A cost-effective counterfeiting prevention method using hashing, QR code, and website

Monir Hossain[1], Momotaz Begum[2], Bimal Chandra Das[3], Jia Uddin[4]

[1]Department of Computer Science and Engineering, Faculty of Engineering, CCN University of Science and Technology, Cumilla, Bangladesh
[2]Department of Computer Science and Engineering, Faculty of Electrical and Electronic Engineering, Dhaka University of Engineering and Technology, Gazipur, Bangladesh
[3]Department of Information Technology and Management, Faculty of Science and Information Technology, Daffodil International University, Daffodil Smart City, Bangladesh
[4]Department of AI and BigData, Endicott College, Woosong University, Daejeon, South Korea

Article Info

Article history:

Received Jan 20, 2024
Revised Feb 28, 2024
Accepted Mar 6, 2024

Keywords:

Anti-counterfeiting
Fake product detection
Hashing
Supply chain
Technologies

ABSTRACT

In this paper, we proposed a cost-effective software method to prevent counterfeiting where we used a website, quick-response (QR) code, and hashing. At the early stage of the product, the system will create a unique ID and a password with a random password generator for all products. Then, the password hash would be stored along with the ID in the database. At the same time, the password would be converted into a QR code for each product. The manufacturer will collect the QR code and ID and attach them to the product. When consumers attempt to verify the product, they will enter the website provided by the manufacturer and scan the QR code. After applying the same hash used before, the code will be checked on the database. After a successful check, the product entity will be destroyed and the life of the product ends. This paper contains flowcharts, figures, cost estimation, and a detailed explanation of the system. As it only requires domain hosting, thus the fixed cost of the system is so lower to bear for small enterprises also. We built a similar system using PHP, HTML, JavaScript for websites, and MYSQL for databases.

Corresponding Author:

Jia Uddin
Department of AI and Big Data, Endicott College, Woosong University
59 Baengnyong-ro, Dong-gu, Daejeon, South Korea
Email: jia.uddin@wsu.ac.kr

1. INTRODUCTION

Counterfeit products are unauthorized replicas or copies of genuine goods, such as consumer products, cosmetics, luxury items, and medicine which bear a close resemblance to the authentic item in terms of appearance, packaging, or branding. These items are typically produced and sold without the knowledge or permission of the original manufacturer or brand owner. They are made to deceive consumers into believing they are purchasing a genuine product, often at a lower price [1], [2]. However, counterfeit goods are generally of inferior quality [3] and may not meet the safety, performance, or ethical standards associated with the authentic products they imitate. Counterfeiting is illegal in most countries and is considered a form of intellectual property infringement. It not only harms legitimate manufacturers or brand owners by diluting their brand reputation and market share but also poses risks to consumer health and safety [4]. Counterfeit goods can range from counterfeit currency [5] and documents to counterfeit designer clothing [6], electronics [7], pharmaceuticals [8], and other consumer goods [9]. An actual picture of counterfeiting we can observe in developing countries [10] like Bangladesh [11], [12]. Director General of

National Consumers of Bangladesh, about the counterfeit foreign products discovered in Dhaka, states, "These products do not have any name of the importers, their address, and even the material requirements planning (MRP). These consumer items cannot be imported in luggage even dodging customs, which means all of these products are counterfeit." By taking fake medicine for years and years, people are becoming more susceptible to health risks and complications [13], [14]. Efforts are made by governments, law enforcement agencies, and brand owners to combat counterfeiting through increased surveillance, stricter regulations, public awareness campaigns, and collaboration with international organizations. But these are not enough. With the advancement of technologies, more technological involvement is also required in this sector to differentiate original and fake products.

The literature review was conducted with meticulous attention and precision to define the problem at hand. Various methodologies are thoroughly examined to propose and implement the current project. The literature that has been reviewed is categorized into distinct sections to facilitate a comprehensive analysis. This classification aids in studying the literature according to its respective context. There are several crucial solutions to combat counterfeiting across various industries [15], such as radio frequency identification (RFID), blockchain, cryptography, and machine learning. Each of these techniques is discussed briefly with their pros and cons below. RFID technology is employed to combat counterfeiting by providing a secure and traceable method of product identification. RFID tags, containing unique electronic codes, are embedded in authentic products. These tags emit radio signals that can be read by authorized scanners. When a product is scanned, its unique code is verified against a centralized database, enabling immediate authentication. If the code is not registered or flagged as counterfeit, an alert is triggered, indicating a potential fake. This real-time verification significantly reduces the chances of counterfeit products entering the supply chain or reaching consumers, safeguarding against fraud and protecting brand reputation [16]–[18]. The cost of 20-50 cents acts as a deterrent for small and medium-level manufacturers to adopt RFID technology. However, for those where cost is not a significant factor, RFID presents benefits despite the potential for tag cloning. By using blockchain technology, Each product is assigned a unique identifier that is recorded on the blockchain, enabling stakeholders to trace its entire lifecycle. This decentralized nature of the blockchain ensures that the data cannot be altered or tampered with, providing a reliable record of each transaction. With the ability to verify the provenance of products, blockchain enhances trust, eliminates counterfeit goods, and enables consumers to make informed purchasing decisions, thereby reducing the impact of counterfeiting [19]–[21]. However, it includes scalability challenges due to the increasing size of the chain and the energy-intensive nature of certain consensus algorithms, such as proof of work, which can have significant environmental impacts. Additionally, the immutability of blockchain can also pose challenges when errors need to be corrected or when data needs to be updated or removed. Thus it is not suitable for small manufacturers. Through the use of cryptographic techniques such as digital signatures, product information can be securely encrypted and verified [22]. By encrypting and validating data using cryptographic key pairs (public and private key), it becomes extremely difficult for counterfeiters to tamper with or forge information, enabling reliable verification and protection against counterfeit goods. But it includes the potential vulnerability of encryption algorithms to technological advancements, such as quantum computing, which could potentially break current encryption methods. Additionally, there is a risk of misusing or mishandling cryptographic keys, leading to security breaches if keys are compromised or lost. Shaik [23] introduced a software technique that incorporates cryptography, mobile apps, and web services. While this approach reduces costs, it does come with the drawback of increased overhead due to the calculation of encryption and decryption. Additionally, the resulting QR code becomes more complex, leading to a significant increase in scanning time. Machine learning also proposed to reduce counterfeiting by analyzing patterns, identifying anomalies, and detecting counterfeit products or activities. By training models on large datasets, machine learning algorithms can learn to differentiate between genuine and counterfeit items, enabling automated and accurate detection, thereby enhancing anti-counterfeiting efforts [24], [25]. The drawbacks of machine learning in anti-counterfeiting include the need for large and diverse datasets for effective training, which may be challenging to obtain in certain cases, and the potential for adversarial attacks where malicious actors attempt to manipulate or deceive the machine learning models to bypass detection methods.

We have examined a concise overview of alternative methods and highlighted their limitations for small and medium-sized manufacturers. The majority of methods rely on mobile apps for product verification at the consumer end. However, considering the diverse range of mobile devices and operating systems available, this necessitates the development of different apps for each system. Consequently, manufacturers face increased implementation costs and resources. Our proposed approach offers significant advantages over alternative methods, particularly those employing software, in terms of time, memory, and cost. Despite this advantage, there is currently no evidence supporting their widespread use for product verification at the consumer end using websites. The main contribution of this paper is summarized as i) Proposing a cost-effective software method with a proper diagram for preventing counterfeiting, using Hasing and a website that makes it more accessible to small and medium-sized enterprises; ii) Developing a complete product life cycle that enables the easy identification of original products; iii) Providing step by step unique packaging technique to ensure more security; iv) Performance and cost analysis of the result of the real implemented system; v) An overview of all possible ways to use this system commercially, and vi) The challenges and future research directions are discussed.

The rest of the paper is organized as follows. In section 2, we have included a detailed description of the materials utilized in our approach and an explanation of our method is supported by figures, images, and tables. Besides, how our approach detects counterfeit and how we can implement it in real life are also included with step-by-step instructions in section 2. We have presented results, critical discussion, limitations, and future scope in section 3. Finally, conclusions are drawn in section 4. For convenient referencing, Table 1 represents the acronyms used in this paper.

Table 1. List of acronyms

Acronyms	Abbreviations
RFID	Radiofrequency identification
HTML	Hypertext markup language
CSS	Cascading style sheets
PHP	Hypertext preprocessor
QR	Quick response
PDF	Portable document format
PNG	Portable network graphic
JPEG	Joint photographic experts group
DBMS	Database management system
URL	Uniform resource locator

2. RESEARCH METHOD

2.1. Materials

In this section, we explain the tools or functionality that will be used to describe our method and also, they play an important role in implementing the system in the real environment. Each tool is explained in such a way that knowledgeable readers can get a clear idea about that. As well as references are added so that an interested reader can know more details.

2.1.1. Hashing

Hashing is a process of converting input data of any size into a fixed-size value or hash code. The hash code is typically a numeric or alphanumeric representation of the input data. Hash functions are mathematical algorithms used to perform this transformation. Hashing is a one-way process shown in Figure 1, one cannot reverse-engineer the original data from the hash code. There are numerous hashing functions available, each designed with specific properties and use cases. Some examples of different hashing functions are [26] MD5, SHA-1, SHA-256 (widely used), SHA-3, Blake2, and MurmurHas. Most of them work in the average time complexity of O(n), where, n represents the size of the input data. So, individuals could develop their custom hash functions as well.

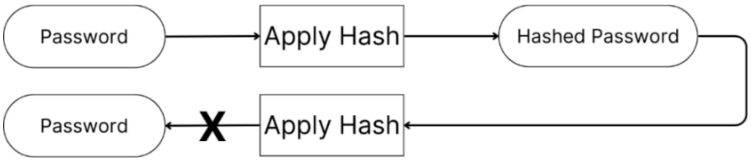


Figure 1. Unidirectional hashing system

2.1.2. Random password generation

A random password generator is a tool or algorithm that generates a password consisting of a combination of random characters [27]. The purpose of a random password generator is to create strong and secure passwords that are difficult for others to guess or crack. It is applied to choose a random character from the defined set of characters that will be used to generate the password. In PHP, the rand() is the built-in function for a random number generator. It is worth noting that the time complexity of the rand() function is usually not a major concern for most applications, as it tends to be relatively fast. Moreover, mt_rand() and random_int() can also be employed to get better-quality random numbers.

2.1.3. Database

A database is an organized collection of data that is stored and managed using specific software called a DBMS [28]. It provides a structured way to store, retrieve, update, and manage data efficiently and securely. MYSQL is also a database that stores data in tables with rows and columns [29].

2.1.4. QR codes

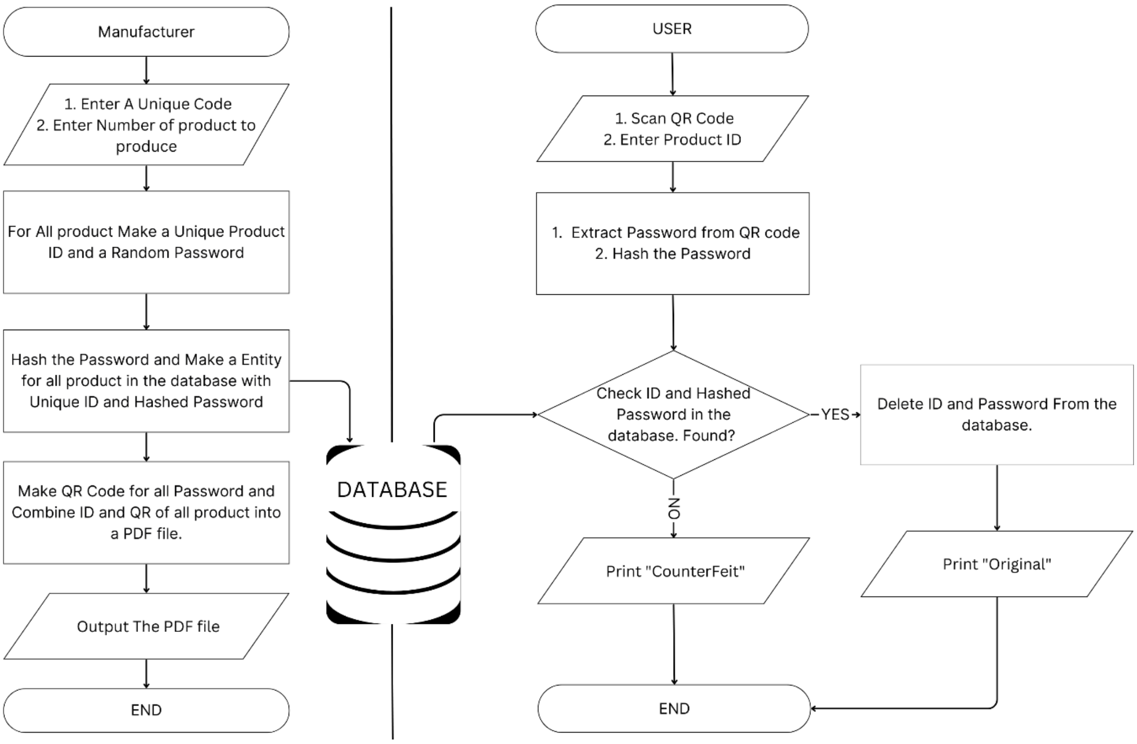
A QR code [30], short for quick response code, is a two-dimensional barcode that contains data quickly and easily scanned using a smartphone or QR code reader. These codes consist of black and white squares arranged in a square grid pattern. QR codes can store various types of information, such as URLs, text, contact details, and more. They are widely used for marketing, advertising, inventory management, mobile payments, and ticketing. With their ability to store large amounts of data and their ease of use, QR codes have become increasingly popular, revolutionizing the way we interact with information in the digital world. “qrlib.php” is used as an open-source library for QR code generation in PHP.

2.1.5. Websites

Websites are online platforms that provide information, services, and resources accessible through the internet. They consist of web pages containing text, images, videos, and interactive elements. Websites are created using various technologies like HTML, CSS, and JavaScript and are accessed through web browsers by users worldwide.

2.2. Proposed method

This section introduces a product life cycle designed to combat counterfeiting in the market. The life cycle of a product's identity begins with the manufacturer's initiative and concludes with user verification through scanning. Figure 2 shows the cycle can be described in two phases: the manufacturer phase shown in (Figure 2(a)) and the verification phase shown in (Figure 2(b)).


Manufacturer
1. Enter A Unique Code
2. Enter Number of product to produce
For All product Make a Unique Product ID and a Random Password
Hash the Password and Make a Entity for all product in the database with Unique ID and Hashed Password
Make QR Code for all Password and Combine ID and QR of all product into a PDF file.
Output The PDF file
END
DATABASE
USER
1. Scan QR Code
2. Enter Product ID
1. Extract Password from QR code
2. Hash the Password
Check ID and Hashed Password in the database. Found?
YES
Delete ID and Password From the database.
NO
Print "CounterFeit"
Print "Original"
END

(a) (b)

Figure 2. The proposed counterfeit detection system (a) manufacturer phase of the proposed system and (b) verification phase of the proposed system

2.2.1. Manufacturer phase

Manufacturers can select a product prefix code for a specific batch of products, although this is not mandatory. They also determine the desired quantity of products to be produced during the season. For instance, let us consider Unilever's aim to produce 100 units of LUX soap for this season. In this case, they might choose the prefix "LX2023." Once the prefix code and quantity are obtained, the system generates a unique ID by placing the prefix code first. Also, a random password is generated for each product using a random password generator. Subsequently, the generated password undergoes a hash function for storage purposes. To enhance accessibility and convenience, the system converts the actual password into a QR code using a QR code generator. Each unique ID and its corresponding hashed password are stored in the database. Moreover, the system generates a PDF containing all the unique IDs and their respective QR codes. Manufacturers must attach one entity (ID and corresponding QR) from PDF to each product's outer package. Coating the ID with the flipped QR code shown in Figure 3 will add extra security [will discuss later] but it is not mandatory, ID and QR code should be attached to the packet in any way.

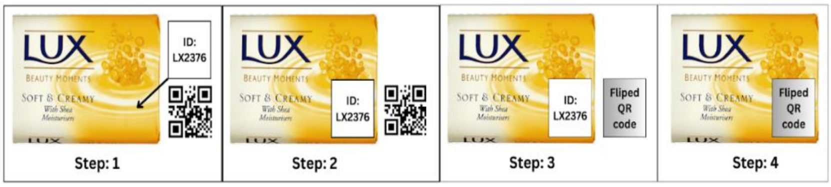


Figure 3. Proposed QR CODE and ID adjustment system for better result

2.2.2. Verification phase

This phase represents the verification and culmination stage of individual product life cycles. Once the purchase agreement is finalized with the seller, customers are granted the opportunity to scan the QR code. Using their mobile devices, customers access the manufacturer-provided website and scan the QR code, subsequently entering the product ID. The system then scans the QR code and retrieves the actual password associated with it. By applying the same hash function used by the manufacturer, a hashed password is generated. Next, the system checks the database for a valid entry matching the provided product ID and hashed password. If a valid entity is found, it is removed from the database, and the user is informed that the product is genuine and original. However, if the product ID and hashed password combination are not found in the database, the system identifies it as a counterfeit product. This phase ensures that customers can verify the authenticity of the product by scanning the QR code, offering a reliable method to distinguish genuine products from counterfeit ones.

2.3. Detection of counterfeit product

To grasp the process of detecting counterfeit items, it is essential to explore how these fraudulent products enter the market. Counterfeiters skillfully replicate the appearance of genuine items by creating master copies of packaging, product size, product shape, and product color. At times, distinguishing between a fake and an authentic product can be exceedingly challenging. Even experts may struggle to identify the discrepancies when presented with both items side by side, as they can appear virtually identical. Our solution introduces an additional layer of security by incorporating unique IDs and QR codes on each product. This implementation significantly enhances the ability to detect counterfeit items. Two possible scenarios may arise. Firstly, counterfeiters may attempt to affix arbitrary IDs and QR codes onto their counterfeit products since they do not possess genuine IDs or QR codes for any product. When consumers scan these products, the mismatch between the ID and QR code and the corresponding database entry will trigger a counterfeit alert. Alternatively, counterfeiters may acquire an ID or QR code from an original product and replicate it onto their fake product. However, this approach proves futile for the counterfeiters. This is because, upon purchase, the original product's identity is instantaneously removed from the database. Furthermore, if the seller engages in this practice, they would only incur losses since the expenses involved in producing the counterfeit product, along with the additional costs, surpass the value of the original item. It is worth noting that an additional security measure can be implemented by manufacturers. They can attach an ID and QR code using a technique where the ID is coated with a flipped (upside-down) QR code, as depicted in Figure 3. This clever approach hides both the ID and QR code from plain sight. Consequently, counterfeiting the ID and QR code from an original product becomes more challenging, providing an extra layer of security.

2.4. Implementation and maintenance

The system can be implemented either by individual manufacturers or through collaborative adoption by multiple companies. The following tasks encompass the entire workflow: i) managing a domain and server, ii) creating a database with two columns for ID and hashed passwords, iii) developing a distinct user and manufacturer interface, iv) enabling the user to scan QR data, input an ID, and verify it in the database through simple API calls, v) allowing the manufacturer to input the desired number of products (N), a product prefix, and generating new entries for all N products in the database with unique IDs and hashed passwords, and vi) providing the ID and QR of the password in PDF format or other format for future reference.

Now, let us consider the scenarios for implementing this system: if a single company adopts this system, they do not need to undertake any additional steps. In the case of multiple companies adopting it jointly, each company may use a unique prefix for formal purposes. Additionally, a login system can be implemented at the manufacturer's end to ensure that one company cannot create entities on behalf of others. Furthermore, this system can be adopted by the government, requiring all companies to generate identities using the system, and users verifying their identities through the system. In this scenario, the government can receive payments from companies based on several factors such as company size or the number of products.

3. RESULTS AND DISCUSSION

A similar system was developed in our lab, illustrated in Figure 2, which incorporates various components. To generate random passwords, we implemented our generator function using the rand() function of PHP to randomly pick a character for each position of password, which has an impressive speed, taking only 14 to 17 microseconds to generate a single password. To create QR codes in PNG or JPEG format, we employed a PHP QR code library named “qrlib.php”. Additionally, we utilized the FPDF library for generating PDF documents. The scanner on the user's end was built using JavaScript.

During our testing of the system, we discovered that the processing time for each entity, which includes random password generation, QR code creation for the password, password hashing, entity creation in the database, and PDF document generation, took approximately 40 milliseconds from the manufacturer's end. On the other hand, the closest system to our system takes (734+141) 875 milliseconds only for encrypt and QR code generation [23]. It indicates that our method is approximately 21 times faster than the nearest one in the first phase. At the user end, after input taking to output is generated on the screen, the processing time is measured to be approximately 94 milliseconds. This time includes several tasks such as QR code decoding, password hashing, searching for the entity in the database, deleting the entity if found, and displaying the results on the user's screen. The tabulated results are shown in Table 2. At this end, (125+628) 753 milliseconds were recorded by the nearest competitor [23]. Here also our proposed system performed 8 times faster. Our findings indicate that the computational requirements are primarily concentrated in the hashing process. Unlike asymmetric encryption, hashing demands less time and computational power for generating and verifying counterfeit products. Additionally, after applying asymmetric encryption, the complexity of the QR code increases substantially, leading to significant scanning times that can frustrate customers.

Table 2. Recorded runtime at our system

List of activities	Recorded time
Time to generate random password	14-17 µs
Time takes at manufacturer end (random password generation + QR making + pdf making + hashing of the password + entity creation in a database)	40 ms per entity
Time takes at the user end (QR decode + hashing of the password + delete from database + receive API response + show in the output)	94 ms

Some other distinctive features can be mentioned that make our method apart from other methods. Implementing a mobile app incurs higher costs due to the need for compatibility across different devices and operating systems, such as Android and iOS. However, by opting for a common website accessible through various devices even using default internet browsers, the initial implementation costs are significantly reduced. An estimation of cost is shown in Table 3. This approach becomes more accessible and encourages small manufacturers to adopt the method, as they can leverage existing infrastructure without the need for extensive device-specific development. Besides, customers will not have the extra trouble of installing additional software. In comparison to the blockchain method, this approach requires less memory. Furthermore, as the blockchain grows larger, it becomes increasingly difficult to manage and control, posing challenges for scalability and efficiency. Besides, no special skilled personnel are needed. Since we are using a centralized database, there is a risk of cyber-attack. Although data will not be leaked due to hashing, backup is necessary to prevent data destruction. But, now cyber-attacks like SQL injection can be detected easily [31]. Future research may look into developing such a system, that does not need any database or internet connection to verify the product without negatively affecting cost and required time.

Table 3. Estimated cost for our proposed system

Description of cost	Amount
Domain cost	$25/year
Hosting cost	$10/year
System development (onetime)	100$ -
QR code labels with ID for each product	2-3 cents

4. CONCLUSION

Counterfeiters have proliferated across various sectors, including medicine, electronics, food, luxury goods, cosmetics, and more. Their activities in areas such as food, medicine, and cosmetics pose a significant threat to public well-being and financial security. The proliferation of counterfeit products has inflicted substantial financial losses on legitimate businesses, severely impacting their revenue streams. Furthermore, these illicit operations evade taxes and VAT, BYPASSING government regulations and creating a detrimental impact on the overall economy. There are different techniques to combat counterfeiting across various industries. We have shown their limitations. In our study, we propose a comprehensive product life cycle approach to combat counterfeiting at a relatively low cost, leveraging a website, QR codes, and hashing techniques. Throughout the study, we have shown “how our method detects counterfeit,” “how it can be implemented,” “how our unique packaging technique provides more security,” and “how it saves time and cost over other methods”. As it saves time and cost, it is a perfect solution for all industries, especially for small and mid-level manufacturers. In conclusion, implementing this system offers a practical, time-saving, and cost-effective solution to combat counterfeiting, safeguarding both the interests of product owners and the well-being of consumers.

ACKNOWLEDGMENTS

This research is funded by Woosong University Academic Research 2024.

REFERENCES

[1] Y. G. Elsantil and E. G. A. Hamza, “A review of internal and external factors underlying the purchase of counterfeit products,” *Academy of Strategic Management Journal*, vol. 20, no. 1, pp. 1–13, 2021.

[2] M. A. H. B. M. Yunos and M. B. A. Lasi, “Factors affecting consumers’ intention to purchase counterfeit products in fashion industry,” *International Journal of Academic Research in Business and Social Sciences*, vol. 10, pp. 939–949, Oct. 2020, doi: 10.6007/ijarbss/v10-i10/8013.

[3] G. Grossman and C. Shapiro, “Counterfeit-product trade,” Cambridge, MA, Mar. 1986. doi: 10.3386/w1876.

[4] H. Park-Poaps and J. Kang, “An experiment on non-luxury fashion counterfeit purchase: The effects of brand reputation, fashion attributes, and attitudes toward counterfeiting,” *Journal of Brand Management*, vol. 25, no. 2, pp. 185–196, Mar. 2018, doi: 10.1057/s41262-017-0077-x.

[5] M. A. Siddiki, M. N. Hossain, K. Akhter, and M. R. Rahman, “Bangladeshi currency identification and fraudulence detection using deep learning and feature extraction,” *International Journal of Computer Science and Mobile Computing*, vol. 12, no. 1, pp. 1–13, Jan. 2023, doi: 10.47760/ijcsmc.2022.v12i01.001.

[6] C. L. Chen *et al.*, “An anti-counterfeit and traceable management system for brand clothing with hyperledger fabric framework,” *Symmetry*, vol. 13, no. 11, pp. 1–32, Oct. 2021, doi: 10.3390/sym13112048.

[7] T. Bryant, Y. Chen, D. S. Koblah, D. Forte, and N. Maghari, “A brief tutorial on mixed signal approaches to combat electronic counterfeiting,” *IEEE Open Journal of Circuits and Systems*, vol. 4, pp. 99–114, 2023, doi: 10.1109/ojcas.2023.3253144.

[8] M. Ten Ham, “Health risks of counterfeit pharmaceuticals,” *Drug Safety*, vol. 26, no. 14, pp. 991–997, 2003, doi: 10.2165/00002018-200326140-00001.

[9] Y. Aghoutane, M. Brebu, M. Moufid, R. Ionescu, B. Bouchikhi, and N. E. Bari, “Detection of counterfeit perfumes by using gc-ms technique and electronic nose system combined with chemometric tools,” *Micromachines*, vol. 14, no. 3, pp. 1–12, Feb. 2023, doi: 10.3390/mi14030524.

[10] B. Glass, “Counterfeit drugs and medical devices in developing countries,” *Research and Reports in Tropical Medicine*, pp. 11–22, Mar. 2014, doi: 10.2147/rrtm.s39354.

[11] M. O. Gani, M. I. Alam, Mostaquim-Al-Islam, S. A. Chowdhury, and M. O. Faruq, “Factors affecting consumers’ purchase intention for counterfeit luxury goods in Bangladesh,” *Innovative Marketing*, vol. 15, no. 4, pp. 27–41, Nov. 2019, doi: 10.21511/im.15(4).2019.03.

[12] M. M. Jashim, J. S. K. Singh, and B. C. Yin-Fah, “Influence of religiosity and attitude towards intention to purchase counterfeit products. an empirical study in Dhaka, Bangladesh,” *International Journal of Psychosocial Rehabilitation*, vol. 24, no. 2, pp. 1137–1148, Feb. 2020, doi: 10.37200/ijpr/v24i2/pr200416.

[13] A. Delepierre, A. Gayot, and A. Carpentier, “Update on counterfeit antibiotics worldwide; Public health risks,” *Medecine et Maladies Infectieuses*, vol. 42, no. 6, pp. 247–255, Jun. 2012, doi: 10.1016/j.medmal.2012.04.007.

[14] E. A. Blackstone, J. P. Fuhr, and S. Pociask, “The health and economic effects of counterfeit drugs,” *American Health and Drug Benefits*, vol. 7, no. 4, pp. 216–224, 2014.

[15] S. P. Gayialis, E. P. Kechagias, G. A. Papadopoulos, and D. Masouras, “A review and classification framework of traceability approaches for identifying product supply chain counterfeiting,” *Sustainability (Switzerland)*, vol. 14, no. 11, pp. 1–20, May 2022, doi: 10.3390/su14116666.

[16] P. Tuyls and L. Batina, “RFID-tags for anti-counterfeiting,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 3960 LNCS, 2006, pp. 115–131. doi: 10.1007/11605805_8.

[17] G. Khalil, R. Doss, and M. Chowdhury, “A novel RFID-based anti-counterfeiting scheme for retail environments,” *IEEE Access*, vol. 8, pp. 47952–47962, 2020, doi: 10.1109/ACCESS.2020.2979264.

[18] G. Khalil, R. Doss, and M. Chowdhury, “A comparison survey study on RFID based anti-counterfeiting systems,” *Journal of Sensor and Actuator Networks*, vol. 8, no. 3, pp. 1–15, Jul. 2019, doi: 10.3390/jsan8030037.

[19] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, “A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain,” *IEEE Access*, vol. 5, pp. 17465–17477, 2017, doi: 10.1109/ACCESS.2017.2720760.

[20] J. Ma, S. Y. Lin, X. Chen, H. M. Sun, Y. C. Chen, and H. Wang, “A Blockchain-based application system for product anti-counterfeiting,” *IEEE Access*, vol. 8, pp. 77642–77652, 2020, doi: 10.1109/ACCESS.2020.2972026.

[21] Y. Lu, P. Li, and H. Xu, “A food anti-counterfeiting traceability system based on blockchain and internet of things,” *Procedia Computer Science*, vol. 199, pp. 629–636, 2021, doi: 10.1016/j.procs.2022.01.077.

[22] M. Lehtonen, N. Oertel, and H. Vogt, “Features, identity, tracing, and cryptography in product authentication,” *2007 IEEE International Technology Management Conference, ICE 2007*, 2016.

[23] C. Shaik, “Preventing counterfeit products using cryptography, QR code and webservice,” *Computer Science & Engineering: An International Journal*, vol. 11, no. 1, pp. 1–11, Feb. 2021, doi: 10.5121/cseij.2021.11101.

[24] E. Daoud, D. Vu, H. Nguyen, and M. Gaedke, “Improving fake product detection using ai-based technology,” in *Proceedings of the 18th International Conference on e-Society (ES 2020)*, IADIS Press, Apr. 2020, pp. 119–125. doi: 10.33965/es2020_202005l015.

[25] H. Zheng, C. Zhou, X. Li, T. Wang, and C. You, “Forgery detection for anti-counterfeiting patterns using deep single classifier,” *Applied Sciences (Switzerland)*, vol. 13, no. 14, pp. 1–18, Jul. 2023, doi: 10.3390/app13148101.

[26] G. D. Knott, “Hashing Functions.,” *Computer Journal*, vol. 18, no. 3, pp. 265–278, Mar. 1975, doi: 10.1093/comjnl/18.3.265.

[27] M. D. Leonhard and V. N. Venkatakrishnan, “A comparative study of three random password generators,” in *2007 IEEE International Conference on Electro/Information Technology, EIT 2007*, IEEE, May 2007, pp. 227–232. doi: 10.1109/EIT.2007.4374533.

[28] M. J. F. Iglesias, “Brief introduction to database systems,” *atlanTTic - Universidade de Vigo*, pp. 1–19, 2018.

[29] B. Christudas, “MySQL,” in *Practical Microservices Architectural Patterns*, Berkeley, CA: Apress, 2019, pp. 877–884. doi: 10.1007/978-1-4842-4501-9_27.

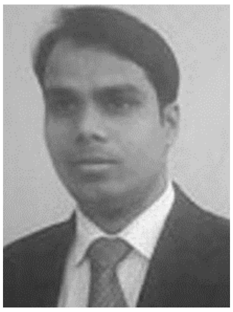
[30] S. Tiwari, “An introduction to QR code technology,” in *2016 International Conference on Information Technology (ICIT)*, IEEE, Dec. 2017, pp. 39–44. doi: 10.1109/icit.2016.021.

[31] H. Furhad, R. K. Chakrabortty, M. J. Ryan, J. Uddin, and I. H. Sarker, “A hybrid framework for detecting structured query language injection attacks in web-based applications,” *International Journal of Electrical and Computer Engineering*, vol. 12, no. 5, pp. 5405–5414, 2022, doi: 10.11591/ijece.v12i5.pp5405-5414.

BIOGRAPHIES OF AUTHORS

Monir Hossain is a Lecturer at the Department of Computer Science and Engineering, CCN University of Science and Technology. He recently completed his B.Sc. in engineering (CSE) from Dhaka University of Engineering and Technology. With a strong background in technical concepts and problem-solving, he combines his engineering expertise with his love for storytelling to create engaging and informative content. His dedication to research and continuous learning enables him to stay up-to-date with the latest advancements in the field, ensuring that his writing reflects cutting-edge knowledge and trends. His research interests include quantum computing, algorithm optimization, cryptography, and quantum machine learning. He can be contacted at email: monirho.cse@gmail.com.

Momotaz Begum Ph.D. is a distinguished professor in the Department of Computer Science and Engineering at Dhaka University of Engineering and Technology (DUET), Gazipur. Her research interests encompass reliability, software engineering, artificial neural networks, data mining, data clustering, information systems, and analysis. Her specialization lies in software rejuvenation and software aging, as well as human pose recognition. She has published 18 journal papers and 9 conference papers in the world’s reputed journals and conferences. She can be contacted at email: drmomotaz@duet.ac.bd.



Dr. Bimal Chandra Das received his bachelor of science with honors and master of science degrees in applied mathematics from the University of Chittagong (CU), Bangladesh in 2000 and 2001 respectively. He received his Ph.D. degree in communication engineering and informatics from the University of Electro-Communications (UEC), Tokyo, Japan in 2018. Currently, he is working as an Associate Professor at Daffodil International University (DIU), Dhaka, Bangladesh. He joined Daffodil International University in 2008 as a Lecturer. He also worked for about 2 years at different universities before joining DIU. He worked as a research associate at The University of Electro-Communications, Japan from April 2015 to March 2018. He received the Japan Government (Monbukagakusho: Mext) Scholarship 2014 for a Ph.D. degree. Recently, he completed a post-doctoral research fellow project work at UEC, Japan. He presented many research papers in Japan, Canada, and the United States. during his Ph.D. research. His research interest includes computer network, network congestion, power-efficient networks, continuous optimization, and conic programming and its applications. He published many research papers and books in the world's reputed journals and conferences. He can be contacted at email: bcdas@daffodilvarsity.edu.bd.

Jia Uddin is an Assistant Professor, at the AI and Big Data Department, at Endicott College, Woosong University, Daejeon, South Korea. He received a Ph.D. in Computer Engineering from the University of Ulsan, South Korea, an M.Sc. in Electrical Engineering (Specialization: Telecommunications), from the Blekinge Institute of Technology, Sweden, and a B.Sc. in Computer and Communication Engineering, from the International Islamic University Chittagong, Bangladesh. He was a visiting faculty at the School of Computing, Staffordshire University, United Kingdom, Telkom University, Indonesia, and the University of Foggia, Italy. He is an Associate Professor (now on leave), at the Department of Computer Science and Engineering, Brac University, Dhaka, Bangladesh. His research interests are industrial fault diagnosis, machine learning/deep learning-based prediction, and detection using multimedia signals. He can be contacted at email: jia.uddin@wsu.ac.kr.