

System and method for brand protection based on the search results.

BACKGROUND

[0001] The present technique relates to the field of brand protection based on the search results.

[0002] Generally, a brand is understood as an identification mark of a product, for example, a name, a specific sign/symbol, term, color, image, sound or a combination thereof, which are designed to differentiate a product (service) from products (services) of the competitor.

[0003] Many companies and commercial organizations invest a lot in brand development and maintaining high quality of their brand-related products. Branding represents methods designed to impress, which contributes to the overall image and the target market segment attitude towards the brand. At any given time, any brand has a certain image (Brand Image), which represents a unique set of associations that are currently in the minds of consumers. These associations express what the brand means right now and represent an immediate promise to consumers given by brand authors.

[0004] In the effect that, in turn, results in an increased risk of unauthorized use of successful and popular brands, Internet scamming, online piracy, and counterfeit goods distribution for the violator's benefit.

[0005] The consequences of these actions for the brand are both material and non-material damage to company owners. For instance, violators can use a website containing the brand name of the Company A to sell their products of lower quality than the brand products of the Company A. Therefore, the Company A suffers material damage as losses caused by violators, which consist in the outflow of funds, as well as non-material damage, such as decrease in credibility of the Company A and compromise the brand in the eyes of consumers.

[0006] Therefore, the matter of brand protection against unauthorized use is particularly sensitive nowadays.

DESCRIPTION OF THE RELATED ART

[0007] Due to the need to protect the brand of companies, many solutions have been developed in the art to solve this problem.

[0008] The patent application US 2016/00253679 A1 (THOMSON REUTERS GLOBAL RESOURCES) describes the following: receiving a data set from the set of services, acquisition of a data set containing a set of brand data for comparison with the reference data set stored in the database and having a set of fields and a request through the digital communication network; an object identification module designed to identify and to extract an object data set from the acquisition data set, to compare the object data set with the reference object data set to allow for object identification, as well as to link an object identifier with the object identified and to determine a set of data about the relationships between entities; a synchronization module designed to receive data obtained from the acquisition data set and to compare the data obtained with the set of known brands data, as well as to generate a set of comparison data and output data indicating a match; an assessment module designed to generate an assessment data set based on the comparison data set; and a graphical user interface designed to graphically represent the set of the data assessed on the display connected to the remote user device.

[0009] The patent US8285830 B1 (STOUT BRODY et al.) describes the following method of brand protection against unauthorized use (cybersquatting) including: providing the user with a web page for sending the trademark to be monitored for possible sealing; receiving the trademark provided; creating a list of typing-error domains for the trademark provided; acquisition of data related to typing-error domains; tracing of HTTP links from the corresponding typing-error domains until the final corresponding destination typing-error domain is reached; monetization identifier determination for the corresponding typing-error domains by analyzing the sent HTTP requests; grouping the typing-error domains based, at least partially, on the predetermined criteria for inclusion in the form of a document,

whereby these predetermined criteria contain the monetization identifier related to the typing-error domains; software preparation of the document for its presentation, whereby the document includes the grouped domains with related data obtained; graphical user interface software to automatically fill in the document with additional data based at least on one piece of input data obtained from the second user or several of them, whereby the additional data contain at least one (a) of the document attachments providing evidence of trademark cybersquatting and (b) a legal argument in support of trademark cybersquatting; receiving one or several inputs from the second user; and automatically filling in the document with additional data for submission to the administrative authority; whereby the method is provided by the computing system containing one or several computing devices.

[0010] The patent application US 2016/0055490 A1 (THOMSON REUTERS GLOBAL RESOURCES) used a different approach to the problem described: the stage (a) describes scanning of the global communications network to identify and collect data on websites that may be involved in unauthorized use of the trademark; then at the stage (b), each website that may be involved in unauthorized use of the trademark is assessed whether it uses the trademark or not by analyzing at least any of the following: (i) the contents of the specified website; and (ii) data about the owner of the specified website.

[0011] The prior art does not describe methods for quickly responding to unauthorized use of the brand, with the possibility to establish the priorities for taking protection measures against violations based on the search results, which can serve one of the potential sources for obtaining accurate and timely data at the current state of the art.

[0012] This technique has been developed to solve some of the problems of the prior art identified by the analysis above.

SUMMARY

[0013] The present technique may comprise, for example, a system and a method for brand protection based on the search results.

[0014] The present techniques may provide brand protection based on the search results.

[0015] The techniques may include a method for brand protection based on the search results performing by the computing device and comprising the next steps:

[0016] receiving and storing in the internal database an information about a brand to be protected;

[0017] identifying the most popular brand queries in search systems;

[0018] collecting search results for at least one identified query over the assessment period;

[0019] calculating a harmfulness coefficient for at least one website contained in the collected search results;

[0020] identifying at least one website having the harmfulness coefficient exceeding a threshold value and defining it as fraudulent one;

[0021] scoring an investment damage score for at least one identified fraudulent website over the assessment period;

[0022] ranking and prioritizing the fraudulent websites by the investment damage score;

[0023] protecting the brand taking measures against the fraudulent websites in accordance with their ranking and priorities.

[0024] The present technique may include a system of brand protection based on the search result, the system comprising:

[0025] a data collection and storage module, the module is configured to receive and save information about the brand to be protected in the internal database; the module is also configured to connect to numerous services that can provide an information about the statistics of search system queries in real time; also the module is configured to scan the Internet and to collect search results over the assessment period;

[0026] a harmfulness analysis module, the module is configured to evaluate the website harmfulness coefficient for the protected brand, to compare the

calculated harmfulness coefficient with the harmfulness threshold value and to consider this website as fraudulent if the specified threshold value is exceeded;

[0027] a damage assessment module, the module is configured to determine the investment damage score for at least one fraudulent website over the assessment period on the base of search results, the module is also configured to rank and to prioritize the fraudulent websites based on the damage data obtained;

[0028] a brand protection module, the module is configured to take measures to protect the brand based on the priorities assigned.

[0029] The most popular search queries for the brand in one particular embodiment of the claimed technique are identified on the base of statistics of the search systems.

[0030] In another one particular embodiment of the claimed technique search result is a snapshot of the query search results, the snapshot comprising websites and their places in the search results.

[0031] The snapshot of the search results in one particular embodiment of the claimed technique is represented by a table containing at least the position of the website in the search results, a link to the website, the title and the description of the link, the information about the device from which the snapshot has been made and its location.

[0032] The snapshots collection in another one particular embodiment of the claimed technique is additionally performed by at least one external remote computing device.

[0033] The snapshot of the search results in one particular embodiment of the claimed technique additionally contains contextual advertising associated with search system queries.

[0034] The harmfulness coefficient in one particular embodiment of the claimed technique is calculated according to the formula:

$R = 1 - \prod_i (1 - w_i)$, where R is the harmfulness coefficient of the website and w_i is the weight of the corresponding indication of the harmfulness of the website.

[0035] The indications of harmfulness of the website in another particular embodiment of the claimed technique including, at least one of: presence of the domain in the list of legal/illegal domains, popularity of the website; presence of the domain in the list of fraudulent domains, absence of a certificate, using of website builders for creation of websites, number of pages of the website, presence of forms for payment or registration in the website; a category of the domain owner, one of: a private person, a legal entity, hidden; costs of hosting; domain zone; country of the hosting provider; relevance of the website.

[0036] In another particular embodiment of the claimed technique the investment damage score over the assessment period is calculated by multiplying the average brand purchase amount; the website conversion rate and an amount of website visitors.

[0037] In other particular embodiment of the claimed technique a calculation of the amount of visitors based on the search results and contextual advertising, the calculation is a summing of numbers of website visitors over the assessment period.

[0038] The statistical number of transitions to the position of the search results in one particular embodiment of the claimed technique is calculated according to the formula: $y = \text{CONST}_1 x^{-\text{CONST}_2}$, where y is the conversion rate and x is the position in the search results; and the constants CONST_1 and CONST_2 are calculated on the base of combination of brand data and search system data over the assessment period.

[0039] In another particular embodiment of the claimed technique the constants CONST_1 and CONST_2 are calculated on the base of readings of the counter available on the website.

[0040] A brand protection measures against the fraudulent websites may include at least one of the following: taking of measures to block the fraudulent

website; taking of measures to reduce the website traffic; taking of measures to remove a fraudulent website from the search results; adding a fraudulent website into the fraudulent resource database; collecting of evidence of fraudulent actions of the website; investigating the ownership of the fraudulent website; legal influence on the fraudulent website, including influence on its owner; notifying customers and/or potential customers about a fraudulent website; and the identification of website affiliation with previously known fraudulent websites.

BRIEF DESCRIPTION OF THE ATTACHED FIGURES

[0041] Fig. 1 – diagram of an exemplary embodiment of the brand protection system based on the search results.

[0042] Fig. 2 – flowchart that illustrates how the brand can be protected based on the search results.

[0043] Fig. 3A – 3B – scheme of areas of interest on a snapshot of the search results made on a stationary device.

[0044] Fig. 3C – 3D – scheme of areas of interest on a snapshot of the search results made on a mobile device.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0045] The following detailed description is presented to enable any specialist in this field to implement and use this technique. Specific details are provided for the purposes of description to give a thorough understanding of this technique. However, it will be clear to a specialist in this field that these specific details are not necessary for the embodiment of this technique. Descriptions of specific applications are provided only as representative examples. Various modifications of the preferred embodiments will be evident to specialists in this field, and the general principles defined herein can be applied to other embodiments and applications without deviating from the scope of this technique.

[0046] This technique is not suspected of being limited to the embodiments shown, but should correspond to the broadest possible scope consistent with the principles and signs described herein.

[0047] Some of the embodiments provide for the system and method for brand protection based on the search results. In these embodiments, the methods are provided that enable to timely identify websites the activities of which cause the most damage to the brand in a given period of time, so called assessment period, as well as to counteract these harmful actions depending on the factors of a particular situation.

[0048] It is also worth noting that any component of the brand protection system based on the search results can be alternatively implemented or called a service, platform, or any other type of the component.

[0049] Fig. 1 shows an exemplary embodiment of the brand protection system based on the search results (130) according to some demonstration embodiments of this technique.

[0050] The brand protection system based on the search results (130) may contain, for example, the following modules or components that can be implemented using appropriate hardware and/or software modules: data collection and storage module (131); harmfulness analysis module (132); damage assessment module (133); brand protection module (134).

[0051] The data collection and storage module 131 is configured to receive and save the information about the brand to be protected in the internal database of the system 130.

[0052] This information includes at least: brand names; a list of official brand-related resources (domains, social networks); a list of official resources of brand partners; the average customer purchase amount; brand presence countries (coverage); target audience language; data on possible seasonal changes in the demand for products; conversion rates for brand products; a list of already known fraudulent resources targeted at the brand; data on the official resource traffic; data on the distribution of types of visitors' devices (mobile phone, computer, tablet); a

period for which it is necessary to determine the damage (start and end of the assessment period).

[0053] The data collection and storage module 131 is configured to connect to numerous services that can provide information about the statistics of search system queries in real time (for example, Wordstat by Yandex, Google.AdWords, etc.) and to save the information obtained in the internal database of the system 130.

[0054] The data collection and storage module 131 is configured to scan the Internet for search result collection over the assessment period (110).

[0055] In addition, it is worth noting that at least one external device connected to the system 130 can be used for scanning. Moreover, a component that performs the necessary actions can be delivered at the external device in a Docker container. In the preferred embodiment, this device can be stationary device (for example, desktop computer, workstation or IoT device) and/or mobile device (for example, smartphone, tablet or laptop). It is worth noting that external devices are connected to the system through direct channels and/or one or several networks or other common channels, including the Internet, intranets and/or other networks, as well as wired and/or wireless communication lines.

[0056] The snapshots obtained after collecting the search results are saved in the internal database in the form of a table for each query, and this table contains the following lines: position, link, title and description of the link, information about the device from which the snapshot has been received, date/time of the snapshot, location of the device on which the snapshot has been made, and the search system. It is worth noting that all the snapshots for each day of the assessment period are saved in the internal database.

[0057] The harmfulness analysis module 132 is configured to evaluate the website harmfulness coefficient for the protected brand based on the website harmfulness parameters defined in the system 130, as well as to compare the calculated harmfulness coefficient with the threshold value predetermined in the system 130.

[0058] The damage assessment module 133 is configured to determine the investment damage score of damage to the brand over the assessment period and to prioritize all the identified fraudulent websites based on the calculated damage.

[0059] The brand protection module 134 is configured to take of measures to protect the brand based on the calculations in the modules (131) – (133). The brand protection module 134 can perform at least the following tasks: taking of measures to block a fraudulent website; taking of measures to reduce the website traffic; taking of measures to remove a fraudulent website from the search results; adding a fraudulent website to the fraudulent resource database; collecting evidence of fraudulent actions of the website; investigating the ownership of the fraudulent website; legal influence on the fraudulent website, including influence on its owner; notifying customers and/or potential customers about a fraudulent website; and the identification of website affiliation with previously known fraudulent websites.

[0060] The functional capabilities attributed to the system herein can be distributed among its components in an alternative way, for example, by combining or further separating the functions of one or more components, or can be distributed among another combination of components. In addition, although they are depicted as separate hardware components, they can be alternatively implemented as separate software modules running on one or several computer servers. Therefore, although only one variant of a specific component can be shown in Fig. 1, it should be understood that other combinations of the components included in the system can be used.

[0061] Fig. 2 represents a flowchart that illustrates how the brand can be protected based on the search results. In other embodiments, one or several illustrated actions may be omitted, repeated and/or performed in a different order. Therefore, a specific arrangement of the stages shown in Fig. 2 should not be considered a limitation of the scope of embodiments.

[0062] So, at stage 201, information that relates to the protected brand is received and saved into the internal database.

[0063] As previously mentioned, this information may include at least: brand names; a list of official brand-related resources (domains, social networks); a list of official resources of brand partners; the average customer purchase amount; brand presence countries (coverage); target audience language; data on possible seasonal changes in the demand for products; conversion rates for brand products; a list of already known fraudulent resources targeted at the brand; data on the official resource traffic; data on the distribution of types of visitors' devices (mobile phone, computer, tablet); the assessment period.

[0064] Then, at stage 202, the most popular brand queries in the search system are identified.

[0065] The statistics of search queries can be obtained from outside services, such as Wordstat by Yandex, Google.AdWords, Google Trends by Google, etc.

[0066] It is also worth noting that the statistics of search queries can be collected depending on the location, since the search results may differ when a user connects to search systems from different countries, language, and period.

[0067] Additionally, the statistics of search queries represents a report of search queries that led to demonstration of adverts or to clicks on adverts for particular brand. These reports are saved in the internal database.

[0068] The statistics obtained at stage 202 represents the most popular queries identified in the reports. The most popular queries may include a query of a brand only or query of a brand with one more relevant word, a query that includes a brand with various combinations of relevant words, a query of the main relevant search terms, a query of the main relevant terms that do not including a brand, etc.

[0069] It is worth noting that in an additional embodiment, the statistics of search queries may be received by the system 130 as input data.

[0070] Then, at stage 203, snapshots of the search results for each popular query identified at stage 202 are collected over the assessment period.

[0071] For instance, a snapshot of the search results is made daily. Alternatively, a snapshot is made with another frequency during the assessment period as shown in Fig. 3A-3D.

[0072] The snapshot of the search results additionally includes contextual advertising, which is depicted for the same queries as shown in Fig. 3B, 3C, where fields A, C, D are advertisement fields, and field B is the field of relevant websites. For the purpose of complete coverage, advertisement is collected from various locations, as well as from various devices.

[0073] In addition, in one embodiment of this technique, snapshots are received from at least one external devices communicating with system 130. The necessary software may be delivered at least to one external device in Docker container; the software is executed at least on one external device and returns the snapshot of search results into the system 130.

[0074] The snapshots obtained after collecting the search results are saved into the internal database in the form of a table for each of the queries identified during stage 202. Such table may contain the following lines: position in the list of search results, link, title and description of the link, geographical position, information about the device from which the snapshot has been received, date and time of the snapshot, location of the device on which the snapshot has been made, and the search system used.

[0075] After completion of stage 203, the method switches to stage 204, wherein the harmfulness coefficient is calculated for each website contained in the database of snapshots of search results.

[0076] The coefficient of harmfulness is calculated according to the formula:

$$R = 1 - \prod_i (1 - w_i) \quad (1),$$

where R is the harmfulness coefficient of the website and w_i is the weight of the corresponding indication of harmfulness of the website.

[0077] Indications of harmfulness of a website include, at least, the following:

presence of the domain in the list of legal/illegal domains,

domain life time;

popularity of the website;

presence of the domain in the list of fraudulent domains,

absence of a certificate,
using of website builders for creation of websites,
number of website pages,
presence of windows for payment or registration at the website;
category of the domain owner, one of: a private person, a legal entity, hidden;
cost of hosting;
domain zone;
country of the hosting provider;
relevance of the website.

[0078] It should be noted that the value of indications of harmfulness may be determined, for example, at least on the base of information obtained from registration data of the domain; information about the website's IP address; public databases with information about the website; direct analysis of contents of the website; information about the hosting provider taken from the official site and other sources.

[0079] Moreover, the weight of each of these indications may be determined either manually by experts or by a specially trained system based on data already accumulated in the system 130.

[0080] It should be noted that the weight of an indication of harmfulness may be additionally changed depending on the brand, its category and country, as well as the information supplied into the system during stage 201.

[0081] After that, during stage 205, harmfulness coefficient of each website is compared to the threshold coefficient R_0 that has been predetermined in the system 130.

[0082] All sites with the coefficient R above R_0 are considered fraudulent, and the method goes to stage 206. If R is below R_0 , the method completes on stage 211.

[0083] It should be noted that the described system 130 thus includes at least the following websites into the list of fraudulent websites:

phishing websites;

sites that distribute illegitimate copies of products (including counterfeit);
sites that illegally use brands or intellectual property (including trademarks);
fake online shops;
unofficial copies of legal resources;
fraudulent resources as such;
websites distributing malware;
sites leading (containing links or redirecting) to other sites of any of the above categories.

[0084] During stage 208, assessment of the investment damage score is calculated for the brand for the previously determined assessment period.

[0085] Damage investment damage score is calculated by determining a number of visitors of fraudulent sites, information about the average purchase price for the brand and conversion of the website.

[0086] Assessment of number of visitors of a fraudulent website is performing jointly both for organic search results and for contextual advertisement.

[0087] The assessment of number of visitors of organic search results is a summing of the numbers of visitors of the fraudulent website by days or with other frequency. It based on the following parameters: statistical number of clicks on an item of search results and the number of requests for a specific website.

[0088] It should be noted that the statistical number of transitions to the position of the search results is calculated according to the function:

$$y = \text{CONST}_1 x^{-\text{CONST}_2}, \quad (2)$$

where y is the conversion rate and x is the position in the search results; either based on the counter available on the website, and the constants CONST_1 and CONST_2 are calculated on the base based of the combination of brand data and search system data over the assessment period.

[0089] It should be noted that there are many studies dedicated to measurement of the indicator of organic search results (CTR) for 10 best results, which indicate that the higher the position in the search results, the greater the number of the website visitors is; the lower the position in the search results, the less

clicks and traffic the website receives (see <https://www.searchenginewatch.com/2012/08/23/organic-vs-paid-search-results-organic-wins-94-of-time/>).

[0090] In addition, CTR indicators are also classified on the basis of the request category: branded or non-branded. For example, in case of a non-branded request, average CTR of the first link is 48%, second link - 12%, third link - 8% and 32% fall on all other search results. In case of a branded request, CTR of the first link is 80%, second link - 6%, third link - 4% and 10% fall on all other search results.

[0091] It should be also noted that the conversion indicators in this technique are calculated on the basis of averaged coefficient data taken from public data of search systems.

[0092] Quantity of request for assessment of visitors of organic search results is also calculated on the basis of averaged data taken from public data of search systems.

[0093] Similarly, the number of visitors of advertisement links is assessed using statistical data of open sources on clicks on advertisements.

[0094] It should be noted that in one embodiment of this technique, the indicator of conversion and position of the website in the search results may be taken from the internal database of the system 130, wherein they have been saved during stage 201.

[0095] In other embodiment of the technique, in case of availability of a visitor counter on the website, the number of visitors can be adjusted.

[0096] Next, an amount of average purchase for the brand and indicator of conversion of the website are extracted from the database for calculation of the investment damage score.

[0097] Moreover, in some embodiments of the technique, if the brand conversion data are unknown, the average data are taken from public sources (for example, <https://www.smartinsights.com/wp-content/uploads/2017/08/Average-lead-generation-rates-by-industry-2017.png>).

[0098] Investment damage score is calculated for each of the identified fraudulent websites based on all previously obtained data by multiplying data of the visitors of websites, website conversion and average purchase price for the brand.

[0099] Obtained investment damage scores for each of the fraudulent sites identified are saved in the internal database.

[0100] Next, during stage 209, all fraudulent websites are ranked in descending order of investment damage score, and priorities are assigned to the sites in the list. The highest priority is assigned to the site with the highest investment damage score, and so on.

[0101] Websites with the highest priority pose the greatest danger in the current period of time. After selecting the websites with the highest danger priority satisfying the criteria, the method switches to stage 210.

[0102] During stage 210, measures are taken to protect the brand, i. e. response is implemented.

[0103] For example, such measures may include:

taking of measures to block the fraudulent website;

taking of measures to reduce the traffic of the website;

taking of measures to force the fraudulent website out of the search results;

addition of the fraudulent website into the databases of fraudulent resources;

collection of evidence of fraudulent activities of the website;

investigation of affiliation of the fraudulent website;

legal influence on the fraudulent website, including influence on its owner;

notification of customers and/or potential customers about the fraudulent website;

identification of affiliation of the website with previously known fraudulent websites.

[0104] Moreover, the required response measures may vary depending on the brand, its specifics, location, etc.

[0105] Moreover, the required response measures may be selected by representatives of the brand or by experts in the relevant field.

[0106] Moreover, the required response measures are determined by the system 130 according to the rules based on the experience accumulated in the system. For example, response measures may vary depending of the brand field, range of the calculated investment damage score, country, possibility of taking a measure for a specific brand, statistics of satisfaction of the company that owns the brand with respect to the response measures, etc.

[0108] It should additionally be noted that the environment in which are executed one or several embodiments mentioned above may include a general purpose computer or a special purpose device, such as a portable PC, a laptop, a tablet PC or a communication device. Certain details of such devices, such as processor, memory, data storage, cloud storage, display, etc. may be left out for clarity. A component, such as processor or memory, to which one or several tasks or functions are assigned, may be a general component temporarily configured for performance of a specific task or function or a specific component designed specifically for a task or a function. The term “processor” used here denotes one or several electronic circuits, devices, chips, processing cores and / or other components configured to process data and / or software code.

[0109] Data structures and software code detailed in this description are usually stored on a durable machine-readable medium, which can be any device or media capable of storing code and/or data to be used by a computer system. Machine-readable storage medium including, without limitation, nonvolatile or volatile memory, electrical, magnetic and optical memory devices, such as disc drives, magnetic tape, CDs, DVDs (digital versatile disks or digital video disks), solid state drives and / or other computer-readable media currently known or developed in the future.

[0110] Methods and processes detailed in the description may be embodied in a code and / or data, which may be stored on a machine-readable medium, as described above. When a process or a computer system reads and executes the code and manipulates the data stored on the medium, the processor or computer system

executes the methods and processes embodied in data, code structures, and stored on the medium.

[0111] Moreover, methods and processes may be programmed in hardware modules, including, without limitation, application specific integrated circuits (ASIC), field-programmable gate arrays (FPGA) and other programmable logic devices known currently or developed in the future; when such module is activated, it executes methods and processing included in the module.

[0112] Embodiments mentioned above are presented only for illustrative and descriptive purposes. They are not intended to be exhaustive or limit this disclosure by disclosed forms. Therefore, many modifications and options will be obvious to specialists in this field of technology. The scope of the technique are defined by the accompanying claims only, not by previous disclosure.

CLAIMS

1. **A method of brand protection based on the search results** performed on a computing device, the method comprising:

receiving and storing in an internal database an information about a brand to be protected;

identifying the most popular search queries for the brand in search systems;

collecting search results for at least one identified query over an assessment period;

calculating a harmfulness coefficient for at least one website contained in the collected search results;

identifying at least one website having the harmfulness coefficient exceeding a threshold value and defining it as a fraudulent website;

scoring an investment damage score for at least one identified fraudulent website over the assessment period, the investment damage score being representative of financial damage caused by the at least one identified fraudulent website to the brand over the assessment period;

ranking and prioritizing the fraudulent websites according to the investment damage score; and

protecting the brand by taking measures against the fraudulent websites in accordance with their ranking and priorities.

2. The method of claim 1, wherein identifying the most popular search queries also comprises using statistics of the search systems.

3. The method of claim 1, wherein the search results is a snapshot of the query search results, the snapshot comprising websites and their places in the search results.

4. The method of claim 3, wherein the snapshot of the search results is represented by a table containing at least a position of the website in the search results, a link to the website, a title and a description of the link, an information about a computing device on which the snapshot has been made and a location of the computing device on which the snapshot has been made.

5. The method of claim 4, wherein the snapshot further comprises contextual advertising, wherein collection of snapshots of the contextual advertising is additionally performed by at least one external remote computing device.

6. The method of claim 3, wherein the snapshot of the search results additionally contains contextual advertising associated with search system queries.

7. The method of claim 1, wherein the harmfulness coefficient is calculated according to the formula: $R = 1 - \prod_i (1 - w_i)$, where R is the harmfulness coefficient and w_i is a weight of the corresponding indication of the harmfulness of the website.

8. The method of claim 7, wherein the indication of the harmfulness of the website includes at least one of the following:

- presence of a domain of the website in a list of legal/illegal domains,
- popularity of the website;
- presence of the domain in a list of fraudulent domains,
- absence of a certificate,
- domain life time;
- using of website builders for creation of websites,
- number of website pages,
- presence of windows for payment or registration at the website;
- category of a domain owner, one of: a private person, a legal entity, hidden,
- cost of hosting;
- domain zone;
- country of a hosting provider;
- relevance of the website.

9. The method of claim 1, wherein the investment damage score over the assessment period is calculated by multiplying an average brand purchase amount; a website conversion rate and an amount of website visitors.

10. The method of claim 9, wherein a calculation of the amount of website visitors is based on the search results and contextual advertising, wherein the

calculation is a summing of numbers of website visitors over the assessment period.

11. The method of claim 10, wherein the summing of numbers of website visitors is based on the following parameters: a statistical number of transitions to the position of the search results and a number of queries made in the search system.

12. The method of claim 11, wherein the statistical number of transitions to the position of the search results is calculated according to the formula:

$y = \text{CONST}_1 x^{-\text{CONST}_2}$, where y is the conversion rate and x is the position in the search results, and the constants CONST_1 and CONST_2 are calculated on the basis of a combination of brand data and search system data over the assessment period,

or calculated on the basis of readings of a counter available on the website.

13. The method of claim 1, wherein the measures against the fraudulent websites for brand protection includes at least one of the following:

taking of measures to block the fraudulent website;

taking of measures to reduce a traffic of the fraudulent website;

taking of measures to force the fraudulent website out of the search results;

addition of the fraudulent website into databases of fraudulent resources;

collection of evidence of fraudulent activities of the fraudulent website;

investigation of affiliation of the fraudulent website;

legal influence on the fraudulent website, including influence on its owner;

notification of customers and/or potential customers about the fraudulent website;

identification of affiliation of the fraudulent website with previously known fraudulent websites.

14. **A brand protection system based on the search results**, the system comprising:

a data collection and storage module configured to receive and save information about a brand to be protected in an internal database; the data

collection and storage module being further configured to connect to numerous services that provide an information about statistics of search system queries in real time, and further configured to scan the Internet and to collect search results over an assessment period

a harmfulness analysis module configured to calculate a harmfulness coefficient for a website for the brand, to compare the calculated harmfulness coefficient with a harmfulness threshold value and to define the website as a fraudulent website if the calculated harmfulness coefficient exceeds the harmfulness threshold value;

a damage assessment module configured to determine an investment damage score for at least one fraudulent website over the assessment period on the basis of the search results, the investment damage score being representative of financial damage caused by the at least one identified fraudulent website to the brand over the assessment period, the damage assessment module being further configured to rank and to prioritize the fraudulent websites according to the investment damage scores obtained;

a brand protection module configured to take measures against the fraudulent websites to protect the brand based on the priorities assigned.

15. The system of claim 14, wherein the most popular search queries for the brand in the network are identified on the basis of statistics of the search systems.

16. The system of claim 14, wherein the search result is a snapshot of the query search results, the snapshot comprising websites and their places in the search results.

17. The system of claim 16, wherein the snapshot of the search results is represented by a table containing at least a position of the website in the search results, a link to the website, a title and a description of the link, an information about a device from which the snapshot has been made and a location of the device from which the snapshot has been made.

18. The system of claim 17, wherein collection of snapshots is additionally performed by at least one external remote computing device.

19. The system of claim 16, wherein the snapshot of the search results additionally contains contextual advertising associated with search system queries.

20. The system of claim 14, wherein the harmfulness coefficient is calculated according to the formula: $R = 1 - \prod_i (1 - w_i)$, where R is the harmfulness coefficient and w_i is the weight of the corresponding indication of the harmfulness of the website.

21. The system of claim 14, wherein the indication of the harmfulness of a website includes at least one of the following:

- presence of a domain of the website in a list of legal/illegal domains,
- popularity of the website;
- presence of the domain in a list of fraudulent domains,
- domain life time;
- absence of a certificate,
- using of website builders for creation of websites,
- number of website pages,
- presence of forms for payment or registration at the website;
- category of a owner of the domain, one of: individual, legal entity, hidden,
- cost of hosting;
- domain zone;
- country of a hosting provider;
- relevance of the website.

22. The system of claim 14, wherein the investment damage score over the assessment period is calculated by multiplying an average brand purchase amount; a website conversion rate and an amount of website visitors.

23. The system of claim 22, wherein a calculation of the amount of website visitors is based on the search results and contextual advertising, wherein the calculation is a summing of numbers of website visitors over the assessment period.

24. The system of claim 23, wherein the summing of numbers of website visitors is based on the following parameters: a statistical number of transitions to the position of the search results and a number of queries made in the search system.

25. The system of claim 22, wherein the statistical number of transitions to the position of the search results is calculated according to the formula:

$y = \text{CONST}_1 x^{-\text{CONST}_2}$, where y is the conversion rate and x is the position in the search results, and the constants CONST_1 and CONST_2 are calculated on the basis of a combination of brand data and search system data over the assessment period,

or calculated on the basis of readings of a counter available on the website.

26. The system of claim 14, wherein the measures against the fraudulent websites for brand protection includes at least one of the following:

taking of measures to block the fraudulent website;

taking of measures to reduce a traffic of the fraudulent website;

taking of measures to force the fraudulent website out of the search results;

addition of the fraudulent website in databases of fraudulent resources;

collection of evidence of fraudulent activities of the fraudulent website;

investigation of affiliation of the fraudulent website;

legal influence on the fraudulent website, including influence on its owner;

notification of customers and/or potential customers about the fraudulent website;

identification of affiliation of the fraudulent website with previously known fraudulent websites.

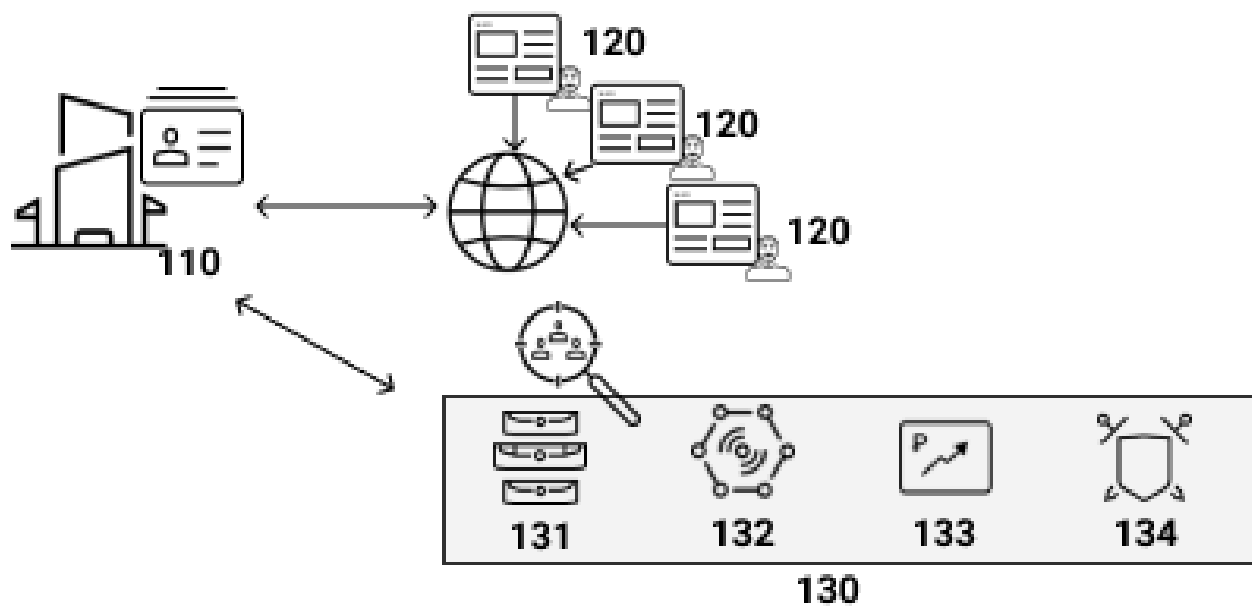


FIG. 1

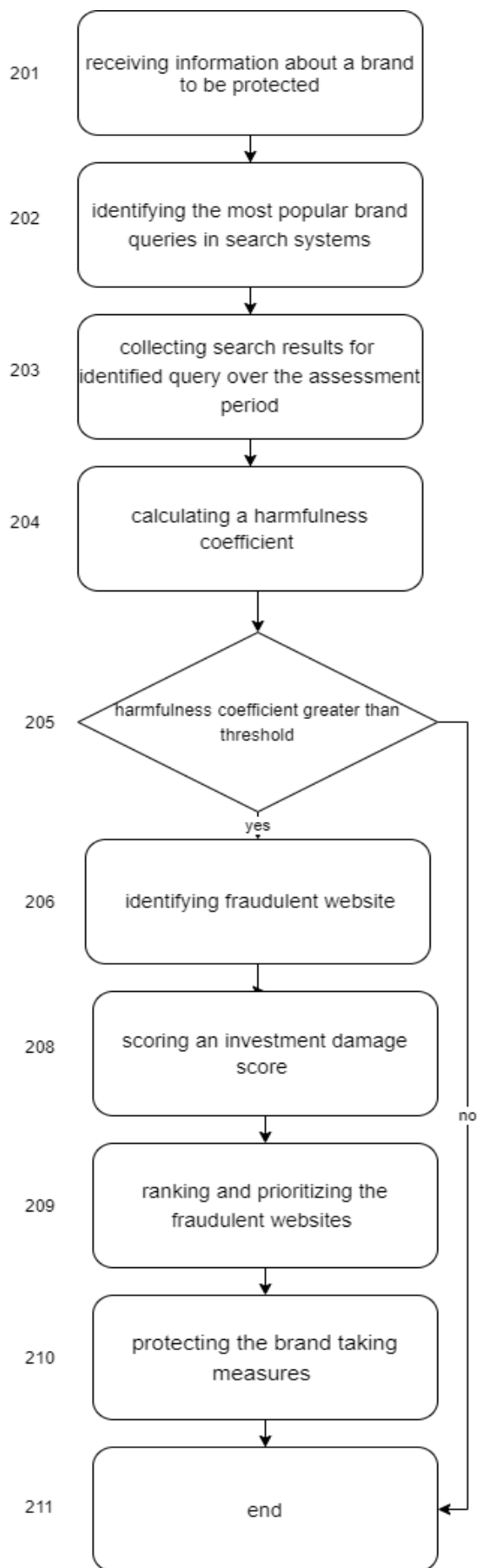


FIG. 2

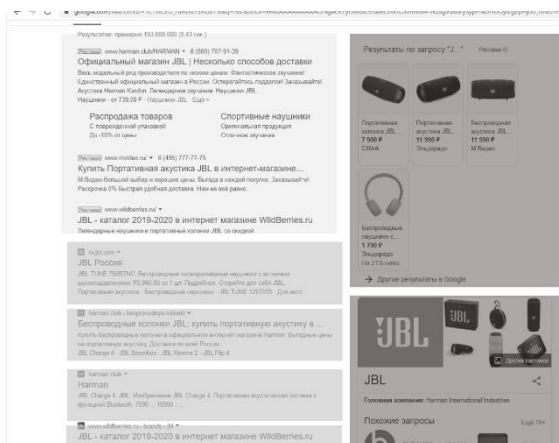


FIG. 3A

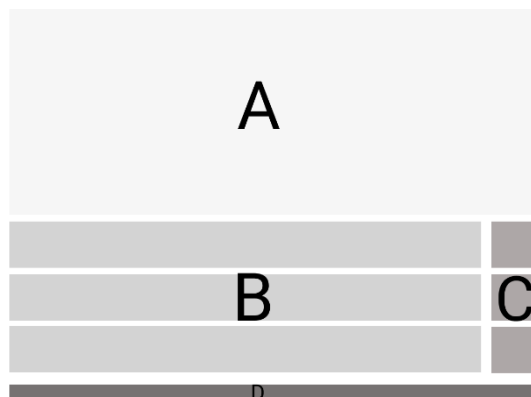


FIG. 3B

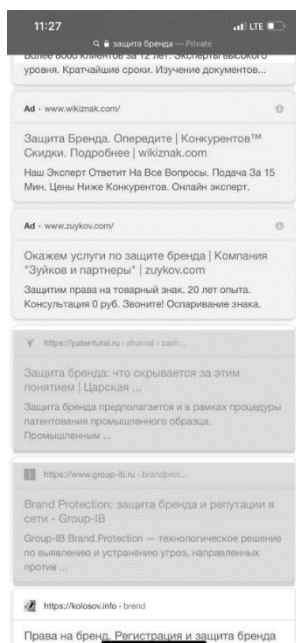


FIG. 3C

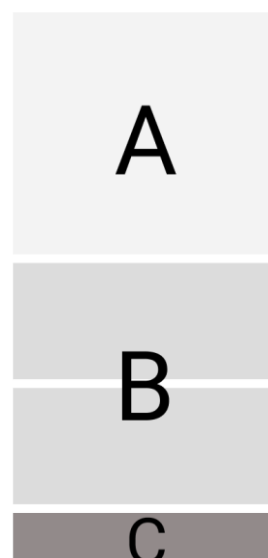


FIG. 3D