IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ADDITIVE MANUFACTURING ENHANCED QUICK RESPONSE CODE AS AN ANTI-COUNTERFEIT SOLUTION FOR NAFDAC MOBILE AUTHENTICATION SERVICES

[1] Ofut, Ogar Tumenayu, [2] Umoh Enoima Essien, [3] Egbung Kenneth Ocheden

[1]Lecturer/Researcher, [2] Lecturer/Researcher, [3] Lecturer/Researcher
[1]Deprtment of Computer science,
[1] Cross River university of Technology, Calabar, Nigeria

Abstract: Counterfeit products are global problem affecting the pharmaceutical industry and others. They are quickly becoming a major threat of our society. The production of personalized items and early prototypes became an easy task for everyone with the arrival of affordable 3D printing solutions and free, user-friendly 3D modeling software, the question of how to provide additional information to the printed shapes came up again. The proposed system can be conveniently implemented with a Fused Deposition Modelling 3D Printing Machines and Smartphones. The 3D printed QR-Code was adopted with the sole aim of eliminating the problem of duplicating and cloning of anti-counterfeit tag. An investigation on the unavoidable and unmanageable process variation on the 3D printing Mechanism was conducted. Evaluations show that the proposed model would outperform the existing system up to 85%.

***Index Terms* - QR code, unclonable, anti-counterfeit, Unmanageable Process Variation, 3D Printing, Additive Manufacturing, Mobile Authentication Service.**

I. INTRODUCTION

Quick Response codes or QR codes are 2-dimensional barcodes that have the storage capability of accommodating various kinds of information such as URL, Addresses, SMS, links, plain text, or contact information etc. The QR Code technology was first introduced in Japan with the sole purpose of tracking automobile parts. QR code can be referred to as a paper-based interactive connectivity link from the physical world image to its online world details. Quick response codes are widely used for tagging products, sharing information, and making digital payments due to their robustness against distortion, error correction features and small size (Garg et al, 2021).

This quite small square image can be decoded by a QR code reader installed on a smartphone. Investigation and experience have shown that the QR code images can at all times be scanned in different positions by mobile devices and it is possible to scan correctly and get all information that are stored in the image. A QR code reader could support the identification of a good by checking the QR code identifier against a remote database (Gianmarco B. et al, 2015).

The idea of the application of Authentication Technologies as an approach to fight counterfeiting is to build a secure authentication protocol. It is a Basic issue of identification and verification of an item from another source on the basis of specified features. In ISO 12931:2012 (ISO (2012) and (Li (2013)), Authentication Technologies are basically classified into Covert and Overt Techniques. The main difference between these two technologies is that the Overt Technologies can easily be used for verification directly by users who are familiar with them, but the Covert Technologies would at all times require the services of a professional with some special laboratory equipment in order to perform verification. Another difference is that (Davison 2011), Overt Techniques are mostly based on the sensorial capability of the human being: sight, sound, smell, touch and taste, while covert techniques are based on the digital information present in the token, which must be processed by a digital device (e.g., a computing device). The choice of an Enhance QR Code security for improving National Agency for Food and Drugs Administration and Control (NAFDAC) Mobile Authentication services for Fighting counterfeit is based on the flexibility of Overt Techniques as well as the growing population of smartphones.

The essence of an enhance QR Code technology is to further improve on the current Mobile Authentication Service (MAS) scheme as one of the anti-counterfeiting strategies to detect substandard and falsified (SF) medical products as introduced by NAFDAC in 2010. The current scheme powered by Sproxil uses scratch codes and Short Messaging Service (SMS) to empower consumers to verify the authenticity of medicines at the point of purchase (NAFDAC, 2018).

The need for the introduction of an Enhance QR code security techniques is to further compliment the current scratch codes and SMS verification process with a Modern sophisticated software with a widely used techniques (QR code) for the identification and tracking goods along the supply chain. The propose enhance QR code Technology would not only be beneficiary to the final consumer as in the case of the current system, but would also benefit the wholesaler that buy directly from the manufacturers in large quantity. With the advent of a secured QR code technology verification can be made during bulk purchase without tempering with the verification seal before it gets to the final consumer.

QR codes are easily collected and processed by a camera than the scratch codes that goes through an SMS clumsy process. The main strength of the QR code technique is its cost-effectiveness, the simplicity of creation of the QR code or its analysis by a consumer mass market device and the fact that a QR code can embed tracking information (Gianmarco B. et al, 2015). The major demerit of a QR code is that it can be easily duplicated or cloned. The easy to clone nature of QR code is the basis of this research work. To address this problem and produce an enhanced unclonable QR code, I hereby propose the use of Additive manufacturing or Three-Dimensional (3-D) printing. Additive manufacturing is an alternative to the traditional product manufacturing process through which three-dimensional (3-D) solid objects are created.

In other words, additive manufacturing is the same as 3-D printing (Lindemann, & Jahnke, 2017). Currently, additive manufacturing enables and facilitates the production of moderate to mass quantities of products that can be customized individually (Attaran, 2017). The benefits of additive manufacturing technologies make it possible to develop new solutions that can solve this problem (Papp et al, 2021). Technological protection is recommended to be the best way to avoid this problem.

Given these advantages, 3-D printing techniques can be used for carving a QR code on the surface of a product pack to deliver the product detail information to the wholesalers and consumers. The whole idea of using 3-D printing techniques for QR codes printing is because of its unavoidable and unmanageable process variation that occur during printing. The concept of 3D printing techniques will serve as an enhancement of the QR codes security because customization of individual QR code can be achieved making each product unique due to the variation provided by 3-D printing.

The variation process cannot in any case be repeated during the 3-D process therefore making it a none duplicated fingerprint. The peculiar nature 3-D printing techniques will make it impossible for the QR codes to be cloned or replicated by attackers of any form because each product is provided with a unique identity by the authorized producer due to the variation concept on the QR Code.

The proposed system is not only cost free but totally compatible with the existing QR code concept with smartphones. To this end, the proposed system is expected to be an end-to-end QR code mobile verification concept as an Anti-Counterfeit solution of 3D printed QR codes products with two parts to include; Mobile Application for QR code Verification, and a web-based verification system.

II. PROBLEM STATEMENT

The problem of study shall border on the improvement of the quality and security of mobile authentication services with the 3D printed QR code on product items. However, the existing Anti-Counterfeit packaging technologies such as Radio Frequency Identification (RFID) tag (Ghaith et al 2019), 1-Dimension Barcode (UPC, 2017), Digital Watermark (Jantana et al, 2013), are in one way or the other inappropriate in product retailing system. Firstly, attackers can hack the Anti-counterfeit system. Secondly, they always require extra sophisticated hardware or special devices to conduct the verification process.

The 3-D printer QR code techniques can immediately improve the security of the products because it is different from the regular QR codes application that can be easily cloned or duplicated. It is deduced that the variation occurrence in the 3-D printed QR code can be used to create customized and unduplicated fingerprint.

III. OBJECTIVE(S) OF THE STUDY

The following objectives are expected to be accomplish:

a) A detailed analysis of the variability of the 3-D printed productions with respect to the different hardware components, and the formulation of standard geometrical attribute into a printer format.

b) Investigation into customization of the QR code fingerprint in the 3-D printing prototype without changing the current traditional QR codes universal protocol.

c) The design of an intelligent fingerprint matching algorithm considering the geometric attributes of the QR codes and the 3-D printing machines mechanism.

d) Evaluation of the security and ability to withstand different attacking scenario will be conducted/.

IV. LITERATURE REVIEW

Identification and Data capturing: According to (Ruchir et al, 2010) Miscellaneous anti-counterfeit technologies are developed in the conventional manufacturing area.

(a)Holography (Robert, 2013) is a photographic recording of a light field based on the principle of interference. It is generated from the interference patterns obtained through the contact of laser beams by either angular image or laser technology. A high-definition hologram can use as a security identity tag.

(b) 1D Barcode, such as Universal Product Code (UPC, 2018), is a well-established optical-machine readable symbol. It contains simple, but high-density linear codes to embed the specific ID information. (c) Water mark is originally an identifying image or pattern in paper that appears as various shades of lightness/darkness when viewed by transmitted light. Later on, it is more widely extended to the digital domain by coding invisible ID into the noise-tolerant carrier (Ron, 1994). (d) RFID tag uses electromagnetic fields to automatically identify and track tags attached to objects. The tag contains electronically stored ID and communicates with the nearby RFID reader (Ari, 2006).

Enhanced QR Code Security: with the rapid increase in QR application and usage in recent time enhancement methods are expected to be explore in order to strengthen it security more. While doing these it would be important to integrate the traditional encryption methods onto the QR code to increase its complexity. In the case of Zhenbo et al. employ a prevalent holographic encryption method, double random-phase encoding in the Fresnel domain, to embed the hologram upon a QR code (Zhenbo et al, 2014). Vongpradhip et al. (Vongpradhip et al, 2012) proposed a method of embedding the watermark text with the QR code by applying DCT (Discrete-Cosine-Transform) transform. However, both methods can be hacked by the reverse methods once the attacker knows the integration domain (Vongpradhip et al, 2012).

Automatic fingerprint Authentication: Automatic fingerprint authentication system are currently being apply in a wide range of application in order to satisfy the demand for accurate identification. An early version of the unclonable identification system was proposed by Tolk (Tolk, 1992) based on random optical reflection patterns generated by the reflective particle tag. Similar works (Ravikanth et al, 2002) and (Pim & Boris, 2006) utilized different optical microstructures based on transparent media. Random, unforgeable fiber texture was studied in (Buchanan et al 2005) and (Bulens et al, 2010). According to (Lukas et al, 2006) studied the camera identification by investigating the unique sensor noise pattern from the captured images. (Dey et al. 2014) explored smartphone fingerprints based on the hardware imperfections during the sensor manufacturing process. Similarly, (Das et al. 2014) proposed to fingerprint devices through on-board acoustic components.

V. METHODOLOGY

The propose Anti-Counterfeit solution for NAFDAC Mobile Authentication Services shall be a cost-free Approach, and shall practically base on two commodities which are; Smartphone and 3D Printing machine. The system shall consist of a Mobile QR-code verification application and web-based verification system.

The Mobile QR-Code verification application shall be regulated and manage by NAFDAC were authorize producer of any of its certified product would be authorize with a 3D Printed QR-code which legitimacy can be verified by the customer. The application is main to capture the image of QR-code and sent it to web-based verification system.

Upon received of the QR-code image the web-based verification system shall verify the QR-code fingerprint and quickly replies the customer through the application. The web-based verification system is assumed to be maintain by NAFDAC because the fingerprint of all QR-code shall be secured in a central database in other not to be hack by adversaries.

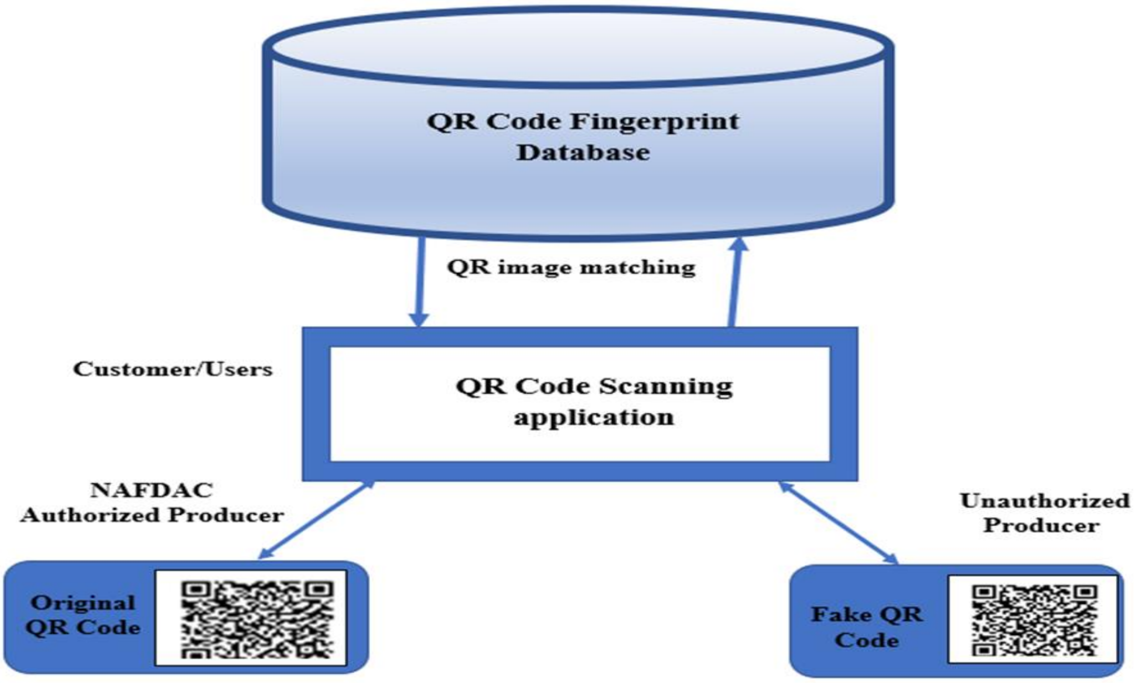
QR Code Fingerprint Database
QR image matching
Customer/Users
QR Code Scanning application
NAFDAC Authorized Producer
Unauthorized Producer
Original QR Code
Fake QR Code

Figure 1.0: Architecture of our threat model

Figure 1.0 shows the architecture of our threat model. We describe all entities as follows:

• **NAFDAC Authorized Producer:** Persons who fabricates the genuine products. In order to provide each product a unique identity, the authorized producer generates a QR code for each product in the all-in-one design, all-in-one manufacturing manner. The customer of interest can download an authorized smartphone app and verify if the product in the distributed store is genuine through the QR code verification.

• **Unauthorized Producer:** Persons who counterfeits high-intellectual or high-value 3D printed products for malicious purposes (e.g., illegal profit). The illegal producer knows that the customer of interest (victim) will use the authorized smartphone apps to verify the genuineness of the products. To convince the customer, he must replicate genuine QR codes on his fake 3D printed products.

• **Customer/User:** Persons who are interested in purchasing a 3D printed product. Customers want to verify the genuineness of the product, and they are educated to use the authorized smartphone app to do that. In practice, they launch the app and scan the QR code on the product they are interested in. Note that the customer can also be the authorized producer who conducts the product investigation.

VI. EXPECTED OUTPUTS/RESULTS

With an enhanced 3-D printed QR code concept the following exceptional outcomes are expected:

i. **Tag Customization:** the 3-D printed QR code tag on each product is an unavoidable and unmanageable process variation making each anti-counterfeit tag unique. With this high security provided, it can defend against counterfeit for both the Seller and the final consumer. Typically, each tag shall have a special verification protocol which makes it more difficult to access the tag content. Also, it will be important to note that the proposed system will not increase the cost.

ii. **Compatibility:** the 3-D printer QR codes does not in any way deviate from the traditional QR code content design structure. The integrated QR code contains two-layer information in our approach: (1) the product legitimacy verification; (2) the original QR content parsing (Chen et al, 2018). Therefore, the proposed system is in compliance with the tradition QR code concept with smartphones.

iii. **Faultless combination:** just like the traditional QR code technology works, the generated QR code can be integrated into the 3D printer design with ease. This natural and faultless combination makes it practically impossible for attackers to remove them for mischievous act.

VII. CONCLUSION

With the increasing versatility of QR codes in the identity-aware applications, we present an end-to-end approach for 3D printed product anti-counterfeit through unclonable QR code generation and verification using commodity 3D printers and smartphones. Considering the general trend of applying 3D printing in product manufacturing, our paper is the first work to explore and leverage the uncontrollable process variations in the 3D printing mechanism through the widely accepted QR code. Our extensive experiments verify the viability of the unclonable QR code fingerprint, which is effective against the 3D printed product counterfeit.

VIII. ACKNOWLEDGMENT

This research work would not have been possible without the financial support of the Tertiary Education Trust Fund (TETFUND) Institutional Based Research Award. We are especially indebted to Prof. Igwe Ewona, director of the directorate of Research and Development, Cross River university of Technology, Calabar, Nigeria.

.REFERENCES

[1] G. Baldini, I. Nai Fovino, R. Satta, A. Tsois, E. Checchi;. 2015. Survey of techniques for the fight against counterfeit goods and Intellectual Property Rights (IPR) infringement. European Commision JRC Technical Report. EUR 27688 EN.

[2] ISO 2012. ISO 12931:2012. Performance criteria for authentication solutions used to combat counterfeiting of material goods.

[3] Davison, M. 2011. Pharmaceutical anti-counterfeiting: combating the real danger from fake drugs. John Wiley & Sons.

[4] National Agency for Food and Drug Administration and Control (NAFDAC) 2018. Guidelines for Procurement and The Management of The Mobile Authentication Service (Mas) Scheme In Nigeria.

[5] Lindemann, C. F. W., & Jahnke, U. 2017. 11 Modelling of laser additive manufactured product lifecycle costs. In M. B. T.-L. A. M. Brandt (Ed.),Woodhead Publishing Series in Electronic and Optical Materials (pp. 281–316).Woodhead Publishing.https://doi.org/https://doi.org/10.1016/B978-0-08-100433-3.00011-7.

[6] Attaran, M. 2017. The rise of 3D printing: The advantages of additive manufacturing over traditional manufacturing. Business Horizons, 60(5), pp.677-688.

[7] Garg P., Chhabra S., Gupta G., Gupta G., Gupta M. 2021. Security And Privacy Issues Related To Quick Response Codes. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics XVII. DigitalForensics 2021. IFIP Advances in Information and Communication Technology, vol 612. Springer, Cham. https://doi.org/10.1007/978-3-030-88381-2_13.

[8] Ghaith Khalil , Robin Doss, and Morshed Chowdhury. 2019. A Comparison Survey Study on RFID Based Anti-Counterfeiting Systems. Journal of Sensor and Actuator Network. doi:10.3390/jsan8030037.

[9] The Global Language of Business 2017. Universal Product Code (UPC). Retrieved 2018-4-17 fromhttp://www.gs1us.org/resources/ standards/ean-upc-visuals.

[10] Jantana Panyavaraporn, Paramate Horkaew, and Wannaree Wongtrairat. 2013. QR Code Watermarking Algorithm Based on Wavelet Transform. In Communications and Information Technologies (ISCIT), 2013 13th International Symposium on. IEEE,791–796.

[11] Chen Song, Zhengxiong Li, Wenyao Xu, Chi Zhou, Zhanpeng Jin, and Kui Ren. 2018. My Smartphone Recognizes Genuine QR Codes! Practical Unclonable QR Code via 3D Printing. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 2, 2, Article 83 (June 2018), 20 pages. https://doi.org/10.1145/3214286.

[12] Ruchir Y Shah, Prajesh N Prajapati, and YK Agrawal. 2010. Anticounterfeit Packaging Technologies. Journal of Advanced PharmaceuticalTechnology & Research 1, 4 (2010), 368.

[13] Robert Collier. 2013. Optical Holography. Elsevier.

[14] The Global Language of Business. 2017. Universal Product Code (UPC). Retrieved 2018-4-17fromhttp://www.gs1us.org/resources/ standards/ean-upc-visuals

[15] Ron G Van Schyndel, Andrew Z Tirkel, and Charles F Osborne. 1994. A Digital Watermark. In Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference, Vol.2.IEEE,86–90.

[16] Ari Juels. 2006. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communications 24,2(2006),381–394.