010). On one hand, product counterfeiting usually results in production and distribution of fake products that are cheaper and sub-standard; and in some cases very dangerous. On the other hand, as an economic engine, it deters and dissuades potential innovators and entrepreneurs from engaging in new product ideas for fear of being sabotaged and/or derailed by counterfeitters. In most of these countries, the governments have not been able to effectively develop, promulgate, and enforce laws to combat or mitigate this economic menace. In Earwood (2014) and Mertha (2011), it’s reported that even in those cases where the governments have been able to promulgate laws; they have not been able to effectively enforce them either by design or as a result of their inability to provide the necessary resources. Besides being emboldened by the availability of sophisticated replication techniques and technology, one of the dominant reasons for the counterfeitters is the belief that an end-user may not be able to make a visual distinction between a counterfeit and original. The other reason is the belief that there is always a market for those who want the original product but cannot afford it, so those people are willing to buy a counterfeit or fake that they can masquerade as an original without their friends noticing the difference.

In Candice (2009) analysis of the factors and impacts of counterfeit sales over the Internet, it concluded that the problem of counterfeiting has been exacerbated with the arrival of the Internet. The scope and reach of the Internet has inconceivably expanded the population, demographics, and geographical coverage for counterfeitters to easily and surreptitiously market and sell their products. The nature of the Internet makes it hard for even conscious consumers to be aware of the product source and/or location – especially, in the case when a counterfeiter wants to remain cryptic. Only few technology savvy consumers can perform the necessary online investigation to verify the originality and location of the products.

The advent and pervasiveness of mobile technology provides a platform for an effective and cost-efficient approach to addressing this menace. In this paper, we present a Mobile Application platform that empowers both the product owner and consumer to secure and verify the authenticity and originality of a product. The product owner is able to securely label the product which a consumer can verify. As a result, a consumer, equipped with a smartphone, can easily, reliably, and cost-efficiently verify whether a product is original or counterfeit.

1.1 Background

In 2008, the Organization for Economic Co-operation and Development (OECD), as part of their effort in addressing the economic, social and environmental challenges of globalization, produced a report covering counterfeiting and piracy that result in the production of tangible goods and found that the effects of counterfeiting are broad and profound spanning such areas as (i) general socio-economic effects (on innovation and growth, criminal activities, environment, employment, foreign direct investment, and trade), (ii) effects on rights’ holders (on sales volume and prices, brand value and firm reputation, royalties, firm-level investment, costs and the scope of operations), (iii) effects on consumers (health and safety risks and consumer utility) and (iv) effects on government (tax revenues, expenditures and corruption). They concluded that “these illicit activities steal market share from legitimate businesses and
undermine innovation, with negative implications for economic growth. Bribery associated with counterfeiting and piracy weakens the effectiveness of public institutions at the expense of society at large.” In related analyses, Quinn (2010) and Gasiorowski (2014) found that counterfeiting and piracy have cost the global economies tremendously including the United States business for an estimated USD 200B - USD 250B annually and USD 9 billion in trade losses due to international copyright piracy; loss of more than 750,000 US jobs; and since 1982, the global trade in illegitimate goods has increased from USD 5.5 billion to approximately USD 600 billion annually. It's also estimated that by 2015, the International Chamber of Commerce (ICC) expects the value of counterfeit goods globally to exceed USD 1.7T.

In March 31st, 2011, Associated Press (AP) reported that China arrested about 3,001 individuals who allegedly were involved in “product piracy and seized fake or counterfeit medicines, liquor, mobile phones and other goods.” The report further states that “Trade groups say illegal Chinese copying of music, designer clothing and other goods costs legitimate producers billions of dollars a year in lost potential sales” and also recognizes that “Intellectual property protection is essential for building an innovation-oriented country and achieving a shift from ‘China manufactured’ to ‘China innovated’.” In several articles by Turnage (2013), Dobson (2010), SEG_MAG (2010), and EOPUS (2013) that analyzed the relationship between enforcement and rate of piracy, they concluded that China, due to its ineffective and lackadaisical attention to intellectual property protection, is the leading source of product counterfeiting in the entire world. Based on the data analysis by Palmer and Maler (2011), it’s estimated that piracy cost the United States about $48B in 2009. In another related report by Planer (2009), it’s stated that “More than one in four consumers buy fake products, at least occasionally, and more than 60% of buyers do so deliberately.” According to the report, most of the people involved in purchasing fake products do so due to financial constraints; and that it has become socially acceptable. The range of products varies greatly from luxury items to car parts and household items. In the case of fake medicines, “they are ineffective in a best-case scenario, but will inflict bodily injuries or death in a less favorable outcome”. Product piracy is not limited to hardware items, computer software are also pirated. According to CBS News (2010), “some 79 percent of software used in China last year was illegally copied.” In the 2011 report “Media Piracy in Emerging Economies” by Joe Karaganis et al (2011), they concluded, based on research on Brazil, India, Russia, South Africa, Mexico and Bolivia, that “most people in those countries bought counterfeited products because the originals were very expensive.” However, others argue that those countries are culturally ignorant of copyrights and intellectual property, which can be mitigated by education and effective enforcement. The report further states that “Changing the law is easy. Changing the practice is hard” by implying that “lobbies have been very successful at changing laws to criminalize these practices, but largely unsuccessful at getting governments to apply them”.

1.2 Current Solutions

Many forms and techniques have been employed over the years in attempting to combat product counterfeiting. Until recently, most of these efforts have not involved the use of technology, rather countries and governments have tried to pass and enforce laws to punish those caught in the act; and also utilized public education on the possible consequences of buying counterfeited or fake products; and advising product owners on product trademarks. In developed economies where systemic economic and legal structures exist, these techniques have proven more successful. As reported by ITA (2009), these approaches include things
like registering product trademarks in jurisdictions where the product is sold and/or where the product is manufactured; recording the trademarks with customs offices; maintaining monitoring services; creating anti-counterfeiting positions within the company; and monitoring online websites closely, etc. Where and when counterfeiting has occurred, victims are advised to consult with counsel regarding strategies to confront the issue.

According to Pogorelc (2013), Östman (2013), and Lancaster (2011), other solutions that utilize technologies come in forms such as the use of mobile technology or Radio Frequency Identification (RFID) tags or Holograms; while Lampert (2006), Romero (2009), Lee & Hyo (2013), and Herley (2004) reported of many detection or deterrence techniques and proposals. In the case of mobile solutions, serial numbers are printed on drug packages which a consumer can text (via SMS – Simple Messaging System) to a designated telephone number to receive a response confirming or denying the authenticity of the drug. When RFID tags are used, they are also printed on drug packages and are verified by using RFID readers. The RFID tag can contain drug information such as ingredients and serial number; and can further be expanded with its delivery historical information. Since hologram was first used in 1989 as a tamper-evident mechanism, many major drug manufacturers use holograms on at least some of their medicines in selected markets, using them in the form of labels, seals, hot-stamped patches, and blister foils, designed to be easily recognized yet difficult to copy accurately.

1.3 Weaknesses of Current solutions

Based on the global data about the use of various devices, CISCO (2013) reported that mobile devices are the fastest growing personal property in the world (CISCO 2013), In spite of that, current counterfeiting solutions as reported by Herley (2004), CBS (2010), Pogorelc (2013), and Lancaster (2011) do not employ the pervasiveness and ubiquitousness of mobile technology. Additionally, in their analyses of intellectual property enforcement and rule of law, Earwood (2014) and Mertha (2011) found that governments and agencies have proven very ineffective in enforcing existing counterfeiting laws. It’s obvious that attempts by governments to curtail counterfeiting by passing laws and punishing those caught have failed woefully. Given the enormous personnel manpower required to cover most businesses in any country in order to identify counterfeit products and prosecute the offenders, many of these approaches have become practically ineffective due to the fact that most of those countries are unable to meet this requirement. Also, as reported by Busari (2013), many legal system failures in prosecuting counterfeiters stem from "frequent changes in justices presiding over cases before their conclusion, the high cost of prosecution, the non-availability of its permanent police team crucial to prosecution, inadequate facts, light sentences, etc.”.

In the case of mobile solution using SMS, it’s not ubiquitous since it depends on the availability of the SMS service on the mobile device. Also, given that the verification source is publicly displayed, it can easily be compromised by counterfeiters publicizing their own verification source and diverting verification requests to that source. Furthermore, it reduces ease of use and creates added burden, and possibility of errors, by requiring the consumer to enter the verification code into their smartphones. In those cases where visual images from the verification may be necessary, using SMS-based systems are inefficient due to latency issues related to bandwidth and the protocol in the transmission of the images.

For RFID-based solutions, it’s not possible for most consumers to actively participate in the verification process since RFID readers are not generally embedded in most smartphones. As reported by Egan (2013), some Android-based smartphones and Tablets support the Near
Field Communication (NFC) capability which enables the device to receive and read RFID signals and data from RFID tags within distance. In general, RFID-based solutions are cost-ineffective because of the significant cost involved that ultimately increases the cost of the product. They are generally used for more expensive products. However, in the event that RFIDs become very cost-effective and most smartphones support RFID readers, then this system can easily be extended to the RFID-platform as described later; bearing in mind that based on the report by Francis (2009), it has been shown that NFC-based systems can be exploited.

Contrary to conventional wisdom, in McGrew (1990) report on the problems and solutions with hologram counterfeiting, it warned that it’s rather easy to counterfeit most holograms. However, the major problem with holograms is the manual process of verification – it depends on the consumer. The consumer, not a reliable source, makes the determination as to the authenticity or originality of the hologram.

2.0 Overview of the System
This system provides an environment for a product owner to securely label his/her product; and for consumers of the product to be able to reliably and ubiquitously verify the authenticity or originality of the product. With the advancements in mobile technology and security, this system utilizes software tools to encode and decode product information and provides a solution that meets and exceeds all of the existing solutions by providing secure product codes that are hard to counterfeit; and providing a platform that enables the consumers to easily obtain and utilize the verification tool. With easy-to-use programmable tools (Encoder), the product manufacturer generates or affixes the secure product codes on each product’s package. The secure codes supported are the non-proprietary 2D codes that are generally available to the public such as QRC (Quick Response Code), PDF417 and Datamatrix. The Encoder accepts product descriptive information from product manufacturer (conforming to the required format) and produces an encrypted text which is encoded in the 2D codes.

In order to scan and decode the encrypted 2D code by a consumer, the Decoder application is made available to the consumers for download and installation in mobile and non-mobile platforms. The Decoder scans, decodes, and displays the encrypted 2D codes.

2.1 Description of the System
This system comprises two major activities – labeling a product by the owner and verifying its authenticity by a consumer.

2.1.1 Secure Product Labeling
In order to label a product, the product owner obtains the eKey package from the Key Issuer, which is used to generate eTexts – Fig. 1. An eKey package consists of one or more eKeys and the eText generator. An eKey is an encryption key uniquely generated and issued to a manufacturer or product owner. Only one eKey can be issued to a manufacturer or product owner. The eText generator is a software component or application that is used to generate the encrypted texts or strings (eText) embedded into an eCode, which is the 2D image (label) – Fig. 2. Therefore, a product owner requests for a key package from the Key Issuer by providing the required information. Upon successful verification, the Key Issuer generates
and issues the eKey and the eText generator to Product Owner. The Product Owner uses the eKey and eText generator with other pertinent product information to generate eText. Then the generated eText can be used to generate an eCode or stored in a database. The eKey must be safeguarded and protected from unauthorized access (by the product owner) just like the private key in the popular Public Key Infrastructure (PKI). If necessary, the eKey can be subject to automated electronic verification via the well-known industry-standard certificate of authenticity when used to prevent unauthorized use. Furthermore, when necessary, the eKey can be regenerated by the Key Issuer.

FIG. 1: Flow diagram for obtaining and using the eKey Package

FIG. 2: Samples of eCodes (QRC, Datamatrix, and PDF417)

2.1.2 Verifying Product Authenticity

In order to verify the authenticity or originality of a product, a consumer uses a free mobile application (eDecoder). The eDecoder enables the consumer to scan, decode, and display the information in the product label (eCode) – Fig. 3. Having downloaded and installed the eDecoder on his/her mobile device, a consumer starts the eDecoder. The consumer, via the
eDecoder and the mobile device’s camera, then scans the eCode, extracts the eText from the eCode, decodes the eText, and displays the result. If the eDecoder is unable to either extract the eText or decode the eText, it displays an error message. If a different 2D decoder is used on the eCode, it can only extract the eText which appears either as an unintelligible string of digits or non-printable string. Only the eDecoder should be able to decode an eText.

FIG. 3: Flow diagram for using the eDecoder mobile application

2.2 Applications of the System

Below are descriptions of some examples or scenarios where the system can be used or applied.

2.2.1 Product Protection

*Generic Pharmaceuticals* is a hypothetical drug manufacturing company whose drugs are being counterfeited in some Developing countries; and they want to use this system to empower those who purchase their drugs to verify the authenticity of the drugs. So, *Generic Pharmaceuticals* applies to the Key Issuer for the eKey package and supplies the required information. After processing the application, the Key Issuer generates and issues an eKey and eText Generator (eKey package) to *Generic Pharmaceuticals*. To generate the eCode for a drug called “Mycodine 50MG”, their eText generation application is used with the company name, drug information (which may include the Serial Number) and verification website. The eCode Generator then produces eTexts which are used to generate the eCodes which can be printed or affixed on the drug’s packets.

If *Mr. John Doe* needs to buy *Testdrug 50MG*, a drug manufactured by *Generic Pharmaceuticals* but concerned about the fact that there is evidence or suspicion that some of *Generic Pharmaceuticals’* drugs are being counterfeited; and *Mr. John Doe* wants to use this system to determine the authenticity of the *Testdrug 50MG* before buying it. He then downloads and installs the appropriate eDecoder mobile application for his mobile phone.
platform – IOS (iPhone), Blackberry OS (Blackberry), Android (Google), etc. Before paying for the drug, Mr. John Doe starts the eDecoder application, focuses the Camera window on the eCode on the drug package, and scans eCode. The eDecoder application captures the eCode image, extracts the embedded eText, decodes it, and displays the result. If the eDecoder were unable to either extract or decode the eText, then Mr. Doe knows that the drug is a counterfeit. Otherwise, he can compare the drug’s serial number on the package with the serial number displayed by eDecoder. If they do not match, then he knows that the drug is a counterfeit.

2.2.2 Document Protection
Related to product counterfeiting, fake documents are also a prevalent problem in developing countries; and the inability to reliably verify documents compounds the issue. This system can be used to address this problem.

Assuming that Testagency is a hypothetical State Government agency that issues payment receipts and certificates (or documents) to its residents; and evidence has shown to Testagency that some miscreants have been forging or faking the receipts and certificates. Whenever the receipts or certificates are presented to a third-party, he/she can only visually inspect the documents and cannot reliably determine the authenticity of the document. As a result, Testagency wants to address this issue by using this system to produce secure e-Codes for the documents and enable the residents and third-parties to verify the authenticity of a document before they pay or accept it.

So, Testagency applies to the Key Issuer for an eKey package and supplies the required information. After processing the application, the Key Issuer generates and issues an eKey and eText generator to Testagency. To generate the eCode for a document with a specific serial number or document ID number, their eText generation application is used with the company name, document information (including the Serial or ID Number) and verification website. The Code Generator then produces eTexts, which are used to generate the eCodes which can be printed or affixed on each document. The relevant information about the document is also stored on the verification website, indexed with the serial or ID number.

When a resident or third-party is issued or presented with the document, he/she can immediately verify the authenticity of the document via the free mobile application. He or she then downloads and installs the appropriate eDecoder mobile application for his mobile phone platform – IOS (iPhone), Blackberry OS (Blackberry), Android (Google), etc. Before accepting the document, he/she starts the eDecoder application, focuses the Camera window on the eCode on the document, and scans eCode. The eDecoder application captures the eCode image, extracts the embedded eText, decodes it, and displays the result. If the eDecoder were unable to either extract or decode the eText, he/she knows that the document is forged. Otherwise, he/she can compare the document’s serial or ID number on the document with the one displayed by eDecoder. If they do not match, then he/she knows that the document is forged. Furthermore, if his/her mobile device has Internet connectivity, the eDecoder can display more information about the document from the verification website.

3.0 Benefits of the System
The main objective of this system is to address the major problems with existing or proposed systems for tackling counterfeiting in developing economies. The benefits of the system include, but not limited to, the following:
1. **Availability** - Unlike other mobile device based verification systems, this system does not require the availability of a GSM service or Internet connectivity in order to verify an eCode. In other words, a consumer only needs a mobile device that can download and install the eDecoder application. The eDecoder does not store any data and, therefore, is not susceptible to update requirements as a result of any changes in the eKey package.

2. **Ease of use** - Being a mobile application, the eDecoder is very easy to use – just focus the camera on the eCode; the eDecoder automatically scans, extracts, decodes, and displays the result. There is no room for error when entering product information – it’s not needed.

3. **Deterrence to Counterfeiters** - Given the versatility of the eDecoder to the consumer and the exorbitant cost and difficulty of any attempt to breach the system, potential fakers or counterfeiters are greatly discouraged.

4. **Cost Effectiveness** - It’s very affordable to either directly print the eCodes on the packages or documents or to print eCodes on labels and affix them on the packages. The eDecoder is a freely available mobile application.

5. **Scalability** - Non-consumer-centric and non-automated counterfeiting solutions are non-scalable as a result of their vulnerability to sudden widespread epidemic of product counterfeiting due to its enormous personnel manpower requirement. This system is easily scalable both in eCode generation by the product owner and verification by the consumer.

4.0 **Business and Economic Case for Developing Economies**

Extensive existence and practice of counterfeiting in developing economies, like Nigeria, is a microcosm of the general problem of lack of reliable verification and standardization in every facet of their national life. This work was motivated partly by the shocking levels of counterfeiting and its economic effects in Nigeria, which recently became the largest economy in Africa (Friedman, 2014). Those who are creative and innovative are dissuaded from materializing, pursuing or implementing their ideas. The fear is that once someone knows about your idea, he/she can easily steal it without any consequence. And once an idea is exposed, it can easily be counterfeited and the product produced and sold at much cheaper price. Most of the time, the perpetrators are those who have the financial capital or connection. And as a microcosm of the general problem in countries like Nigeria, as reported by Obi (2014), NAN (2013) and Abioye (2011), existing Intellectual Property laws are either not enforced or are victims of the endemic corruption in the society. These have created a devastating level of flippant attitude towards innovative thinking at all levels of Nigerian life; and those who dare to do otherwise usually are too secretive about their ideas to their detriment. Given the level of unemployment in Nigeria, many of the unemployed college graduates who would have become part of the economic engines via entrepreneurial ventures are dissuaded from engaging in innovative and creative business ideas, as noted by Waziri (2013) and Ladan (2013). Many of these potential entrepreneurs would pursue their business ambitions if there were meaningful ways for them to control their fate as they take those business risks. Unfortunately, the business environment is not conducive for such situations – one can easily lose everything without recourse.

What these potential entrepreneurs need is the ability, without depending on their government, to secure, protect, and market their ideas; and cost-effectively enable their
consumer base to reliably identify their products. The understanding is that, even when counterfeits exist, it’s helpful for the consumer to be able to make a distinction; and consequently, they will be able to manage and maintain their customer base; and generate economic activities and employment for their country.

5.0 Status of the System
A patent was filed and granted in Nigeria in December 2012 under Certificate Number 00079, RP Number NG/P/2012/679, and title "A system and method for reliable product security and verification".

The eKey package (both the eKey and eText generators) has been designed and implemented. The eText generator is available as an ActiveX or Java component (and in the future as a C/C++ library) that can easily be integrated into applicable custom software development. The eDecoder that supports QRC eCodes has also been implemented and published in the Android mobile operating system platform (Google Play).

This system has been piloted in a couple of Nigerian States, where it is been used to protect vehicle Emblems issued annually by the state governments. The state governments and authorized agents have been losing revenue from the sale of the Emblems as a result of other agents who have been faking the Emblems. The agents have, in the previous years, expended monetary and human resources in an effort to curtail the counterfeiting without success. With this system, as documented in the State’s internal annual budgetary documents, their revenue increased by at least 50%; and they did not employ or expend additional resources to protect the Emblems since they can no longer be faked or forged. Also, vehicle owners were able to easily verify the authenticity of their Emblems at the point of purchase. This system has also been accepted by the Ghanaian Driver and Vehicle Licensing Authority (DVLA) for protecting its vehicle stickers and will be deployed sometime in 2014.

6.0 Conclusions
The system presented in this paper addresses the core issues facing various entities all over the world in their efforts to effectively combat the numerous forms of counterfeiting. Some of the techniques employed in fighting counterfeiting have yielded some positive results; however, the counterfeiters seem to always be one step ahead in exploiting new technologies and terrains. By providing the consumers with a cost-effective, reliable, ubiquitous solution, this system is the ultimate nightmare to existing or potential counterfeiters. The system is very easy for consumers to use and product owners to integrate into their production systems; and it has wide applicability to any item that requires reliable protection.

7.0 References


