(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 July 2017 (06.07.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/114569 A1

(51) International Patent Classification:
B42D 25/36 (2014.01) *B42D 25/45* (2014.01)
B42D 25/29 (2014.01) *B42D 25/328* (2014.01)
B42D 25/43 (2014.01) *B42D 25/351* (2014.01)

(21) International Application Number:
PCT/EP2015/081398

(22) International Filing Date:
30 December 2015 (30.12.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **INSTITUTE OF PHYSICS BELGRADE, UNIVERSITY OF BELGRADE** [RS/RS]; Pregrevica 118, Belgrade, 11080 (RS).

(72) Inventors: **PANTELIC, Dejan**; Nemanjina 7, Belgrade, 11080 (RS). **RABASOVIC, Mihailo**; Svetozara Papica 1/51, Belgrade, 11080 (RS). **KRMPOT, Aleksandar**; Jasenova 8/15, Belgrade, 11030 (RS). **LAZOVIC, Vladimir**; Jurija Gagarina 127, Belgrade, 11070 (RS). **PAVLOVIC, Danica**; Boška Živikovica 18c, Belgrade, 11260 (RS).

(74) Agent: **WINKLER, Andreas**; WINKLER IP, P.O. Box 347013, 28339 Bremen (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SECURITY DEVICE INDIVIDUALIZED WITH BIOLOGICAL PARTICLES

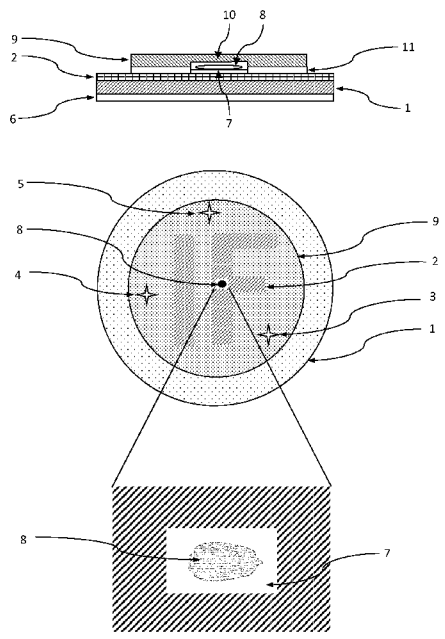


Fig. 3

(57) Abstract: The invention is directed to a security device with hologram, individualized by permanently attaching particles of biological origin, possessing large variability of optical effects and complexity of internal structure. Biological species and corresponding particles are chosen to maximize variability and complexity, while having durability, tamper sensitivity and micron size thickness. The security device comprises a transparent substrate (1) with at least one embedded hologram (2) on its upper surface; at least one inimitable biologic particle (8) arranged and attached on or above the upper surface of the substrate (1); a transparent superstrate (9), having a recess (10), and adhering to the substrate (1) and enclosing the biological particle(s) (8).

WO 2017/114569 A1

Published:

— *with international search report (Art. 21(3))*

Security device individualized with biological particles

Field of Invention

The present invention relates to security devices for identification and authentication of goods, articles and documents.

Background of the Invention

Optically variable devices (OVD) are a common protective element on various types of documents (e.g. identity cards, passports, visas, bank cards) – see the book "Optical document security" ed. by R. L. Van Renesse, Artech House, (1998). Holograms and other diffractive elements are mainly used, because their protective value is based on complexity of micron and submicron structures. Manufacturing is a complicated and expensive process whose final result is a master hologram – a single, unique prototype. To make protection commercially acceptable, the master hologram is copied and multiplied, resulting in a replica shim used for embossing into a plastic foil, which is then integrated into a document using a hot tool. The final result is a series of documents possessing exactly the same protective OVD. This is a significant drawback, because, if the OVD is counterfeited, a large number of fake documents can be manufactured.

As a result, there is ongoing research for a simple and affordable document individualization method. This makes counterfeit much harder, because each and every document has to be copied individually, i.e. large scale production of false documents becomes impossible. However, the trivial individualization by simply printing numbers will not work, because it is too simple and affordable, if using modern printing technologies (e.g. laser printing). Therefore, the individualization-bearing features must possess a significant amount of complexity, together with unrepeatable, individual properties. They have to be comparable in its uniqueness with biometric characteristics, such as: fingerprints, iris and retina pattern, but significantly more complex and miniscule. Currently used OVD security methods are not well suited for individualization (fingerprinting), as this will significantly increase the production prices.

Attempts to obtain "fingerprint" documents are based on the idea of the physical one-way functions, which are alternatively called the physically unclonable functions (C. Boehm, M. Hofer, "Physically unclonable functions in theory and practice", Springer, 2013). These are physical devices simple to manufacture, yet extremely difficult to reverse engineer and copy. Random structures can be highly significant for document security, because they offer simple and cheap production, almost impossible re-origination and unique features. It was proposed to tag documents with randomly dispersed objects such as metal, fluorescent or optical fibers ("Optical document security" ed. by R. L. Van Renesse, Artech House, (1998), pg. 210 - 211, and references therein). More details can be found in: "Counterfeit deterrent features for the next generation currency design", Committee on Next-Generation Currency Design, National Materials Advisory Board, Commission on Engineering and Technical Systems, National Research Council, Publication NMAB-472, (1993), Section: Random Pattern/Encryption Counterfeit-Deterrence Concept, pg. 74 - 75, and in Appendix E of the same document: "Methods for authentication of unique random patterns", pg. 117 – 119. Yet another technique uses holographic platelets as fingerprinting device (US2010110514 (A1), 2010 – R. Hradency, T. Tethal, L. Kotacka, I. Jermolajev, J. Drinkwater, C. Hradency, "Security articles and devices containing coded holographic platelets and methods of manufacturing the same").

Natural fibrous structure of paper-based substrates was used (J. D. R. Buchanan, R. P. Cowburn, A-V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, M. T. Bryan, " 'Fingerprinting' documents and packaging", Nature 436, (2005) 475). Laser beam was scattered from the paper surface and its statistics was observed and recorded. This, however, requires a large scale scanning of the document surface which is a slow process, and paper structure may be strongly affected by printing and everyday usage.

Yet another technique was described in R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, "Physical One-Way Functions," Science 297, (2002) 2026 - 2030, where mesoscopic scattering from disordered array of plastic spheres embedded in a transparent substrate was used to construct physical one-way function. The response of the system strongly depends on the illumination direction, again producing unique individual characteristics. The proposed method is limited by the physical requirements for the mesoscopic scattering, resulting in a 10 mm x 10 mm sized tag, with 2.5 mm thickness, which is unsuitable for the modern plastic card

technology. Furthermore, the dimension of scattering particles is rather large – 500 - 800 μm in diameter, with 100 μm average spacing – resulting in a bulky system which can be reverse engineered by techniques like micro-tomography.

It is a common knowledge that certain natural characteristic of living creatures are inherently complex and hard to reproduce. This was first realized by Benjamin Franklin who used this for document protection (Farley Grubb, "Benjamin Franklin and the birth of the paper money economy", Essay based on March 30. 2006 lecture, published by Federal Reserve Bank of Philadelphia). He made casts of plant leaves (correctly recognizing the uniqueness of their venation) and used them to print the first dollar bills. Due to further technological advancements, Franklin's method became obsolete, and was replaced with different printing techniques, such as: intaglio, guilloche, watermark, holograms, etc.

Two patents (WO 2007031077 (A1) 3/2007, C. Hamm-Dubischar, "Inorganic marking particles for characterizing products for proof of authenticity method for production and us thereof", and DE10238506 A1, 3/2004, H. Rauhe, "Producing information-bearing micro-particulate mixtures involves defining code that can be implemented using natural or subsequently applied particle characteristics selected from e.g. morphology") disclosed an idea for document protection which uses natural complexity of aquatic organism inorganic shells (like diatoms and radiolarians) according to characteristics of their surfaces. The practicing method is, however, not disclosed. Another problem is that the optical effects are not very pronounced, as well as their variability, and the complexity can be observed only at the sub-wavelength levels, using electron microscopy. Technique for estimating the degree of complexity was not described, either. Variation among the specimens of the same species is rather small. In that respect, the method can be used only for the forensic level of document authentication.

Recently, there was a significant amount of research aimed at using the principles of optics in nature for document protection (J. Sun, B. Bhushan and J. Tong, "Structural coloration in nature", RSC Adv., 2013, 3, 14862–14889). Variability of biological structures was also observed (L. P. Biro and J-P.Vigneron, "Photonic nanoarchitectures in butterflies and beetles: valuable sources for bioinspiration", Laser Photonics Rev. 5, No. 1, 27–51 (2011)). Biotemplating was used to manufacture butterfly scale-like structures using metals

(S.Sotiropoulou, Y. Sierra-Sastre, S. S. Mark, and C. A. Batt, "Biotemplated Nanostructured Materials", Chem. Mater. 2008, 20, 821–834).

Embossed holograms have been individualized by using a two-stage process (US7420720 (B2) — 2008-09-02, G. Dausmann, I. Ments, "Optical element and method for the production thereof"). The first one generates a master hologram with a background image. In the second, additional embossing shims are used containing letters or numbers, capable of uniquely marking a hologram.

Another way of individualization is described (DE102007063504 (A1) 2009-05-07, J. Ehreke, A. Leopold, "Individualized hologram manufacturing method for e.g. passport"), where a master hologram is used for the permanent part of holographic image, whereas a spatial light modulator is used for the variable information. Both images are combined on the third holographic medium.

The randomized systems described above must be machine-inspected, based on radiation scattering with consequent optical or microwave detection (in the case of metal inclusions). Recorded pattern is encrypted and stored in a central repository or on the document itself. Public key encryption method is used, as described in the report: Counterfeit deterrent features for the next generation currency design. A technique is based on two keys: a secret one, used for encryption, and a public one, used for the decryption.

All the methods use a complexity of natural structures, but their variability remained completely unused in the context of document protection. Document variability was rather attained by randomly dispersing particle- or thread-like entities across the document, as described in the patent literature (US 8408470B2, 2013, N. Komatsu, S-I. Nanjo, "Object for authentication verification, authentication verifying chip reading device and authentication judging method").

Summary of the Invention

The problem solved by the invention is individualization of mass-produced security devices with holograms. This is done by attaching biological particles with pronounced individuality.

The invention is directed to a security device, comprising:

a transparent substrate with at least one embedded hologram on its upper surface;

at least one inimitable biological particle arranged and attached on or above the upper surface of the substrate;

a transparent superstrate, having a recess, and adhering to the substrate and enclosing the biological particle(s)

The security device of the invention preferably comprises at least one predefined position without diffracting structures being formed on the substrate, and the inimitable biological particle(s) being placed at said position.

More preferably, the predefined position(s) without diffracting structures is (are) transparent, thus forming at least one window, wherein the inimitable biological particle(s) is (are) placed in at least one of said windows.

In one embodiment of the invention, more than one predefined positions are provided and arranged according to a predetermined pattern.

Preferably, the inimitable biological particle(s) is (are) selected from scales, hairs or bristles from the Lepidoptera wing or body.

Alternatively or additionally, the inimitable biological particle(s) is (are) selected from scales from the Coleoptera species cuticle and/or Araneae species body.

Furthermore, the inimitable biological particle(s) may be selected from hairs or bristles of the Trichoptera species.

In a preferred embodiment of the invention, the inimitable biological particle(s) is (are) firmly attached to the substrate by a transparent adhesive.

Alternatively, the inimitable biological particle(s) can be held in place on the substrate only by the natural attractive forces between the particle(s) and the substrate, without using adhesive substances.

In one embodiment of the invention, it is also proposed that the inimitable biological particle(s) is (are) cut in a predetermined shape, before arrangement on or above the substrate.

In another embodiment, more than one inimitable biological particles are used.

In one embodiment, the inimitable biological particles are stacked on one another, before arrangement on or above the substrate.

Preferably, the inimitable biological particle(s) is (are) inscribed with information, before or after arrangement on or above the substrate and/or enclosing of the biological particle.

More preferably, the inimitable biological particle(s) is (are) overtly inscribed with information by cutting through its (their) surface.

Alternatively, the inimitable biological particle(s) is (are) covertly inscribed with information by permanently bleaching its (their) fluorescence.

In a preferred embodiment of the invention, the inimitable biological particles of several species are chosen according to their variability of optical properties.

Preferably, the substrate comprises a transparent adhesive layer on its lower surface.

The invention is also directed to the use of the security device of the invention for identification and authentication of goods, articles and documents.

Finally, the invention is directed to a method of manufacturing a security device of the invention, comprising the following steps:

(1) providing a transparent substrate with at least one embedded hologram on its upper surface;

(2) demetalizing the hologram at at least one predefined position to form at least one transparent window;

(3) attaching at least one inimitable biological particle in said window; and

(4) placing a recess of a transparent superstrate over the window and adhering the superstrate to the substrate to enclose the biological particle(s).

There are several criteria which must be simultaneously fulfilled in order to provide the device with a unique fingerprint, usable for document protection purposes.

The first criterion for biological particle selection is according to variability of optical properties across their surface (near-field) or in the far-field of the scattered radiation. Detected optical properties include optical field amplitude and phase, field vorticity, reflection and transmission spectral distribution, overall biological particle shape, moiré pattern, polarization pattern, iridescence, diffraction, and fluorescence. The second selection criterion is the underlying complexity of biological particle structure, which has to span the range from nano-meter to micron-size features, intricately distributed in three-dimensions. The third criterion is their fragility, necessary for tamper sensitivity. The fourth criterion is the non-degradability of the structure, at least within the validity period of the document. The fifth criterion is the thinness of the structures such that they can be easily integrated within holographic OVDs, whose thickness is of the order of several tens of microns. The selection process requires fulfillment of all five criteria.

Preferred biological particles are those which can be found in the cuticle of various species of Lepidoptera (scales, hairs or bristles), Coleoptera (scales), Trichoptera (hairs or bristles), Araneae (scales). There is a general ground-plan of these structures, with the details

significantly depending on the species. They are self-contained (Fig. 1), plate-like or cylindrical, having a wall of submicron thickness, which encloses the internal volume. Inside the particle, a number of features may exist, such as nano-pillars, photonic crystals, fluorescent nano-particles. One or both external surfaces are patterned with grating-like ridges and cross-ridges (Fig. 2). Ridges have a lamellar structure, similar to the Bragg grating. The main constituent is chitin, a biological polysaccharide insoluble in water and many other solvents. They are permanent remnants of individual cells, and may endure without changing their optical properties for long periods – it is known that dried insects like butterflies may survive for decades in entomological collections. Iridescence, diffraction pattern or fluorescence of individual particles may strongly vary across the surface (of the order of 50 x 150 μm^2), as can be seen in Fig. 1. Thickness is of the order of few microns, resulting in fragility of the whole structure, which is stable enough to be transferred and adhered to the hologram substrate.

A hologram may be prepared for individualization by making special marks on the hologram surface which define a local coordinate system. Particles are attached to the hologram in the positions defined with respect to the said coordinate system. Large surface-energy adhesive may be used to permanently fix the particles to the hologram surface. A particle is protected from tampering by the transparent superstrate, which is permanently affixed to the hologram using high surface-energy adhesive or hot-stamping. A recess is made in a superstrate, such that the particle is protected from high pressures exerted during the stamping process.

A single particle or a plurality of them can be attached to the hologram in a predefined pattern. Only a subset of attached particles might be used for authentication purposes, while the rest is there as a distraction, which makes counterfeit harder, as a counterfeiter would not know which particles are used for authentication. Biological particles which possess different optical properties on their front and rear side may be used to produce security features which can be read from both sides in perfect alignment (see-through register).

Brief Description of the Drawings

Fig. 1: Optical image of an individual butterfly scale, where the strong, local variability of iridescence can be observed.

Fig. 2: Scanning electron microscope image of the butterfly scale, where the complexity of its internal structure can be seen.

Fig. 3: Exploded view of the security hologram presented in two orthogonal projections.

Fig. 4: A security hologram with a window, where a number of individually cut and shaped Lepidoptera or Coleopteran scales are positioned inside the window.

Fig. 5: A security hologram with an array of windows where individual Lepidoptera or Coleopteran scales are attached.

Fig. 6: A security hologram with an array of windows where the individually cut and shaped Lepidoptera or Coleopteran scales are attached.

Fig. 7: A security hologram with an array of windows where the individually overtly inscribed Lepidoptera or Coleopteran scales are attached.

Fig. 8: A security hologram with an array of windows positioned in a rectangular grid. Windows are partially filled with Lepidoptera or Coleopteran scales as to produce a binary or bar-code.

Fig. 9: A security hologram without windows, where Lepidoptera or Coleopteran scales are randomly distributed across the hologram surface.

Fig. 10: A security hologram with an array of windows positioned in a quasiperiodic or aperiodic tiling (e.g. Penrose tiling).

Detailed Description of the Invention

In cooperation with the attached drawings, the technical contents and detailed embodiments of the present invention are described hereinafter, however, not limiting its scope of protection which is exclusively defined by the claims. Any equivalent variation and

modification made according to the appended claims is to be included into their scope of protection.

Reference is made to Fig. 3 which presents two orthogonal views of one embodiment of the security device of the present invention. It is composed of a substrate 1, having a hologram 2 embedded on its upper surface. Additional marks 3, 4 and 5, whose dimensions are smaller than 200 μm, are incorporated into the hologram 2. The lower surface of the substrate 1 carries an adhesive layer 6, which can be activated either by heat or by pressure in order to integrate the security device with an article, good or document. The upper surface of the substrate 1 comprises a small patch of adhesive 7, whose surface is just large enough to receive a biological particle 8. The biological particle 8 is permanently attached onto the adhesive 7.

The biological particle 8 is then covered with a superstrate 9, having a recess 10 large enough to enclose the biological particle 8, without touching its upper surface. The lower surface of the superstrate 9 is covered with a transparent layer of heat or pressure activated adhesive 11, such that the recess 10 is left without adhesive layer. Superstrate 9 and substrate 1 are attached to each other, such that they enclose the biological particle 8.

In another embodiment, depicted in Fig. 4, the hologram 2 is demetalized at the places where the biological particles 8 are to be put, thus producing a window 12 which enables observation of the optical properties of the biological particle from underneath.

In a further embodiment as shown in Fig. 5 a number of cut shaped butterfly scales 8 are positioned inside the hologram window 12, following the previously described procedure.

Reference is made to Fig. 6, representing another embodiment of the security device of the present invention designed and manufactured to have an unspecified number of opaque or transparent windows without a diffraction grating 13, 14, 15, 16 and 17. The windows are positioned in an orderly manner, corresponding to certain symmetry, as in Fig. 6. The windows are of identical dimensions, width and height of each window being within the range of 150 μm – 300 μm. A transparent adhesive patch is placed inside each window and individual iridescent Lepidoptera or Coleopteran scales 8 are attached to each patch.

Preferred, but not limited to, Lepidoptera species are those possessing silver spots or patches on their wings, such as: *Issoria lathonia*, *Argyrophorus argenteus*, *Dione moneta*, *Dione juno*, *Agraulis vanillae*, *Aryinis addipe, Argynis aglaja, Argynis paphia.* Other Lepidoptera species, possessing structurally colored scales, may be used, too, such as: *Diachrysia chrysitis*, *Macdunnoughia confusa*, *Autographa gamma*, *Jordanita globulariae*, *Callophrys rubi*. Preferred Coleoptera species are those possessing scales on their cuticle: *Hoplia coeruela*, *Pseudomyagrus waterhousei*, *Lamprocyphus augustus*, *Hypera diversipunctata*, *Prosopocera lactator*, *Cyphus hancocki*, *Entimus imperialis*, *Sphingnotus mirabilis*, *Hoplia argentea*, some Curculionidae, some Collembola. Preferred Trichoptera species are: *Pseudoleptocerus chirindensis*, *Phylloicus abdominalis*, *Nectopsyche punctata*, *Banyallarga vicaria*, *Hesperophylax designates*, *Polycentropus flavomaculatus*, *Mystacides azurea*, *Mystacides longicornis*, *Anthripsodes albifrons*, *Limnephilus binotatus*. Preferred Araneae species are those possessing scales on their cuticle, such as: *Maratus volans*, *Maratus splendens*, *Phidippus audax*, *Pamphobeteus antinuous*, *Cyriopagopus lividum.*

Windows can be either filled with scales from a single species, or with scales from several different species. The hologram 2 with scales 8 is covered with a transparent foil having recesses exactly matching the positions of windows on the hologram. A thin layer of a transparent adhesive is placed on the bottom side of a cover, without covering the recesses.

In yet another embodiment individual Lepidoptera or Coleopteran scales 8 are cut shaped, using laser machining, and then placed inside the hologram windows 12, as shown in Fig. 7, following the previously described embedding procedure.

In a further embodiment, depicted in Fig. 8, Lepidoptera or Coleopteran scales 8 are overtly inscribed with information 20 (e.g. text, numbers, image, barcode) by cutting through the scale 8, preferably by laser. Information 20 can be inscribed before or after the encapsulation of the scale 8 in the security device 1. The scales are cut by using short pulse laser - preferably pico-second or femto-second, whose energy is slightly above the damage threshold of scales. The laser beam is introduced in a microscope, where it is focused by the objective, directly onto the scale. The laser beam position is controlled using a pair of computer-controlled, galvanometer-scanning mirrors.

In an alternative embodiment Lepidoptera or Coleopteran scales 8 are covertly inscribed with information 20 (e.g. text, numbers, image, barcode), by bleaching the scale fluorescence. Information 20 can be inscribed before or after the encapsulation of the scale 8in the security device 1. The scales are bleached by using short pulse laser - preferably pico-second or femto-second, whose energy is slightly below the damage threshold of scales. The laser beam is introduced in a microscope, where it is focused by the objective, directly onto the scale. The laser beam position is controlled using a pair of computer-controlled, galvanometer-scanning mirrors.

In yet another embodiment, windows 12 are arranged in a regular rectangular grid (Fig. 9), and their occupancy depends on the binary encoding of information, wherein a window occupied with a scale designates binary 1, and an unoccupied window designates binary 0.

In yet another embodiment, there are no windows on the hologram 2, and scales 8 are randomly distributed on the hologram surface (Fig. 10).

A further embodiment is depicted in Fig. 11, where windows 12 are placed according to quasiperiodic or aperiodic tiling (e.g. Penrose tiling).

Claims

1. A security device comprising:

a transparent substrate (1) with at least one embedded hologram (2) on its upper surface;

at least one inimitable biologic particle (8) arranged and attached on or above the upper surface of the substrate (1);

a transparent superstrate (9), having a recess (10), and adhering to the substrate (1) and enclosing the biological particle(s) (8).

2. The security device according to claim 1, wherein at least one predefined position without diffracting structures is formed on the substrate (1), and the inimitable biological particle(s) (8) is (are) placed at said position.

3. The security device according to claim 2, wherein the predefined position(s) without diffracting structures is (are) transparent, thus forming at least one window (12), wherein the inimitable biological particle(s) (8) is (are) placed in at least one of said windows.

4. The security device according to any of claims 2 or 3, wherein more than one predefined positions are provided and arranged according to a predetermined pattern.

5. The security device according to any of the preceding claims, wherein the inimitable biological particle(s) (8) is (are) selected from scales, hairs or bristles from the Lepidoptera wing or body.

6. The security device according to any of the preceding claims, wherein the inimitable biological particle(s) (8) is (are) selected from scales from the Coleoptera species cuticle and/or Araneae species body.

7. The security device according to any of the preceding claims, wherein the inimitable biological particle(s) (8) is (are) selected from hairs or bristles of the Trichoptera species.

8. The security device according to any of the preceding claims, wherein the inimitable biological particle(s) (8) is (are) firmly attached to the substrate (1) by a transparent adhesive.

9. The security device according to any of claims 1 to 7, wherein the inimitable biological particle(s) (8) is (are) are held in place on the substrate (1) only by the natural attractive forces between the particle(s) and the substrate..

10. The security device according to any of the preceding claims, wherein the inimitable biological particle(s) (8) is (are) cut in a predetermined shape, before arrangement on or above the substrate (1).

11. The security device according to any of the preceding claims, wherein more than one inimitable biological particles (8) are used.

12. The security device according to claim 11, wherein the inimitable biological particles (8) are stacked on one another, before arrangement on or above the substrate (1).

13. The security device according to any of the preceding claims, wherein the inimitable biological particle(s) (8) is (are) inscribed with information, before or after arrangement on or above the substrate (1) and/or enclosing of the biological particle.

14. The security device according to claim 13, wherein the inimitable biological particle(s) (8) is (are) overtly inscribed with information by cutting through its (their) surface.

15. The security device according to claim 13, wherein the inimitable biological particle(s) is (are) covertly inscribed with information by permanently bleaching its (their) fluorescence.

16. The security device according to any of the preceding claims, wherein the inimitable biological particles of several species are chosen according to variability of their optical properties.

17. The security device according to any of the preceding claims, wherein the substrate (1) comprises a transparent adhesive layer (6) on its lower surface.

18. Use of the security device according to any of the preceding claims for identification and authentication of goods, articles and documents.

19. A method of manufacturing a security device according to any of claims 1 to 17, comprising the following steps:

(1) providing a transparent substrate (1) with at least one embedded hologram (6) on its upper surface;

(2) demetalizing the hologram (6) at at least one predefined position to form at least one transparent window (7);

(3) attaching at least one inimitable biological particle (8) in said window (7); and

(4) placing a recess (10) of a transparent superstrate (9) over the window (7) and adhering the superstrate (9) to the substrate (1) to enclose the biological particle(s) (8).

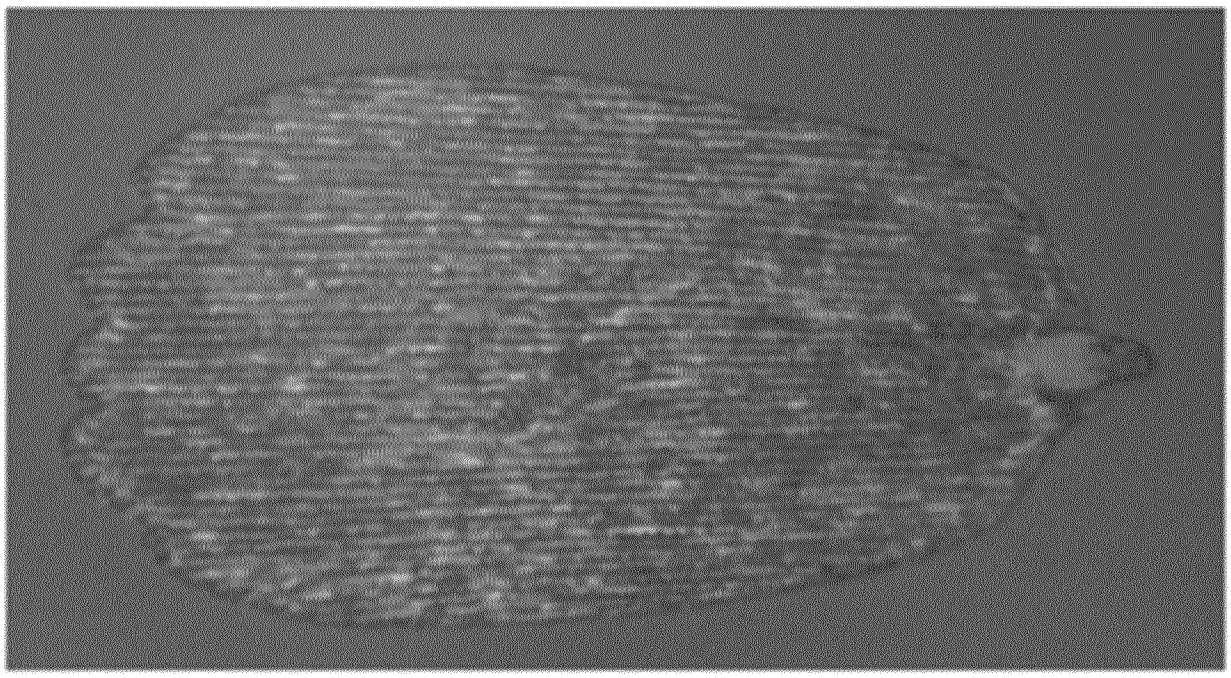


Fig. 1

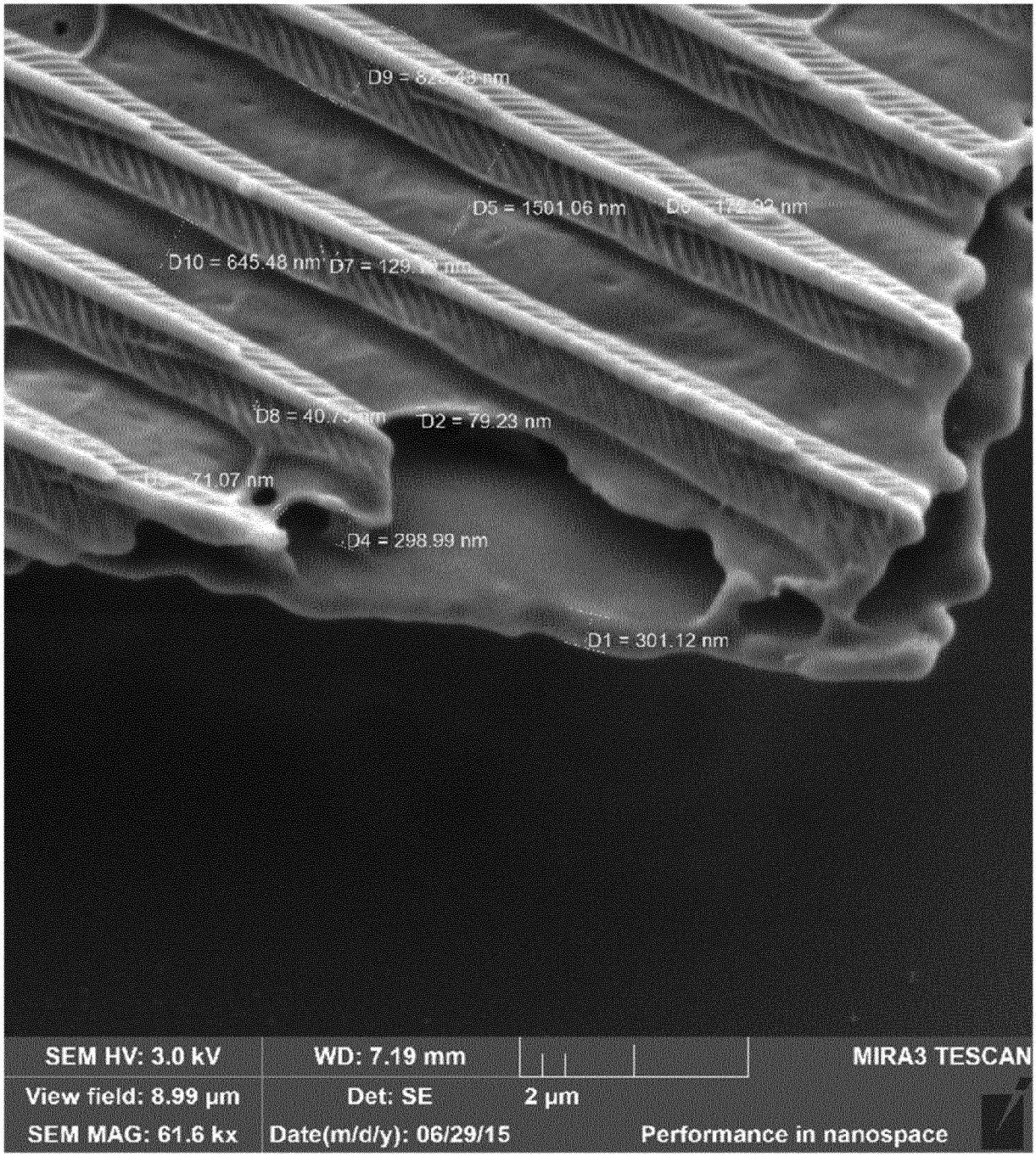

D9 = 82
D5 = 1501.06 nm
D10 = 645.48 nm
D7 = 129
D8 = 40.7
D2 = 79.23 nm
71.07 nm
D4 = 298.99 nm
D1 = 301.12 nm
SEM HV: 3.0 kV
WD: 7.19 mm
MIRA3 TESCAN
View field: 8.99 µm
Det: SE
2 µm
SEM MAG: 61.6 kx
Date(m/d/y): 06/29/15
Performance in nanospace

Fig. 2

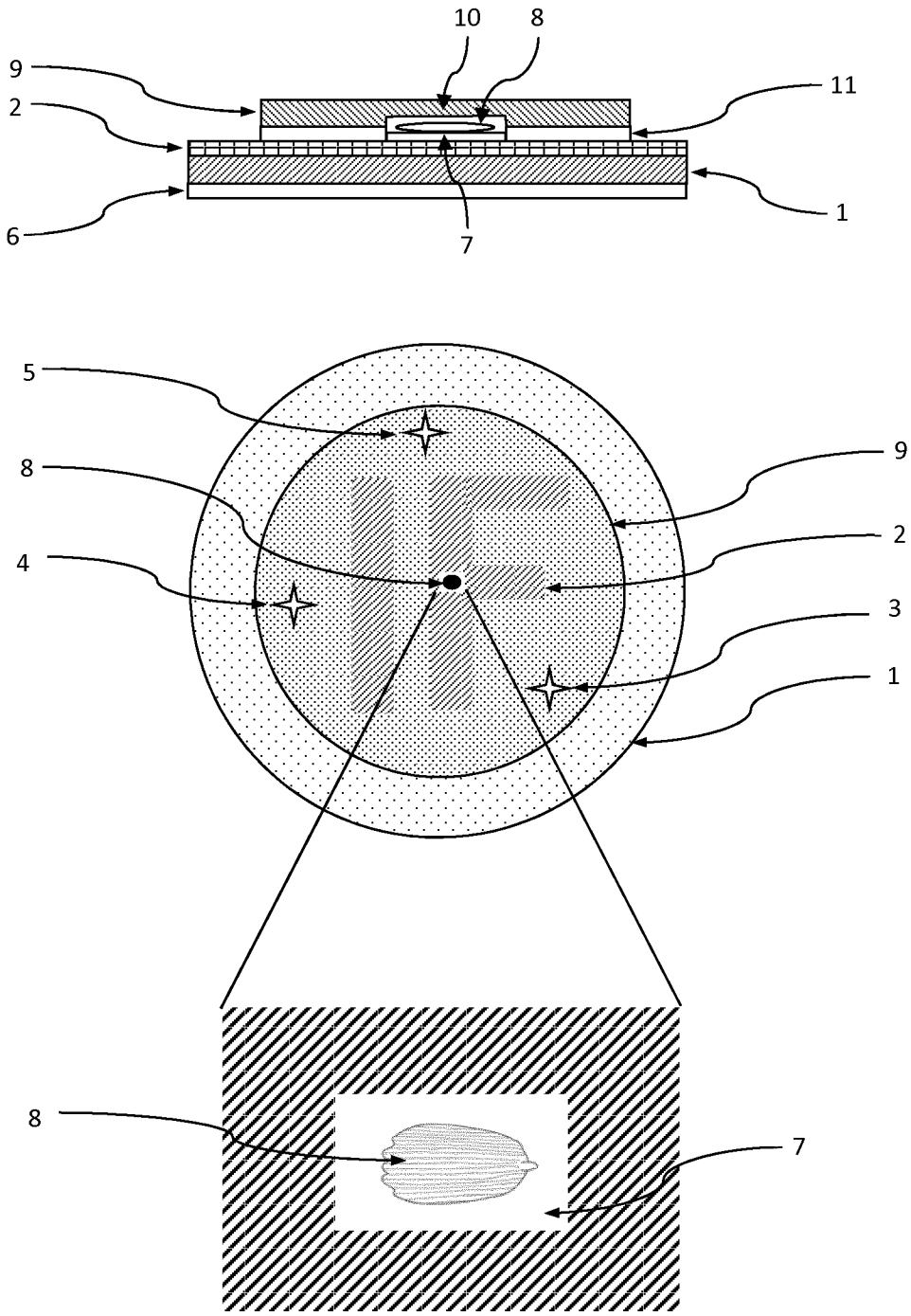


Fig. 3

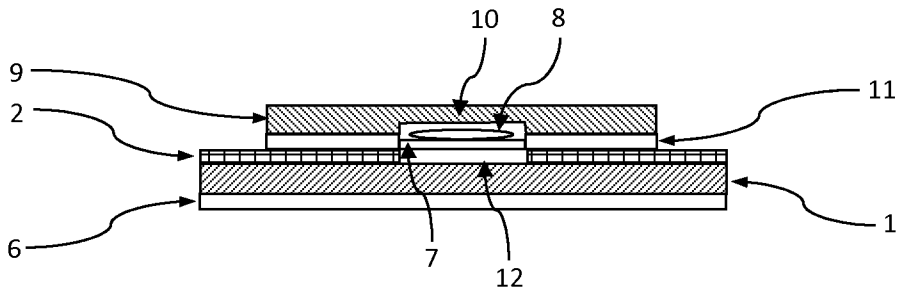


Fig. 4

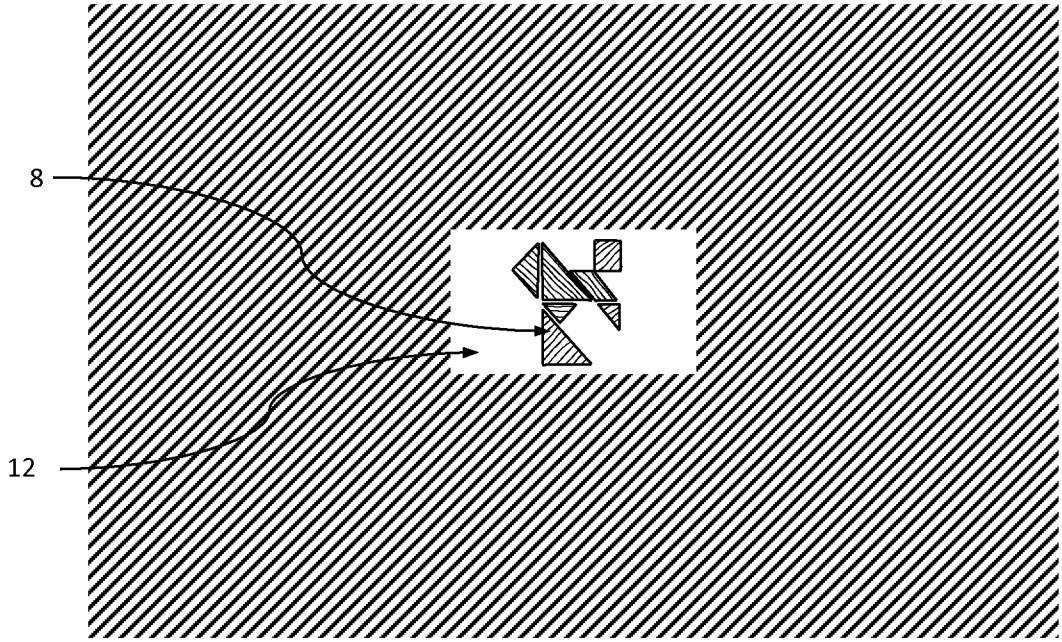


Fig. 5

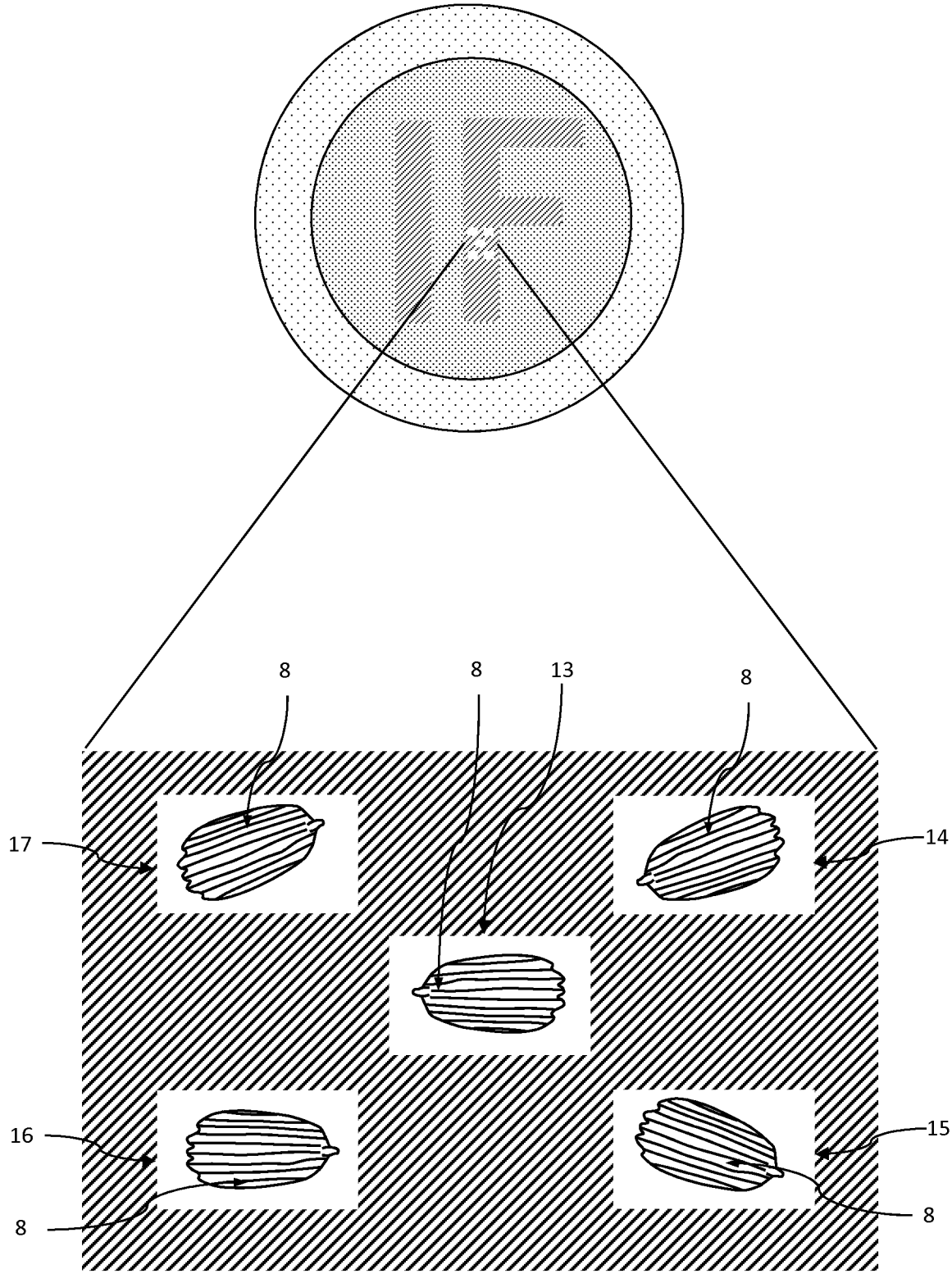


Fig. 6

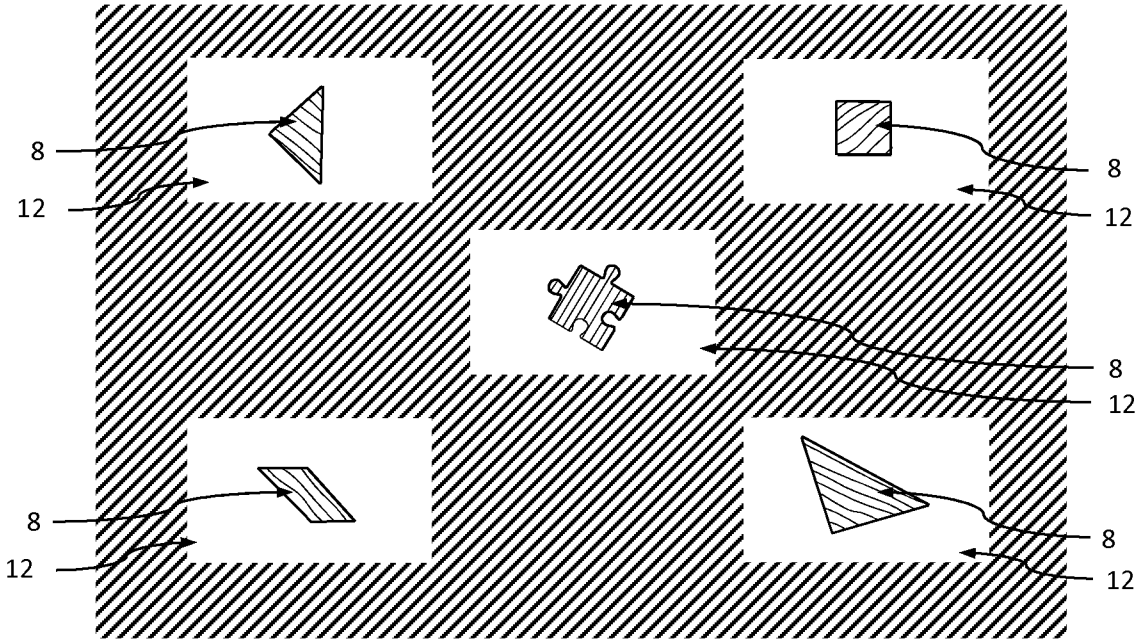


Fig. 7

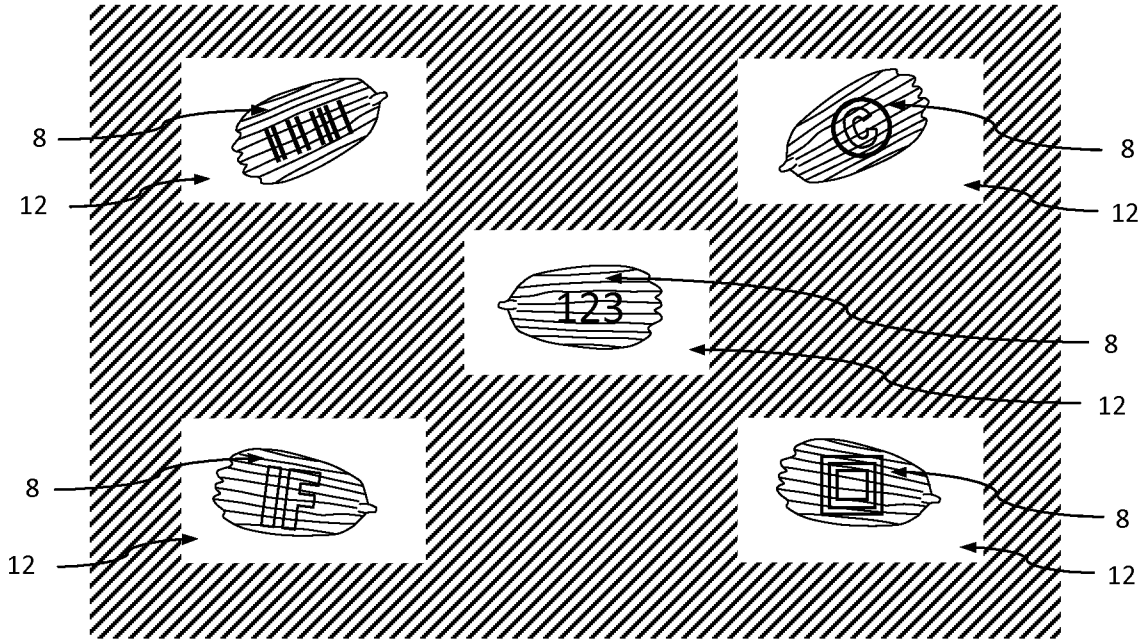


Fig. 8

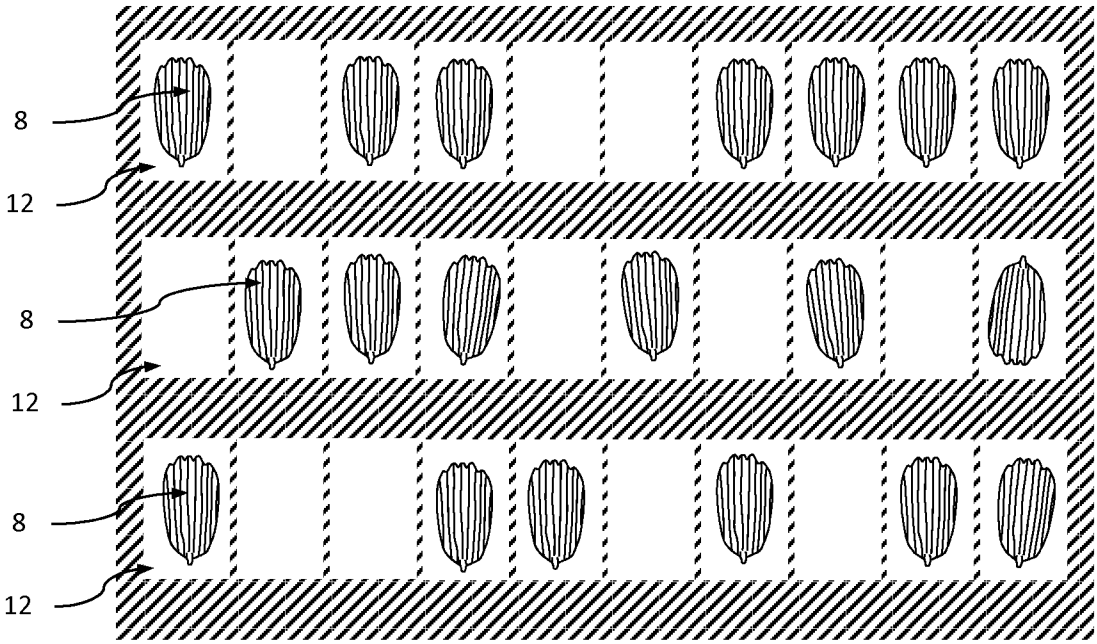


Fig. 9

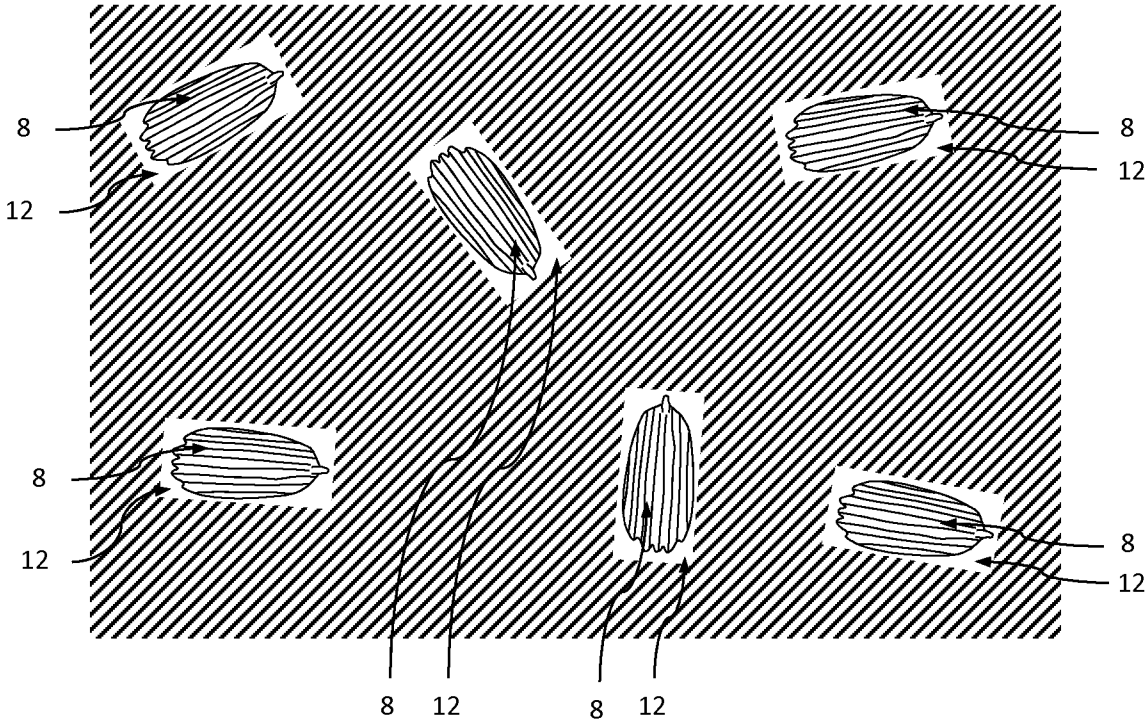


Fig. 10

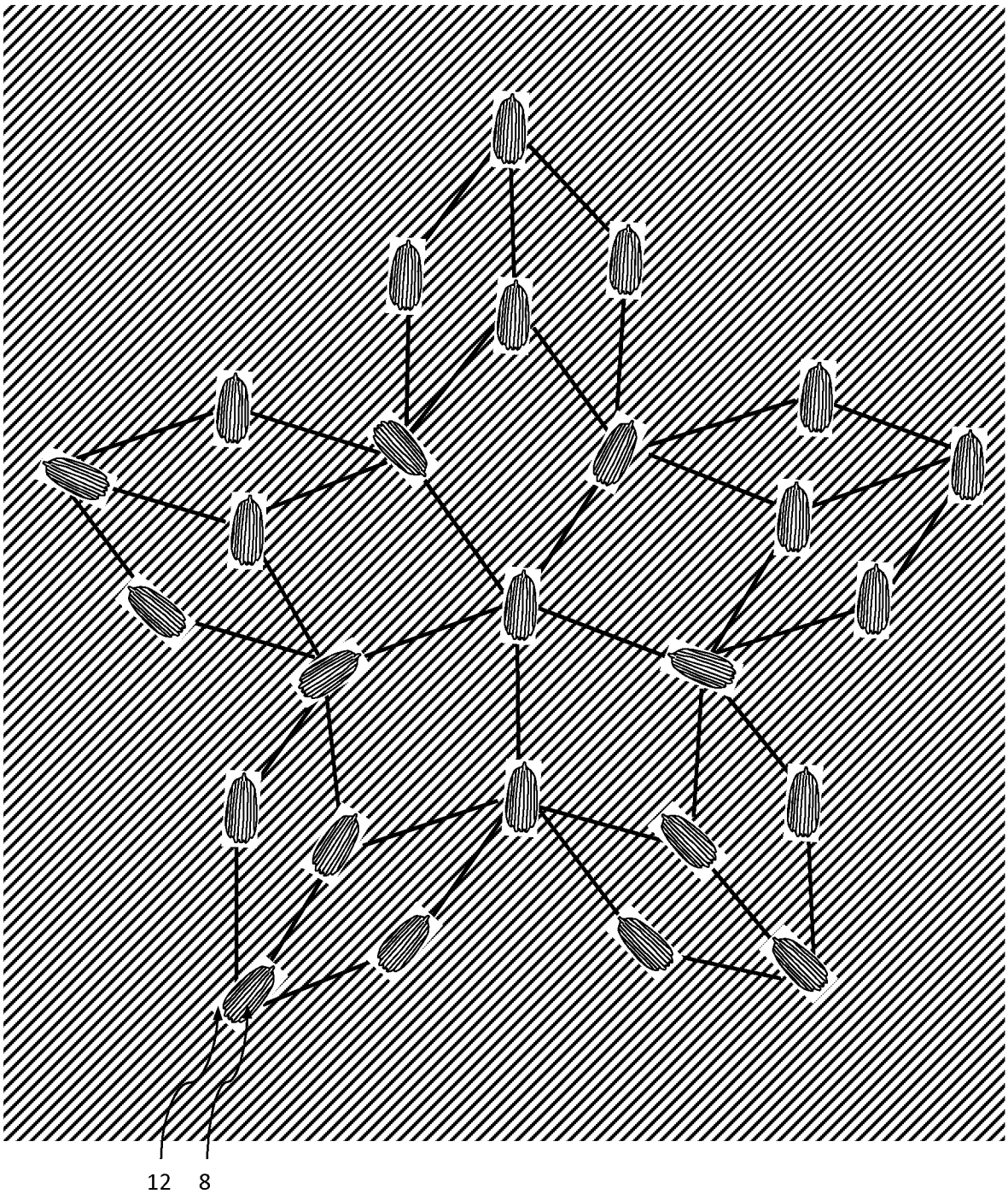


Fig. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/081398

A. CLASSIFICATION OF SUBJECT MATTER
INV. B42D25/36 B42D25/29 B42D25/43 B42D25/45 B42D25/328
B42D25/351
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
B42D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2009/052811 A2 (STIFTUNG A WEGENER INST POLAR [DE]; HOCHSCHULE BREMERHAVEN [DE]; DUBIS) 30 April 2009 (2009-04-30)	1-3,18
A	page 5, line 23 - page 7, line 2 page 12, line 15 - page 13, line 3 page 14, lines 7-9 page 14, line 29 - page 15, line 26 page 16, line 27 - page 17, line 10; figures 1,2	4-17,19

	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
25 August 2016	12/09/2016

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	D'Incecco, Raimondo

1

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Mastercard ET AL: "Card Identification Features Card Front Security Features Overview Security Feature Current Requirement/Placement New Requirement/Placement MasterCard Brand Mark Card front No change MasterCard Card Front Features and Designs Card Front Requirements", , 31 December 2005 (2005-12-31), XP055297501, Retrieved from the Internet: URL:https://www.mastercard.com/uk/merchant/en/downloads/10862_MasterCard_Card_Identification_Features.pdf [retrieved on 2016-08-24] see the credit card on the upper left corner and the copyright icon dated 2005 -----	1-19
A	WO 2007/031077 A1 (STIFTUNG A WEGENER INST POLAR [DE]; HAMM-DUBISCHAR CHRISTIAN [DE]) 22 March 2007 (2007-03-22) cited in the application page 14, line 13 - page 15, line 23 page 19, line 5 - page 20, line 18; figures 1,3 -----	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/081398

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2009052811 A2	30-04-2009	AT 510275 T	15-06-2011
		DE 102007052009 B3	04-12-2008
		EP 2227788 A2	15-09-2010
		WO 2009052811 A2	30-04-2009
WO 2007031077 A1	22-03-2007	DE 102005045642 A1	29-03-2007
		WO 2007031077 A1	22-03-2007