International Journal of Internet Manufacturing and Services

ISSN online: 1751-6056 - ISSN print: 1751-6048
https://www.inderscience.com/ijims

Research on cloud anti-counterfeiting product packaging design based on internet of things

Dapeng Zhou, Miao Miao

DOI: 10.1504/IJIMS.2024.10059277

Article History:

Received:	27 February 2023
Last revised:	23 May 2023
Accepted:	07 July 2023
Published online:	19 February 2024

Research on cloud anti-counterfeiting product packaging design based on internet of things

Dapeng Zhou*

Department of Architectural Engineering,
Henan Polytechnic Institute,
Nan Yang, 473000, China
Email: zhoudadapeng@126.com
*Corresponding author

Miao Miao

Department of Economics and Trade,
Henan Polytechnic Institute,
Nan Yang, 473000, China
Email: 258685878@qq.com

Abstract: Aiming at the problems such as low security coefficient of security and large error of package generation in cloud security product packaging, the design method of cloud security product packaging based on the internet of things technology was studied. Firstly, the thumbnail of the cloud security watermark is formed after the image is downsampled according to the sampling theory. The security information is initially hidden by displacement transformation, and the cloud security encryption watermark is generated by combining with the NTRU algorithm. Finally, the internet of things (IoT) technology was introduced to design the backscatter modulation of cloud anti-counterfeiting wireless communication, and a package automatic generation system embedded with package cloud anti-counterfeiting code was constructed. The maximum likelihood estimation optimisation generation system was used to realise the package design of cloud anti-counterfeiting products. The experimental results show that the security factor of the proposed method is 0.99, the packaging generation error is less than 0.2%, and the time is less, so the method has higher application value.

Keywords: internet of things technology; IoT; cloud anti-counterfeiting products; packing design; NTRU algorithm; cloud anti-counterfeiting watermark.

Reference to this paper should be made as follows: Zhou, D. and Miao, M. (2024) 'Research on cloud anti-counterfeiting product packaging design based on internet of things', *Int. J. Internet Manufacturing and Services*, Vol. 10, No. 1, pp.60–76.

Biographical notes: Dapeng Zhou received his Master's in Designing from the Henan University in 2010. He is currently an Associate Professor in the Department of Architectural Engineering of Henan Polytechnic Institute. He has directed many educational projects concerning designing. He has published a lot of journal papers, treatises and patents in designing.

Miao Miao received her Master's in Administrative Management from the Zhengzhou University in 2015. Her research interests include administration, economics and trade. She has participated in many management-related projects. She is currently a teaching assistant in the Department of Economics and Trade of Henan Polytechnic Institute.

1 Introduction

The competition among various industries is becoming increasingly fierce with the continuous development of social economy. The appearance of fake and inferior products in the competition of economic development has seriously disturbed the fairness of social and economic competition (He et al., 2021). Counterfeit and shoddy products are infringement of intellectual property rights. Without authorisation, they counterfeit important features or quality marks of rival products. In the current context, fair competition and normal market order cannot be separated from the assistance of anti-counterfeiting packaging (Minh et al., 2021). Many high-tech anti-counterfeiting methods have emerged in the field of product packaging in order to reduce the counterfeiting of products with the development of electronic information technology. The emergence of these anti-counterfeiting methods effectively reduces the risk of products being counterfeited. However, in the constant change of market economic rules, there are also many constraints on the anti-counterfeiting of product packaging (Molina-Gonzalez et al., 2022), which leads to the failure of anti-counterfeiting of product packaging, seriously affecting the fair competition in the market, and these anti-counterfeiting labels do not play the role of safety protection, but increase the production cost of products (Ansari et al., 2022). For this reason, a variety of anti-counterfeiting packages with high security and low cost have been designed in the field of product packaging anti-counterfeiting. However, there are some limitations of anti-counterfeiting packaging at the present stage, such as the high error of packaging generation. Relevant scholars have analysed this problem and carried out research.

Wang et al. (2021) proposes a three-layer non-cloning anti-counterfeiting method through huge coding capacity algorithm and artificial intelligence authentication. This method constructs three layers of anti-counterfeiting, and the first layer is verified by portable smart phones. In the second security layer, the confocal Raman system can be used to visualise the non-cloned surface-enhanced Raman scattering (SERS) security signal at low magnification. In the third layer, the aggregated SERS signal under the high amplification Raman mapping generates an unrepeatable pattern with shape-specific information. Through further concrete application of artificial intelligence (AI), identification and authentication, anti-counterfeiting design is realised. The security coefficient of this method is high, but it takes a long time due to the complexity of the algorithm. Smith et al. (2021) proposes to use deep machine learning to quickly authenticate plasma anti-counterfeit labels with high coding ability. This method designs anti-counterfeit labels for counterfeit goods. Its high coding ability is designed into the label through the size of Au NP, which provides a series of colour responses, and uses deep machine learning to authenticate labels to allow high-precision and rapid matching of labels with specific products. In addition, the label contains descriptive metadata, which is used to match the label with a specific batch number to achieve anti-counterfeit

design. This method mainly considers the applied anti-counterfeiting materials, and takes the materials as the starting point, and better designs the anti-counterfeiting labels, but the anti-counterfeiting safety coefficient of this method in practical application is low. Lu et al. (2021) studies electrochromic and electrochromic dual-functional AIE polymers are used to simultaneously realise high capacity storage and multi-level anti-counterfeiting of product packaging design. Two kinds of electrochromic and electrochromic dual-functional polymers with aggregation induced emission (AIE) characteristics were prepared. After the voltage is applied, the absorption spectrum and fluorescence spectrum of AIE polymer can change reversibly, accompanied by changes in appearance colour and emission. A dual-mode display device was prepared by using a simple spray technology based on the controllable characteristics of the polymer. By adding colour change multiplexing to two-dimensional space, a four-dimensional colour coding device is constructed. In addition, the colour coding device can also be applied to multi-level anti-counterfeiting field. It can dynamically convert encrypted information under different voltages. This method effectively improves the speed of anti-counterfeiting, and its anti-counterfeiting generation takes a long time. The specific implementation needs further practice. Li (2023) proposes a laser digital holographic encryption password system for anti-counterfeiting marks on the outer packaging of products is constructed. According to the laser digital imaging method, the relationship architecture between the plaintext data and the key in the anti-counterfeiting information of the product packaging was established, and the pseudo-random sequence processing was carried out on the laser holographic image of the appearance map by using the ciphertext chaotic mapping method. The laser digital holographic digital encryption and coding model of the anti-counterfeiting identification of the product outer packaging was established to realise the anti-counterfeiting product packaging design. However, the astringency of this method will take a long time, resulting in poor practical application effect.

On the basis of the above research on product packaging security, this paper proposes to design a new research method of cloud security product packaging design based on the internet of things (IoT) technology in order to improve the security of cloud security product packaging design and solve the problems of low security factor of security product packaging, high packaging generation error and high design time. The design of cloud security product packaging is realised by introducing the IoT technology, and combining the displacement transformation and NTRU algorithm. It is expected to improve the security factor to more than 0.9, reduce the error to less than 1.0%, and reduce the time to less than 0.5s. The overall design scheme is as follows:

1 Cloud security watermark embedded in product packaging is generated. Considering the transparency of image quality after embedding watermark, the binary image is transformed into a thumbnail by image sampling transformation, and the watermark information is embedded on the thumbnail, so as to realise the flip of pixels on the thumbnail, and then the visual impact of the change of the whole image will be reduced. Then, the information is initially hidden by the shift transformation of pixel value points. In order to improve the security, the NTRU algorithm is introduced. The algorithm is used to optimise the cloud security, realise the generation of cloud security watermark, and lay a foundation for the embedding of cloud security watermark into product packaging.

2 Design and implement the packaging of cloud anti-counterfeiting products based on IoT technology. In order to embed the cloud security watermark into the package of

the cloud security product and realise the package design of the cloud security product, the IoT technology is introduced to construct the data input and output of the cloud security watermark information generated above through the radio frequency technology of the technology, that is, the backscatter modulation is designed, through the combination of the mixer (logic gate), IF signal and impedance switch, the wireless communication of the cloud security is realised. On this basis, the embedding process of cloud security product packaging security code label is constructed, and then the automatic generation system of cloud security packaging based on IoT technology is constructed. The maximum likelihood estimation method is introduced to optimise the generation system, and the automatic generation model of cloud security product packaging image is constructed to achieve the final cloud security design.

3 Experimental analysis. Design the experimental scheme, design the experimental parameters in the experimental scheme, determine the research object, and analyse the anti-counterfeiting safety coefficient, packaging generation error and time consumption index of the proposed method, Smith et al. (2021) method and Lu et al. (2021) method for 100 cloud anti-counterfeiting products.

4 Conclusion. Explain the purpose and method of the study, and explain the results and conclusions of the study.

2 Cloud anti-counterfeit watermark generation embedded in product packaging

A cloud anti-counterfeiting method with high security is required in order to avoid products being counterfeited in the packaging design of cloud anti-counterfeiting products. This paper mainly uses the form of embedding watermark (Zermi et al., 2021) to achieve the purpose of product cloud anti-counterfeiting. The embedded watermark is a binary image (Bose et al., 2022; Cao et al., 2021; Cruz, 2022; Zamani and Amini, 2020). Considering the transparency of the image quality after embedding the watermark, the binary image is transformed into a thumbnail through image sampling transformation, and the watermark information is embedded in the thumbnail, so that the pixel on the thumbnail can be flipped, and the impact of the change of the whole image on the vision will be reduced.

According to the sampling theory, the image thumbnail will be formed after the image is down-sampled, and the pixels will only shift without losing any pixels. Set and respectively set the horizontal sampling step and vertical sampling step, that is one pixel is took at every point in the horizontal direction and one pixel at every point in the vertical direction, so as to form a thumbnail of the original image. Define the original binary image as:

$$B = \{C(x, y) \mid 0 < x < d, 0 < y < e\} \tag{1}$$

where, (x, y) represents the pixel point coordinates, and $C(x, y)$ represents the pixel value point of (x, y).

Since the watermark in the cloud anti-counterfeiting uses a thumbnail map, so (x, y) should be sampled to the first (n, m) block of the thumbnail map B', then the mapping relationship between the two is:

$$n = (x-1)\%A_e + 1 \tag{2}$$

$$m = (x-1)\%A_d + 1 \tag{3}$$

After completing the thumbnail coordinate mapping, the coordinates within the cloud anti-counterfeiting watermark block are defined as (f, h), which is obtained through the original coordinates (x, y) as:

$$f = \left[\frac{x}{A_e}\right] \tag{4}$$

$$h = \left[\frac{y}{A_d}\right] \tag{5}$$

Together with the above formula, the coordinates of $C(x, y)$ are mapped to the cloud anti-counterfeiting watermark. The formula is:

$$x' = (n-1)\alpha + f \tag{6}$$

$$y' = (m-1)\beta + h \tag{7}$$

where α represents the height of the cloud anti-counterfeiting watermark block, and β represents the width of the cloud anti-counterfeiting watermark block. Then the pixel value corresponding to the coordinate is $C'(x', y')$.

After determining the coordinates in the product cloud anti-counterfeiting watermark, use the displacement transformation of the coordinates to hide the information, but the security of the hidden information only through the displacement transformation cannot achieve the expected goal, that is the security coefficient is not optimal. Therefore, after the displacement transformation of the pixel coordinates in the cloud anti-counterfeiting watermark, the NTRU algorithm (Camacho-Ruiz et al., 2021; Cho et al., 2020) is introduced. The highly encrypted hidden information can be achieved to achieve the anti-counterfeiting goal through the combination of the two algorithms. The specific information hiding steps of product cloud anti-counterfeiting are as follows:

Step 1 Determine the displacement length of the coordinate point. Set the point displacement in the cloud anti-counterfeiting watermark binary image is to (x'', y''). In order to anti-counterfeiting of the product cloud and avoid product counterfeiting, the length of the point displacement is:

$$G(x', y') = \sqrt{|x'' - x'|^2 + |y'' - y'|^2} \tag{8}$$

Step 2 After the displacement, determine the cloud anti-counterfeiting watermark information after the displacement, and the formula is:

$$C''(x', y') = C'(x', y') - \gamma G(x', y') \tag{9}$$

where γ represents the transformation coefficient.

Step 3 NTRU algorithm is introduced to encrypt the cloud anti-counterfeiting watermark after the displacement transformation to further improve the anti-counterfeiting effect. NTRU algorithm is based on polynomial encryption. Therefore, the polynomial is given, and the formula is:

$$J = \sum_{i=0}^{N} K_i C''(x', y') \tag{10}$$

Step 4 Convolution operation polynomial, the formula is:

$$L = J * Z \tag{11}$$

where Z is a binary polynomial formula is:

$$Z_i = \sum_{i=0}^{N} z_i = \left[z_0, z_1, \cdots z_N \right] \tag{12}$$

where z_0, $z_1 \cdots z_N$ represent the key corresponding to the information.

Step 5 Use the above polynomials to generate the public key of product cloud anti-counterfeiting. The formula is:

$$L' = J^{-1} * J * Z_i * S \tag{13}$$

where J^{-1} represents the inverse of the polynomial J, and S represents a positive integer.

Step 6 Randomly select a small coefficient polynomial Q as the blind polynomial, calculate the ciphertext, the formula is:

$$R = L' * Q + C''(x', y') \bmod \delta \tag{14}$$

where δ represents the large moduli number.

Step 7 After determining the ciphertext R, determine the decryption formula for product cloud anti-counterfeiting. The formula is:

$$U - J * R \bmod \delta \tag{15}$$

Step 8 After determining that the decoding cannot be performed, generate the cloud anti-counterfeit watermark that is finally embedded in the product package. The formula is:

$$O = R\left[\int L' \int L'' \right] \tag{16}$$

where L' represents the root of the polynomial.

So far, the cloud anti-counterfeiting watermark generation design embedded in the product packaging has been completed. The product cloud anti-counterfeiting information is mainly hidden in this process. The image is down-sampled according to the sampling theory to form a thumbnail of the image before hiding the information, and then the information is initially hidden through the displacement transformation of pixel value points. On this basis, the NTRU algorithm is introduced. Through the combination of algorithms, the security of the product cloud anti-counterfeiting is further improved; it

lays the foundation for embedding cloud anti-counterfeit watermark into product packaging.

3 Design and implementation of cloud anti-counterfeit product packaging based on IoT technology

In order to embed the anti-counterfeit code into the cloud anti-counterfeit product packaging and realise the cloud anti-counterfeit product packaging design after the above cloud anti-counterfeit product packaging anti-counterfeit code is generated, this paper introduces the IoT technology to achieve the final cloud anti-counterfeit design. The IoT technology appeared in the 1990s (Xu et al., 2022; Jiao et al., 2021; Fahmideh et al., 2021). In this technology, radio frequency technology and communication technology jointly cover all networks to realise mutual identification, information sharing and other functions between items. At present, this machine is mainly used by various sensor devices to realise its functions. It forms a huge network through sensor-based devices to facilitate the management of goods. This technology has the ability of comprehensive perception, realises the dynamic recognition of objects by means of sound and light points, and also has the ability of intelligent processing to realise the intelligent control of research objects. This paper introduces this technology to realise the packaging design of cloud anti-counterfeit products to improve the anti-counterfeit performance of cloud anti-counterfeit products because of the high potential of this technology. The three dimensional levels in the IoT technology can effectively solve various information security problems. The relationship between the three dimensional levels is shown in Figure 1.

In the packaging design of cloud anti-counterfeit products, the wireless radio frequency technology in the IoT technology is introduced to achieve anti-counterfeit design. Firstly, the input and output of anti-counterfeiting information are realised through the radio technology chip inside the technology. The communication control mode of the radio technology chip of IoT technology used in the packaging of cloud security products is backscatter modulation, and the backscatter modulation design is shown in Figure 2.

The communication control mode in Figure 2 is backscatter modulation. The backscatter modulation of the IoT technology designed in this paper controls the wireless communication of the wireless network through the impedance switch, that is, the input and output of anti-counterfeiting information. According to Figure 2, the principle of cloud anti-counterfeiting wireless communication of the IoT technology is that the cloud anti-counterfeiting data signal to be sent is a signal with two levels, which is modulated through a mixer (logic gate) and IF signal. The modulated cloud anti-counterfeiting signal is sent to the impedance switch, which changes the transmission coefficient of the antenna, thus completing the modulation of the carrier signal. Realise the wireless communication identification of the IoT. The chip size is small, attached to the cloud security product package security watermark, through the way of label security. The embedding process of the security watermark in the package of cloud security products is shown in Figure 3.

Figure 1 Schematic diagram of hierarchical relationship of three dimensions of IoT technology

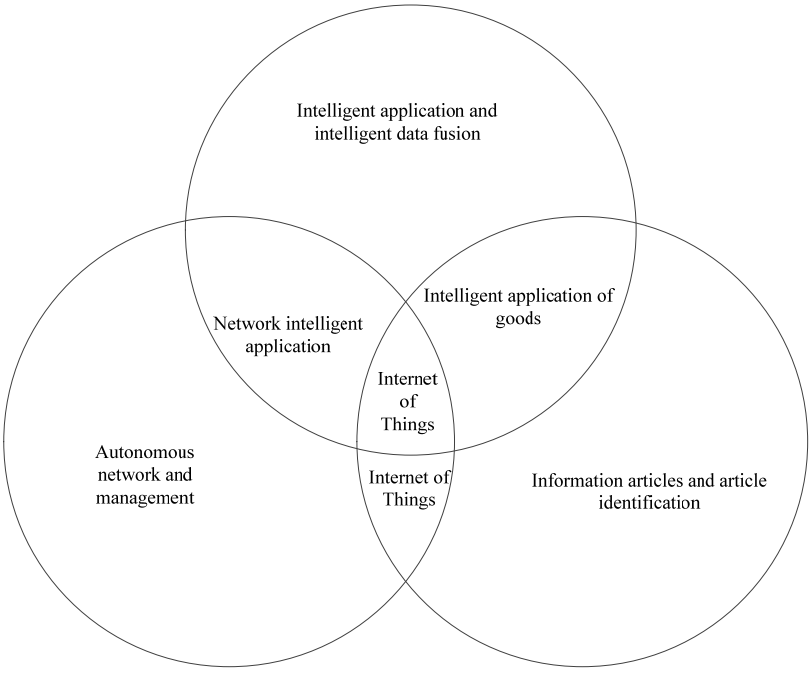
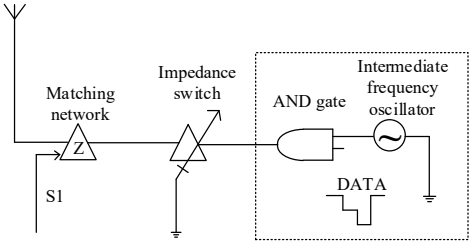


Figure 2 Backscatter modulation of IoT technology



According to the embedded watermark of cloud anti-counterfeit product packaging anti-counterfeit code, based on the IoT technology, a cloud anti-counterfeit product packaging automatic generation system is designed. The system module structure mainly includes cloud anti-counterfeit product packaging information acquisition module, packaging image automatic generation module and cloud anti-counterfeit product packaging automatic verification module. The overall structure of the system is shown in Figure 4.

In the design of the cloud anti-counterfeit product packaging automatic generation system, the main function of the cloud anti-counterfeit product packaging information collection module is to collect the image contour information and security information of the relevant cloud product packaging. Attention should be paid to the accuracy of the cloud anti-counterfeit product packaging information in the design of this module. The maximum likelihood estimation method (Robert et al., 2022) is used to locate the

coordinates of the cloud anti-counterfeit product in the module information collection, and the cloud anti-counterfeit encryption is performed through the above method, to improve security, the coordinate information corresponding to the anti-counterfeit watermark of its cloud product is:

$$C''(x', y') \leftarrow O \tag{17}$$

Figure 3 The embedding process of anti-counterfeiting code label in cloud anti-counterfeiting product packaging

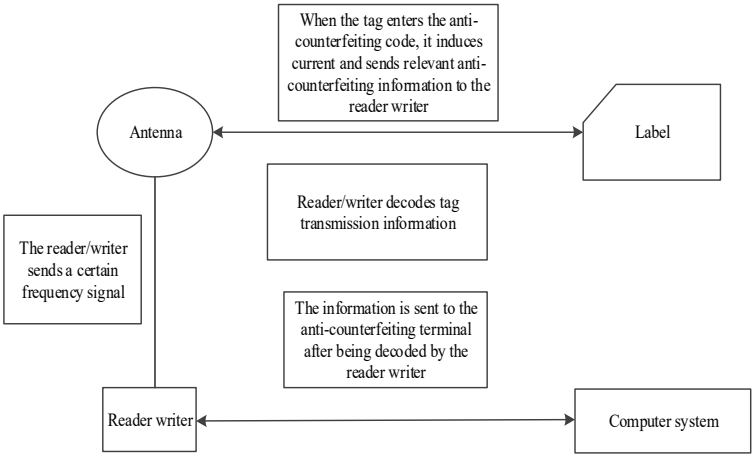


Figure 4 Basic composition of automatic generation system for cloud anti-counterfeit product packaging

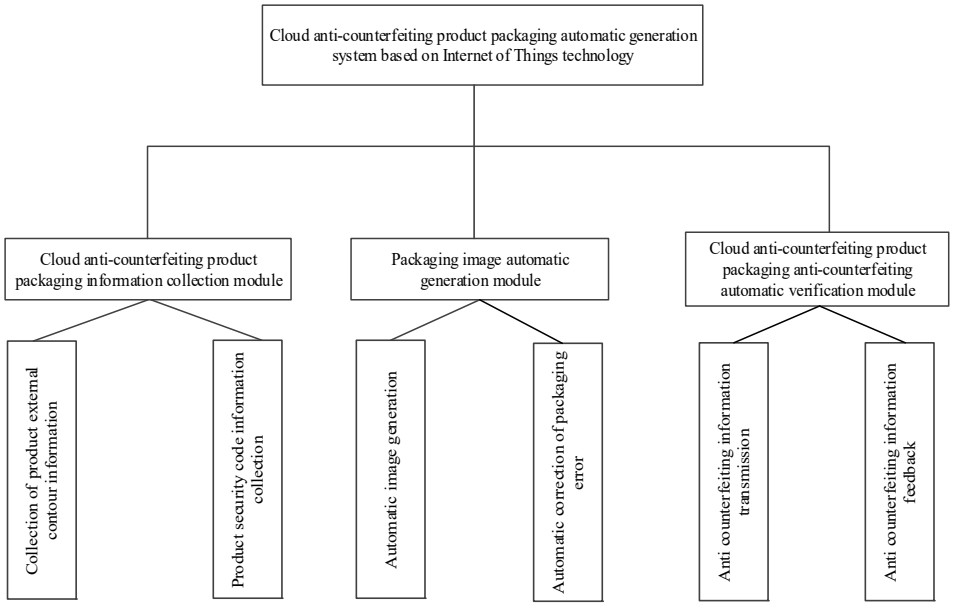
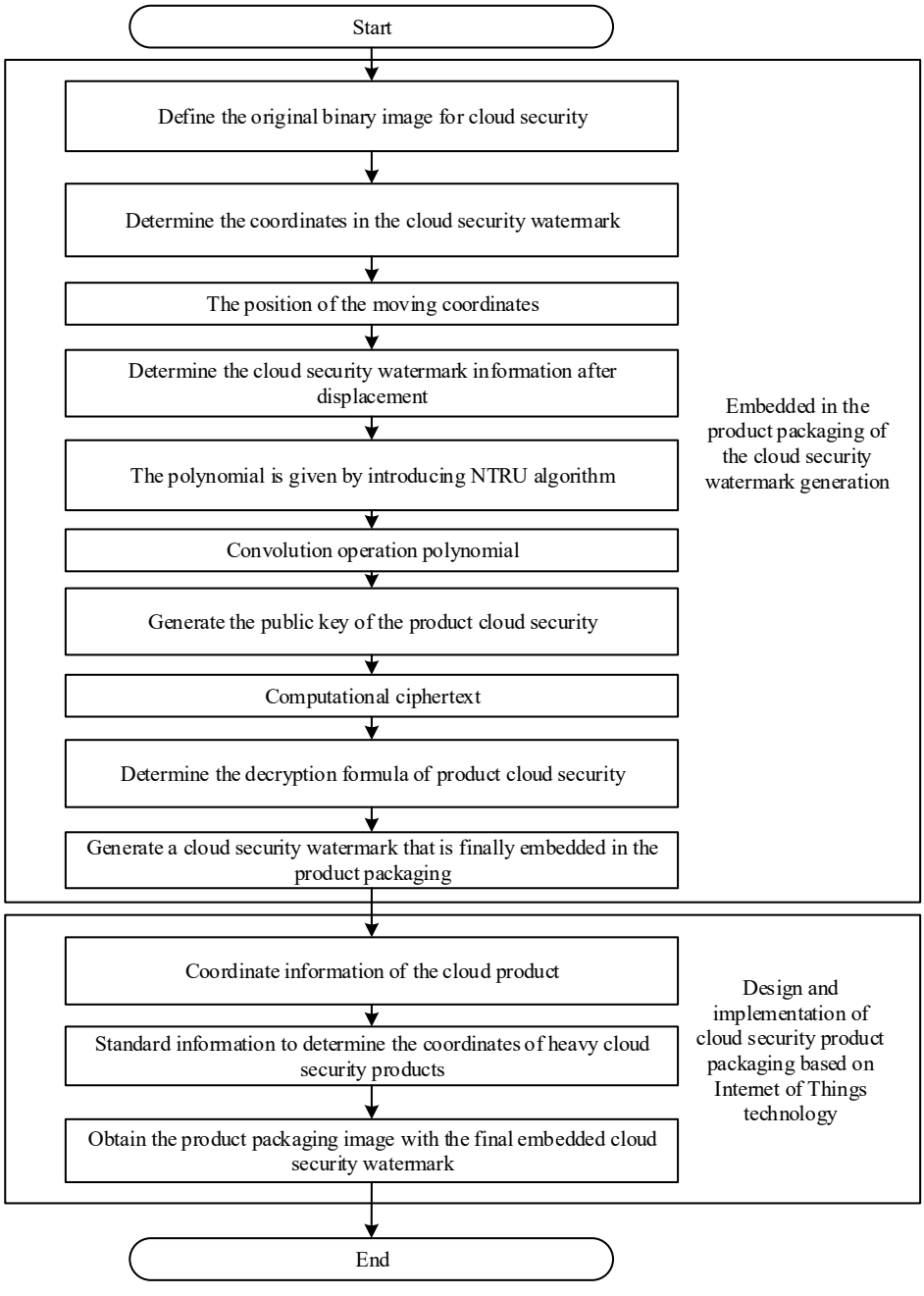


Figure 5 Cloud anti-counterfeit product packaging design process based on IoT technology



The minimum maximum likelihood estimate is used to determine the standard information of the watermark coordinates of the heavy cloud anti-counterfeiting product, and the results are as follows:

$$\breve{X} = \sum_{i=1}^{N} C''(x, y')P \tag{18}$$

where $\breve{X}$ represents the standard information for determining the watermark coordinates of heavy cloud anti-counterfeiting products, and P represents the minimum maximum likelihood estimate.

In the automatic generation module of packaging image and the automatic verification module of cloud anti-counterfeit product packaging, we should pay attention to the embedding and security verification of the above image cloud anti-counterfeit product watermark (Bilal et al., 2021). At this time, we can build an automatic generation model of cloud anti-counterfeit product packaging image, that is, the final embedded cloud
anti-counterfeit product packaging image, the formula is:

$$W = \breve{X} \frac{Y}{\sqrt{2(1 - COS\vartheta)}} v_i \tag{19}$$

where W represents the automatic generation model description of the cloud anti-counterfeiting product packaging image, Y represents the anti-counterfeiting calibration coefficient, and v_i expresses the security coefficient after the automatic generation of the packaging.

The cloud anti-counterfeit product packaging design has been completed based on this. The specific flow of the cloud anti-counterfeit product packaging design method based on the IoT technology is shown in Figure 5.

Thus complete the packaging design of cloud security products based on the IoT technology. In the packaging design of cloud security products, as the current anti-counterfeiting method, this method introduces the IoT technology. Through the radio frequency technology of this technology, the wireless communication mode of cloud security watermark information is designed, that is, the backscatter modulation is designed. In this method, maximum likelihood estimation is introduced after the initial hiding of security information through displacement. The algorithm is used to further encrypt the cloud security watermark that needs to be embedded in the product package, so as to improve the security. After completing the design of embedded cloud security watermark, the generated cloud security watermark is embedded into the product package through the technology combined with the IoT technology, so that it has higher security performance, easy to implement and simple algorithm.

4 Experimental analysis

4.1 Experimental scheme design

One hundred cloud anti-counterfeiting products of a company in the current quarter were selected as the research objects, and the cloud anti-counterfeiting product packaging design was carried out for these research objects in the experimental test. Table 1 shows the basic information of the package of cloud security products.

The packaging automatic generation system in the test is designed with relevant software based on the existing hardware system support. The whole experiment is implemented in the MATLAB platform, and the selected radio frequency equipment

conforms to the analysis of this experiment. The experimental parameters of the specific study are shown in Table 2.

Table 1 Basic package information of cloud anti-counterfeiting products

Item contained in the product package	*Specific content*
Certificate of qualification	Display the inspection certificate on the package
Product name, factory name and factory address	Product name, factory name and factory address indicated in Chinese. Imported products for sale in the domestic market must bear signs in Chinese.
Product specification, grade	According to the characteristics and application requirements of the products, the specifications and grades of the products shall be indicated, and the names and contents of the main ingredients in the products shall also be indicated.
Products for limited use	Production date, shelf life or shelf life should be indicated in an obvious place.
Mark	A registered trademark that has been approved by the Department of Industry and commerce, marked 'R' or 'Note'.
Warning note	For products that are likely to cause damage to the product itself or may endanger the safety of human life and property, there should be warning signs or warning instructions in Chinese.
Other terms	The manufacturer shall indicate the code name, serial number and name of the standard implemented on the product or its description and package.

Table 2 Design of experimental parameters

Parameter	*Data*
Automatically generate system protocol mode	UDP
Data transmission volume of IoT/s/piece	1,000
Automatic generation of system support network	Compatible
Anti-counterfeit code/block	1,000
Product packaging image pixel/dpi	1,024*1,098
Radio frequency operating frequency/Ghz	3.4
Generation error/%	< 1
Test iterations/time	100

On the basis of the set parameters, the mode of comparing the proposed method, the Smith et al. (2021) method and the Lu et al. (2021) method was selected for the test.

4.2 Experimental performance specifications

In order to effectively analyse the performance of the method, the experimental indexes were selected as security factor of anti-counterfeiting, automatic packaging generation error and automatic packaging generation time. In the experimental test, 100 kinds of cloud anti-counterfeiting products are taken as the research object, and different

experimental indexes are tested respectively. Among them, the formula for calculating the security factor of anti-counterfeiting is:

$$P = \frac{P_0}{P_1} \tag{20}$$

where P_0 represents security performance and P_1 represents actual threat.

The urgent formula for calculating the error generated automatically by packaging is:

$$P = \frac{\sum_e^E |K_0 - K_e|}{E} \tag{21}$$

where K_0 represents the actual value, K_e represents the generated value, and E represents the number of samples.

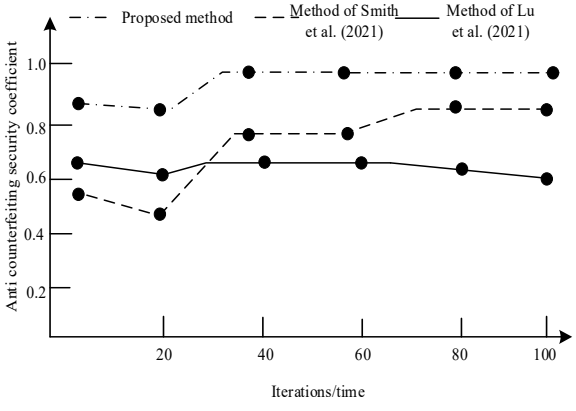
Packaging automatically generates time-consuming statistics through the computer that comes with house arrest.

The higher the value of the security factor of the three experimental performance indicators, the higher the security of the method, the lower the value of the automatic packaging generation error and the time of automatic packaging generation, the more accurate the package of the cloud security product generated by the method, and the higher the effect.

4.3 Analysis of experimental results

The anti-counterfeiting safety coefficient of the proposed method, Smith et al. (2021) method and Lu et al. (2021) method for 100 cloud anti-counterfeiting products was analysed in the test. This index reflects the anti-counterfeiting safety of the product packaging, and is a key indicator of property rights and economy to protect enterprise children. The value range of this index is between [0, 1]. The closer the value is, the better the anti-counterfeiting safety is. The results after comparison are shown in Figure 6.

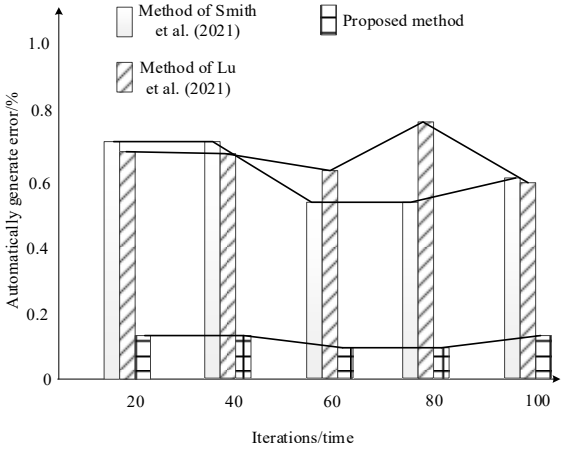
Figure 6 Analysis of security coefficient results of cloud anti-counterfeiting products with different methods



It can be seen that the proposed method, the Smith et al. (2021) method and the Lu et al. (2021) method have certain differences in the anti-counterfeiting security coefficients of 100 cloud anti-counterfeiting products by analysing the experimental results in Figure 6. Among them, the maximum anti-counterfeiting safety coefficient of the proposed method is about 0.99, and the maximum anti-counterfeiting safety coefficient of the Smith et al. (2021) method and Lu et al. method are about 0.81 and 0.61, respectively. From the data analysis, it can be seen that the proposed method has the best anti-counterfeiting security coefficient for 100 cloud anti-counterfeiting products, which verifies the reliability of the proposed method. This is because the method in this paper, based on the traditional method, transforms the cloud security binary image into a thumbnail through image sampling transformation, and imparts watermark information on the thumbnail, so as to realise the flip of pixels on the thumbnail, and thus reduce the visual impact of the change of the whole image. In addition, NTRU algorithm is introduced to optimise the cloud security watermark. Thus improving the security factor of cloud anti-counterfeiting products and increasing security.

The error of the proposed method, Smith et al. (2021) method and Lu et al. (2021) method on the automatic generation of 100 cloud anti-counterfeiting product packages was analysed in the test. The error was mainly determined from the edge of the package and the embedding of the package anti-counterfeiting code label. The results are shown in Figure 7.

Figure 7 Error analysis of cloud anti-counterfeit product packaging (see online version for colours)



By analysing the experimental results in Figure 7, it can be seen that the proposed method, the Smith et al. (2021) method and the Lu et al. (2021) method have certain differences in the error generated by the packaging of 100 cloud anti-counterfeiting products. With the continuous change of iteration times, the error generated by the three methods on the packaging of 100 cloud anti-counterfeiting products fluctuated to a certain extent, and the error volatility of the proposed method showed a downward trend, and was lower than 0.2%, while the generation error of the other two methods was higher, always higher than the proposed method, The error of the proposed method is more than 0.4% lower than that of the literature method. So we can see the feasibility of

the proposed method. This is because the proposed method introduces the IoT technology to design the package of cloud security products, and at the same time introduces the maximum likelihood estimation algorithm, through which the cloud security watermark that needs to be embedded in the product package is further encrypted and the generation error is reduced.

In the test, the proposed method, Smith et al. (2021) method and Lu et al. (2021) method were analysed to analyse the time consumption of automatic generation of 100 cloud anti-counterfeiting products packaging, and the results are shown in Table 3.

Table 3 Analysis of time-consuming results of automatic generation of cloud anti-counterfeiting product packaging (s)

Generation times/time	*Proposed method*	*Smith et al. (2021) method*	*Lu et al. (2021) method*
10	0.11	0.22	0.30
20	0.12	0.24	0.31
30	0.13	0.27	0.32
40	0.13	0.30	0.36
50	0.15	0.31	0.38
60	0.15	0.32	0.39
70	0.15	0.33	0.40
80	0.16	0.36	0.43
90	0.17	0.38	0.45
100	0.17	0.41	0.47

By analysing the experimental data in Table 3, it can be seen that the time consumption of the proposed method, Smith et al. (2021) method and Lu et al. (2021) method for automatic generation of 100 cloud anti-counterfeiting products packaging changes with the number of experiments. When the number of iterations is 50, the proposed method, Smith et al. (2021) method and Lu et al. (2021) method take about 0.15 s, 0.31 s and 0.38 s to automatically generate the packaging of 100 cloud anti-counterfeiting products, respectively; When the number of iterations is 100, the proposed method, Smith et al. (2021) method and Lu et al. (2021) method take about 0.17 s, 0.41 s and 0.47 s to automatically generate the packaging of 100 cloud anti-counterfeiting products, respectively; From the data results, we can see that the proposed method takes less time, which can verify that the proposed method is more effective. This is because the cloud security watermark generation algorithm embedded in product packaging introduced by the proposed method and the cloud security product packaging design algorithm of the IoT technology are relatively simple, and the cloud security watermark is shortened, so it effectively reduces the time of automatic generation of the cloud security product packaging.

5 Conclusions

The security of cloud anti-counterfeit product packaging design is related to the competitive advantage of enterprises. There are many problems in its product packaging

design, such as large error in automatic packaging generation and long time consuming. A cloud anti-counterfeit product packaging design method based on IoT technology is designed.

1 In this method, the thumbnail is constructed, the displacement is transformed, and the NTRU algorithm is combined to hide the security product information and generate the cloud security watermark embedded in the product package. By introducing the radio frequency technology in the IoT technology, the wireless communication mode of the cloud security watermark information is designed, that is, the backscatter modulation is designed, and then the cloud security product package security code watermark is embedded. An automatic generation system based on the package information acquisition module of cloud security products, the automatic generation module of package image and the automatic verification module of package security of cloud security products was constructed. The coordinates of cloud security products were located and the model was automatically generated by the maximum likelihood estimation method to realise the package design of cloud security products.

2 This method has achieved a good performance in the security coefficient of cloud security products, with the highest security coefficient of about 0.99, while the highest security coefficient of the literature method is only 0.81. Compared with different methods, it can be seen that the security coefficient of the proposed method is increased by more than 0.18, which verifies that the cloud security product packaging designed in this paper has higher security performance.

3 The proposed method also designs the generation of cloud security product packaging. Therefore, the error of automatic generation of cloud security product packaging is analysed through experiments. The generation error of this method is less than 0.2%, which is more than 0.4% lower than that of the literature method, and the reliability of the proposed method is verified.

4 In order to further verify the application performance of the proposed method, the automatic generation time of cloud security product packaging is analysed. The maximum generation time of this method is only 0.17 s, while that of the literature method is 0.41 s and 0.47 s respectively. Comparing the generation time of the proposed method, it can be seen that the generation time of the proposed method is reduced by more than 0.24 s, indicating that the method has the shortest time. Enhance the speed of cloud anti-counterfeiting product design.

References

Ansari, A., Aldajani, K., Alhazaa, A. and Albrithen, H.A.A. (2022) 'Recent progress of fluorescent materials for fingermarks detection in forensic science and anti-counterfeiting', *Coordination Chemistry Reviews*, Vol. 462, No. 6, pp.1–40.

Bilal, M., Wu, M. and Li, Q. (2021) 'Multi-label active learning from crowds for secure IIoT', *Ad Hoc Networks*, Vol. 121, No. 10, pp.1–9.

Bose, S.K., Singla, D. and Basu, A. (2022) 'A 51.3-TOPS/W, 134.4-GOPS in-memory binary image filtering in 65-nm CMOS', *IEEE Journal of Solid-State Circuits*, Vol. 57, No. 1, pp.323–335.

Camacho-Ruiz, E., Sanchez-Solano, S. et al. (2021) 'Timing-optimized hardware implementation to accelerate polynomial multiplication in the NTRU algorithm', *ACM Journal on Emerging Technologies in Computing Systems (JETC)*, Vol. 17, No. 3, pp.1–16.

Cao, Y., Tang, L., Jin, R., Li, J.Q., Wang, J., Dong, Z.G. (2021) 'Grayscale image for broadband linear polarization measurement by ultracompact metasurface', *Optics Letters*, Vol. 46, No. 5, pp.1117–1120.

Cho, G.H., Lim, S. and Lee, H.S. (2020) 'Algorithms for the generalized NTRU equations and their storage analysis', *Fundamenta Informaticae*, Vol. 177, No. 2, pp.115–139.

Cruz, M.L. (2022) 'Enhancement of grayscale image display with amplitude Fourier holograms, employing a limited bandwidth phase', *Applied Optics*, Vol. 61, No. 19, pp.5657–5665.

Fahmideh, M., Ahmed, A., Behnaz, A., Grundy, J. and Susilo, W. (2021) 'Software engineering for internet of things: the practitioner's perspective', *IEEE Transactions on Software Engineering*, Vol. 21, No. 9, pp.1–11.

He, X., Li, H., Wang, J., Li, Y. and Xu, Z (2021) 'Tunable dual-mode MOF-based composite fluorescent materials: stimuli-responsive and anti-counterfeiting application', *Crystal Growth & Design*, Vol. 21, No. 3, pp.1625–1635.

Jiao, J., Wu, S., Lu, R. and Zhang, Q. (2021) 'Massive access in space-based internet of things: challenges, opportunities, and future directions', *IEEE Wireless Communications*, Vol. 28, No. 5, pp.118–125.

Li, X.Q. (2023) 'Anti-counterfeiting logo design of product outer packaging based on laser digital holographic technology', *Laser Journal*, Vol. 44, No. 3, pp.247–251.

Lu, L., Wang, K., Wu, H., Qin, A. and Tang, B.Z. (2021) 'Simultaneously achieving high capacity storage and multilevel anti-counterfeiting using electrochromic and electrofluorochromic dual-functional AIE polymers', *Chem. Sci.*, Vol. 12, No. 20, pp.7058–7065.

Minh, N.H., Kim, K., Kang, D.H., Yoo, Y.E. and Yoon, J.S. (2021) 'Fabrication of robust and reusable mold with nanostructures and its application to anti-counterfeiting surfaces based on structural colors', *Nanotechnology*, Vol. 32, No. 49, pp.495302–495311.

Molina-Gonzalez, J., Ramirez-Garcia, G., Desirena, H. and Meza, O. (2022) 'Anti-counterfeiting strategy based on multiwavelength photothermal particles to disclose thermal imaging', *Ceramics International*, Vol. 48, No. 7, pp.9075–9082.

Robert, G., Dubois, V. and Legrand, P. (2022) 'Using maximum likelihood estimation approach to adjust parameters of multiphase equations of state: molybdenum as an example', *Journal of Applied Physics*, Vol. 131, No. 10, pp.1–12.

Smith, J.D., Reza, M.A., Smith, N.L., Gu, J. and Skrabalak, S.E. (2021) 'Plasmonic anticounterfeit tags with high encoding capacity rapidly authenticated with deep machine learning', *ACS Nano*, Vol. 15, No. 2, pp.2901–2910.

Wang, J.Y., Zhang, Q., Chen, R.Z., Li, J., Wang, J.H., Hu, G.Y., Cui, M.Y., Jiang, X., Song, B. and Yao, H. (2021) 'Triple-layer unclonable anti-counterfeiting enabled by huge-encoding capacity algorithm and artificial intelligence authentication', *Nano Today*, Vol. 41, No. 9, pp.1–9.

Xu, W., Zhang, J., Huang, S., Luo, C. and Li, W. (2022) 'Key generation for internet of things: a contemporary survey', *ACM Computing Surveys*, Vol. 54, No. 1, pp.14.1–14.37.

Zamani, H. and Amini, A. (2020) 'Ellipse recovery from blurred binary images', *IEEE Transactions on Image Processing*, Vol. 7, No. 1, pp.2697–2707.

Zermi, N.N., Amine, K., Redouane, K. et al. (2021) 'A DWT-SVD based robust digital watermarking for medical image security', *Forensic Science International*, Vol. 320, No. 7, pp.1–9.