METHODS AND TECHNOLOGIES FOR PROTECTING PHARMACEUTICAL PRODUCTS IN POLYMER PACKAGING FROM COUNTERFEITING

Chistyakova T. B[1], Makaruk R. V[1], Sadykov I. A[2] and Kohlert C[3]

Abstract—**This article considers the problem of protecting pharmaceutical products with polymer packaging from counterfeiting. This issue has grown vital in almost the entire world, as the significant harm can come not only to the producer, but the legitimate producer, but the consumers as well. Due to this, the issue of protecting these products against forgery, and creating and improving existing approaches to anti-forgery protection, becomes a crucial one. The authors suggest methods and technologies for protecting pharmaceutical products' polymer packaging based on modern ideas from IT and manufacturing such as image recognition, client-server software architecture, mobile apps, digital signatures, luminophores, and PVC film. Testing the authors' approach showed the effectiveness of the presented methods and technologies. The results should be of interest to companies producing pharmaceuticals.**

Keywords—pharmaceutical products; polymer packaging; counterfeiting; protection against forgery; image recognition; hardware-software solution; encryption; identification

I. INTRODUCTION

At present, the volume of counterfeit production in certain industries is comparable to the volume of legitimate production. This problem is prevalent in practically every field of economic activity, including pharmaceutical production. Counterfeit medicine make up 10 to 80% of the overall pharmaceutical sales in Russia, which provides the counterfeiters with annual income of approximately 7 billion dollars. Worldwide, counterfeit medicine sales amount to 600 billion U.S. dollars. Counterfeiting has become a major social issue, not just because such products cause the legitimate producers loss of trust and income, but also because counterfeit pharmaceuticals can lead to severe health issues, and even death [1-5].

Traditional anti-counterfeiting methods such as holograms, radiofrequency identifiers, etc., have a number of drawbacks and can only be applied to finished products, which is inadequate for pharmaceuticals, for example, as only the packaging itself could be protected. Furthermore, an analysis of the methods used currently shows that an analysis of the methods used currently shows that increasing the protection's effectiveness can only be accomplished with non-deterministic algorithms based on randomness, as this increases the probability that the security features will not be fully reproduced. The currently existing protection methods utilizing magnetic bits and metallic nanoparticles resolve this issue, however are extremely expensive. Further, any protection method used for food or medical products must avoid making the packaging toxic. An additional issue is that there is no full software-hardware solution that takes into account the peculiarities of pharmaceutical production, the production volume of which is in the billions [1, 6].

Thus, developing a software package of methods, models, and forms of counterfeit protection for polymer packaging of pharmaceutical products produced in large quantities, as well as a computer system that enables encryption and identifying packaging, is financially justified.

II. PROBLEM DEFINITION

An overview of the anti-counterfeiting systems on the market shows us that the field is actively developing. Among the existing systems, there are some that address the flaws of the traditional protection methods, however they have their own issues, such as needing to label each package with a unique mark. Table 1 [7, 8] shows the compared characteristics of several systems currently on the market. None of the available technologies are adequate for full protection of pharmaceutical packages, as the production volumes of pharmaceutical products greatly complicate any attempt to mark every single one (due to production costs). Furthermore, pharmaceutical packaging may become deformed during use (for example, when a customer pops a tablet out of its packaging), which makes sticker untenable for the task as well.

[1]Department of computer-aided design and control, Saint-Petersburg State Institute of Technology, Saint-Petersburg, Russian Federation, chistb@mail.ru
[2]Engineering-Server Atlassian, Sydney, Australia, smecsia@gmail.com
[3]Department of Process Technology, Klöckner Pentaplast Europe GmbH & Co.KG, Montabaur, Germany , c.kohlert@kpfilms.com

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

TABLE I. RELATIVE CHARACTERISTICS OF COUNTERFEIT PROTECTION SYSTEMS

System	Encryption: technology and label element	Identification: reading the label	Protection level
Tesa scribos	Special stickers. Several levels of protection. Labeling equipment.	Special equipment, a closed system.	High
ForgeGuard	Special non-unique labels. Single protection level.	Special scanning equipment.	Low
RFID (various systems)	A label with an antenna and chip. One invisible protection level. Special equipment.	Special readers. A closed system.	High

Having analyzed the existing anti-counterfeiting systems, we can ascertain the necessary characteristics of our anti-counterfeiting protection method software package. A generalized functional scheme of the anti-counterfeiting protection method package is presented in figure 1, where the following notation is used: Z_i – a package's digital signature; F_i – identification result output parameter vector; V_i – the vector of configurable parameters of the deformable package area coordinate assessment; R_i – 3-point circumscribed circle radius, in pixels; I – encryption picture in either ".jpg" or ".bmp" format; X_i – encoding input parameter vector.

The proposed process for product protection consists of several steps:

- Labeling the product with a unique code;
- Entering this code into a registry of legitimate codes;
- Testing product legitimacy by scanning this code;
- Searching for the scanned code in the legitimate code database.

The first two steps together make up the "encryption" stage. At that stage, the unique package code is entered into the legitimate code registry. The remaining steps are merged into the "identification" stage. The product package is identified by looking up its code in the registry of legitimate codes.

The created anti-counterfeiting system satisfies the following requirements:

- It uses protection elements that are not labels and can not be detected with the naked;

- It uses a unique code for each separate package, one based on an element of randomness in order to prevent its reconstruction;

- It can encode a large number of products (up to a billion per product type a year);

- It can identify a product sample within reasonable time (no more than a minute);

- It can partially identify the product (within the input error range) should the product's packaging become deformed;

- It allows for encryption and identification parameters to be reconfigured to suit the customer's requirements;

Keeping in mind the overall functional scheme of the anti-counterfeiting method software package as well as the specifics of the subject area, the developed software package consists of the following elements:

- The encryption subsystem, which consists of package scanning(photo) equipment as well as the software, which takes the digital photo and uses the user-specified configuration and unique code creation algorithm to calculate that code and send it to the server to be stored in legitimate code registry;

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

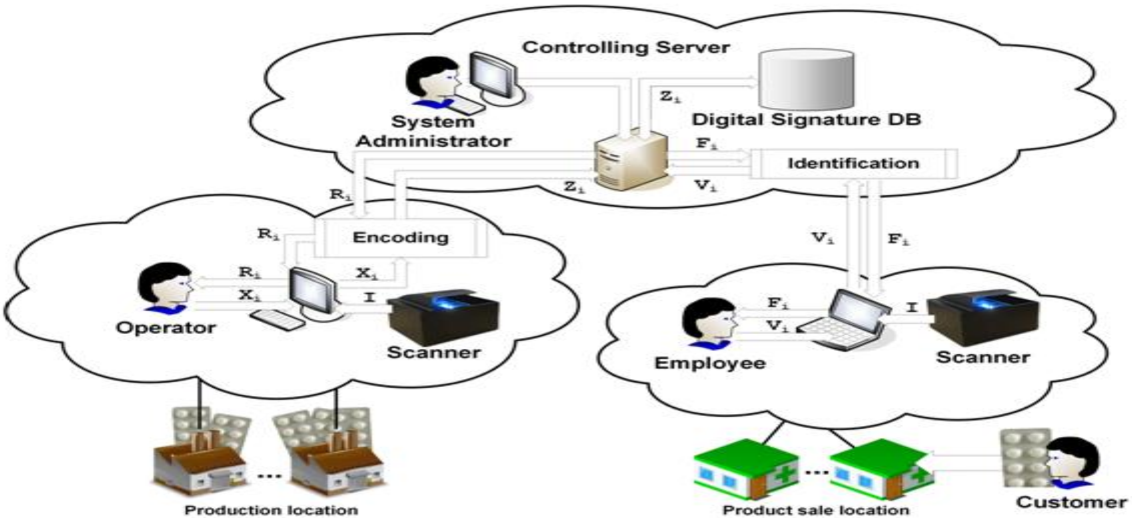

Fig. 1. Software package overall architecture.

- The identification subsystem, which consists of package scanning(photo) equipment (it's possible to use a smartphone for this provided it has the appropriate app installed), as well as software that can get take the digital photo and, using user-specified configuration and code formation selection, produce the unique code for that package and send it to the server to verify its presence in the legitimate code registry.

The server component, which consists of a database containing information regarding products that the software produces codes for, the registry of valid codes, as well as a component that can enter valid codes into the registry or verify code presence therein.

- In order to implement the developed methods and technologies for forgery protection, a two-layer package protection method is proposed according to which, the polymer film the packaging is made of contains randomly spread out luminophore particles that cannot be seen with the bare eye. Activating these particles requires ultraviolet or infrared light, or smartphone camera flash. The cost of creating such protection elements is less than .01 cents/square meter, and the luminophore content in the resulting polymer film is only 0.001%, which corresponds approximately to 1-5 pigment particles per square centimeter of film [6, 9, 10]. The luminophores found to be most appropriate to the task are photoluminophores. This is due primarily to the composition of the substances, as well as the simpler and more universal excitation method for this type of luminophore.

III. Polymer Packaging Encryption

The photo encryption process depends on such parameters as the encryptable object (polymer film or credit card), selected encryption element (As of right now, the software package permits one of three elemts – a triangle, a circle, and a rectangle), diameter of the applied particle (in microns), and the permitted encryption variance.

The first step of the encryption is image recognition, i.e. selecting the *n* brightest areas from the set and presenting them as points on the packaging material surface. Then, out of those *n*, *k* (the size of the hash) points are randomly selected. The size of the hash, just as the encryption method, can be configured by the manufacturer depending on production volumes, product protection level demands, and scanning equipment resolution. In the second encryption step, a set of points *n* is analyzed and separated into subsets. It is important to note that during normal product use by the customer (for example, when taking tablets out of their blister packs), the luminophore micro particles can shift from their initial position, which complicates identification. In order to prevent deformation from blocking packaging identification, it is necessary to discard points in damaged areas S_{def} from consideration [1, 9, 10].

The total number of points n_i, recognized on the *i*-th package is formed randomly and depends on the number of luminophore particles distributed on its surface.:

$$n_i = k + l + m_i + o_i, \qquad (1)$$

where $3 < l < k$; $m_i < n_i$; $k \leq n_i - m_i$; n_i is the total number of points on the packaging; m_i is the number of points within deformed areas; k is the number of bright points; l is the number of points used during encryption; o_i is the number of remaining points.

Thus, polymer packaging encryption occurs in three steps:

1. An operator gets a vector of deformed areas *O* based on image parameters by overlaying a mask in the form of

geometric primitives J as vectors on the deformed areas S_{def} and removes them from the packaging surface image S_{pack}.

2. Based on the encoding parameters X_i, a geometric code of the polymer packing Y_i is formed, taking into account the deletion of the deformable packing regions O.

3. A digital signature Z_i formed based on the polymer package geometric code Y_i, and encoded packaging characteristics G_i is created. It ensures code uniqueness when encrypting the i-th package, for $i = 1...N$ (N is packaging production volume, its volume is calculated in billions).

IV. Identifying Polymer

In order to check the legitimacy of the packaging (perform identification), image recognition of elements in geometric alignments must occur once more, followed by a search for the created digital signature in the database so as to assess the product type and check for counterfeiting. During identification, the input is the processed package image, the brightest points k, the amount of them, and a randomly selected set l of points from k which is used to calculate the digital signature. The complexity of the digital signature depends directly on their amount. For example, for the triangle method of encryption, if l = 4, then the number of triangles is equal 4. At l = 5, the number of triangles is already 10, and at 6 points it becomes 20. Accordingly, the number of attributes making up the digital signature is twice the amount of triangles [1, 9, 10].

Packaging identification occurs in 2 stages. The first stage is verifying a full match for the digital signature based on l points. The second is iteration over all combinations of points from k with l and comparison of the geometric element attribute values r_j that were created based on p-th combination of points with the values $r_{cp,j}$ from the legitimate digital signature DB:

$$\forall r_{p,j} : \left| r_{c\,p,j} - r_{p,j} \right| \le \mu,\ p = 1..Q_{\max\,\text{full}},\ j = 1..N_l \qquad (2)$$

Where N_l is the number of attributes to be saved that together make up the digital signature; $Q_{max\ full}$ is the maximum number of checks permitted to be done at the first identification stage; μ is the maximum permitted geometric element (triangle, circle) attribute variance compared to the saved values (in degrees, pixels, and square pixels).

If at least one match of the locally created digital signatures and the information stored on the database occurs, the package is confirmed as legitimate. The maximum number of checks at the first stage equal:

$$Q_{\max\,\text{full}} = C_k^l = \frac{k!}{l!(k-l)!},\ N_l = f(\mathrm{M_i}) \qquad (3)$$

where M_i is the package encryption method.

Should the first step finish without a match, an attempt to find a partial digital signature match using l-1 points is made:

$$\forall r_{p,j} : \left| r_{c\,p,j} - r_{p,j} \right| \le \mu,\ p = 1..Q_{\max\,\text{part}},\ j = 1..N_{l-1} \qquad (4)$$

where $Q_{max\ part}$ is the maximum number of checks at the second identification step; N_{l-1} is the number of saved digital signature attributes when building geometric elements using l-1 points.

The maximum number of checks at this step equals:

$$Q_{\max\,\text{part}} = C_k^{l-1} = \frac{k!}{(l-1)!(k-l+1)!},\ N_{l-1} = f(\mathrm{M_i}), \qquad (5)$$

If a partial match is found between at least one of the partial digital signatures and one digital signature stored in the database, the packaging is accepted as legitimate, though the user gets a warning about possible package deformation. The package is confirmed to be counterfeit if neither the first nor the second identification step produce a match [1, 6, 9, 10].

V. Polymer Film Encryption And Identification Algorithms

The input parameters for the encryption algorithms are the coordinates of the selected bright spots in the photos. The algorithm output is parameters of the resulting geometric elements. The main requirement for an encryption algorithm is consistency (a set of points will produce the same output unless the points are changed). The reason for its primacy being that orientation is not controlled during the polymer film photographing, and can be different during encryption and identification. However, the same points are recognized in both pictures, and their relative positions remain unchanged, though their coordinates may. As a result, the point processing algorithm was created in such a way that any point set orientation on a plane will produce the same parameters.

In order to keep the encoding system general, a library of encryption methods that uses various geometric models has been developed. Creation of these geometric models uses l random points from an array B_k of the k brightest points. Each method is characterized by r geometric models based on which the digital signature (Z) is created. The checksum of the digital signature A is a number calculated for each set of geometric models, and depends on the encryption method used:

- Using triangle edges, it saves the two minimal angles $r_j = \{a_{j1}, a_{j2}\}$ of each j-th triangle for $j = 1 \ldots u$; The overall number of attributes saved is expressed using the formula:

$$N_l = u \cdot 2 = C_l^3 \cdot 2 = \frac{l!}{3 \cdot (l-3)!} \qquad (6)$$

The checksum of the j-th packaging's digital signature is calculated according to the:

$$A_i = \sum_{j}^{n} (a_{j_{\text{med}}} + a_{j_{\min}}),\ n = u = \frac{N_l}{2},\ i = 1..N, \qquad (7)$$

Where a_{jmed} and a_{jmin} are the average and minimal values for the edges of the j-th triangle

- Using the radii of the circumscribed circles, we save the $r_j = R_j$ of each j-th circle for $j = 1 \ldots N_l$. The overall number of attributes saved is expressed using the formula:

$$N_l = u = C_l^3 = \frac{l!}{6 \cdot (l-3)!} \qquad (8)$$

The checksum of the i-th package's digital signature is calculated according to the formula:

$$A_i = \sum_{j=1}^{n} R_j \cdot (n - j + 1) - R_n,\ n = u = N_l,\ i = 1..N, \qquad (9)$$

where R_j is the radius of the j-th circle.

- Using the area of the triangles we made with triangulation preserves the areas $r_j = S_j$ of each j-th triangle for $j = 1 \ldots N_l$. The overall number of attributes saved is expressed using the formula:

$$N_l = u = l + l_{\text{int}} - 2,\ j = 1..N_l, \qquad (10)$$

where l_{int} is the number of points internal to the triangle.
The digital signature checksum is calculated according to the formula:

$$A_i = \sum_{j=1}^{n} S_j \cdot (n - j + 1) - S_n,\ n = u = N_l,\ i = 1..N, \qquad (11)$$

Where S_j is the value of the area of the j-th triangle.

Thus, the digital signature of the i-th package is a set of the following parameters:

$$Z_i = \{r_{ij}, A_i, l, k, M, f, t, d\},\ j = 1..u,\ i = 1..N \qquad (12)$$

A description of the encryption algorithm that enables us to create the digital signature for the i-th package is presented in figure 2.

The identification algorithm (figure 3) allows establishing the degree of pharmaceutical packaging legitimacy with consideration for the input maximum deviation of the encryption geometric element parameters μ from the values of the digital signature. The input parameters for the identification algorithm are encryption parameters, the scanned image, the selected encryption method, as well as the maximum permitted deviation of the identification

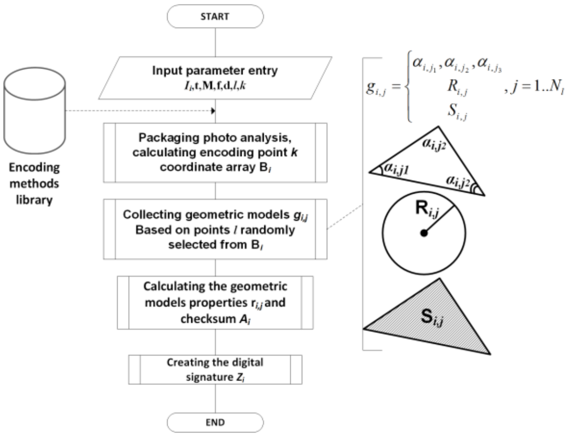
START
Input parameter entry
I_i,t,M,f,d,l,k
Encoding methods library
Packaging photo analysis, calculating encoding point k coordinate array B_i
Collecting geometric models $g_{i,j}$ Based on points l randomly selected from B_i
Calculating the geometric models properties $r_{i,j}$ and checksum A_i
Creating the digital signature Z_i
END
$g_{i,j} = \begin{cases} \alpha_{i,j_1}, \alpha_{i,j_2}, \alpha_{i,j_3} \\ R_{i,j} \\ S_{i,j} \end{cases}, j = 1..N_l$
$\alpha_{i,j1}$
$\alpha_{i,j2}$
$\alpha_{i,j2}$
$R_{i,j}$
$S_{i,j}$

Fig. 2. Generalized digital signature algorithm.

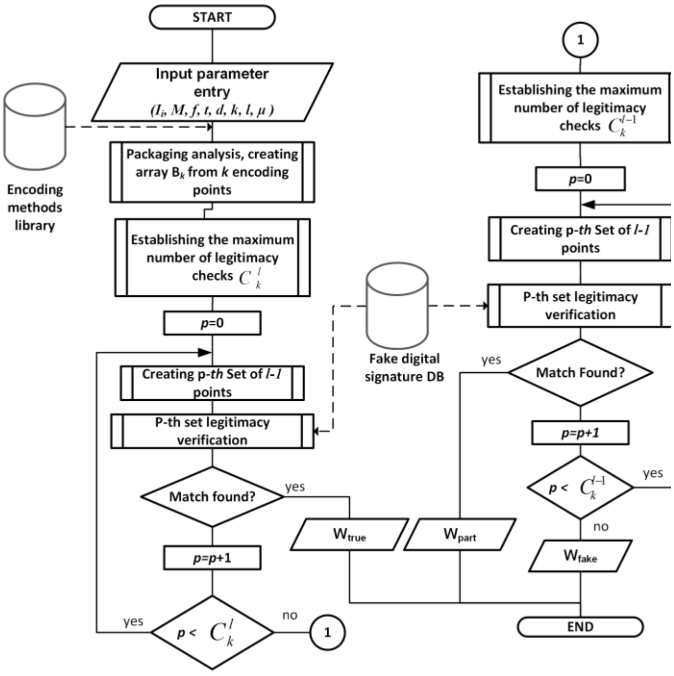
START
Input parameter entry
$(I_i, M, f, t, d, k, l, \mu)$
Encoding methods library
Packaging analysis, creating array B_k from k encoding points
Establishing the maximum number of legitimacy checks C_k^l
p=0
Creating p-th Set of l-1 points
P-th set legitimacy verification
Match found?
yes
p=p+1
$p < C_k^l$
yes
no
1
Fake digital signature DB
W$_{\text{true}}$
W$_{\text{part}}$
1
Establishing the maximum number of legitimacy checks C_k^{l-1}
p=0
Creating p-th Set of l-1 points
P-th set legitimacy verification
Match Found?
yes
p=p+1
$p < C_k^{l-1}$
yes
no
W$_{\text{fake}}$
END

Fig. 3. Pharmaceutical packaging identification algorithm.

values r_j compared to the stored values r_{cj}. The algorithm's output is the degree of packaging legitimacy $F \in \{W_{tue}, W_{fake}, W_{part}\}$. The identification algorithm allows us to ensure the legitimacy of whole and partially deformed packaging by verifying the full and partial consistency of the digital signature possibilities and the *i*-th identifiable package with the legitimate digital signature in the database.

VI. TESTING

The proposed pharmaceutical product polymer packaging protection methods and technologies have already been implemented and went through testing at Klöckner Pentaplast Europe GmbH & Co. KG polymer film plants in Europe and Russia. Testing was done using EP-73 polymer film, produced according to GOST 25250-88 at polymer film plant "OOO Klöckner Pentaplast Rus" in Saint-Petersburg, and the average identification time per package was no more than 30 second even with over a million fake digital signatures in the database.

The specialized version of the software adapted to mobile devices was tested at the joint polymer film center of "Klöckner Pentaplast GmbH" and Saint Petersburg State Institute of Technology. Sample data is presented in table 2.

TABLE II. DATA FOR TESTING THE MOBILE APP

Samples	Luminophore	Film	Production
LUM_02 Form 1	LWB520 – 0.08ppm, 20 points/cm^2	Transparent 200 microns	Calender
LUM_04 From 1	HK300 – 0.18ppm, 40 points/cm^2	Transparent 200 microncs	Rolling
LUM_04 Form 3	HK300 – 0.04ppm, 10 points/cm^2	Colored with pink pigment, and filled with chalk. 350 microns	Rolling

Testing results: The «Lum_04 Form3» sample provides the most system stability and result reproducibility due to:

- An appropriately rounded shape;
- Conformity to the minimal luminophore spot size;
- Luminophore spot glow period.

The proposed methods and technologies for product protection are patented in Germany and Europe [9, 10].

VII. CONCLUSION

The developed encryption methods and technologies offer an opportunity to select one of a few pharmaceutical packaging counterfeiting protection types using various protective features and objects. The developed identification algorithm also allows partial package identification with a preset maximum geometric element parameter deviation from the encrypted value.

Testing showed that the cost of such a system is minor due to the low concentration of pigments in the product, and cheap, widespread data processing equipment (lights, camera). This technology is offered to all customers and users of "Klöckner Pentaplast GmbH" polymer films for protecting their products against counterfeiting. Using the proposed physical and mathematical protection methods as well as the encryption/identification algorithms enable pharmaceutical package identification within a reasonable timespan. This software package is flexible and can be configured for various product types and anti-counterfeit pharmaceutical packaging encryption methods.

ACKNOWLEDGMENT

The authors are grateful for the experimental data provided by «Klöckner Pentaplast Europe GmbH & Co. KG».

REFERENCES

[1] Chistyakova T.B., Sadykov I.A., Kohlert C., Ivanov A.B.: Methods of Coding and Identification of Pharmaceutical Production to Provide a Protection Against Forgery. In: Information technologies, pp. 52-57 (2011) (in Russian).

[2] Cockburn R., Newton P., Agyarko E., Akunyili D., White N. (2005) The Global Threat of Counterfeit Drugs: Why Industry and Governments Must Communicate the Dangers. PLoS Med 2(4): e100. https://doi.org/10.1371/journal.pmed.0020100.

[3] Newton P., Green M., Fernández F., Day N., White N.: Counterfeit anti-infective drugs. In: The Lancet Infectious Diseases, Vol. 6, No 9, pp. 602-613 (2006). http://dx.doi.org/10.1016/S1473-3099(06)70581-3.

[4] Kramer A.: Drug piracy: a wave of counterfeit medicines washes over Russia. In: The New York Times, Ssept. 5, 2006. URL: http://www.nytimes.com/2006/09/05/business/worldbusiness/05fake.html.

[5] Newton P., Green M., Fernández F.: Impact of poor-quality medicines in the 'developing' world. In: Trends Pharmacological Sciences, Vol. 31, Issue 3, pp. 99-101 (2010). DOI: http://dx.doi.org/10.1016/j.tips.2009.11.005.

[6] Kohlert C., Kohlert M., Chistyakova T., Ivanov I., Sadykov I.: Counterfeit-proofing based on the principle of randomness. In: Kunststoffe international, Vol. 7, pp. 32-35. (2010).

[7] Fujifilm ForgeGuard Anti-Counterfeit Label <http://ideasmodern.com/ideas/fujifilm-forgeguard-anti-counterfeit-label/>

[8] Market-leading security technologies for product and brand protection <http://www.tesa-scribos.com/eng/security_technologies>

[9] Patent DE 10 2008 032 781 A1. C. Kohlert, B. Schmidt, W. Egenolf, T. Chistjakova. Verpackungsfolie für Produktauthentifizierung, Authentifizierungsverfahren und – system.

[10] Patent WO 2010/003585 A1. C. Kohlert, B. Schmidt, W. Egenolf, T. Chistjakova. Packaging film for product authentication, authentication method and system.