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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 May 2004 (27.05.2004)

PCT

(10) International Publication Number
WO 2004/045123 A1

(51) International Patent Classification[7]: H04K 1/00, H04L 9/00, 9/32, G06F 11/30, 12/14

(21) International Application Number: PCT/US2003/035607

(22) International Filing Date: 6 November 2003 (06.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/424,240 6 November 2002 (06.11.2002) US

(71) Applicant: SYSTEMS RESEARCH & DEVELOPMENT [US/US]; 6600 Bermuda Road, Suite A, Las Vegas, NV 89119 (US).

(72) Inventor: JONAS, Jeffrey, James; 9717 Winter Palace Drive, Las Vegas, NV 89145 (US).

(74) Agent: STINE, Thomas, K.; MARSHALL, GERSTEIN & BORUN LLP, 6300 Sears Tower, 233 South Wacker Drive, Chicago, IL 60606 (US).

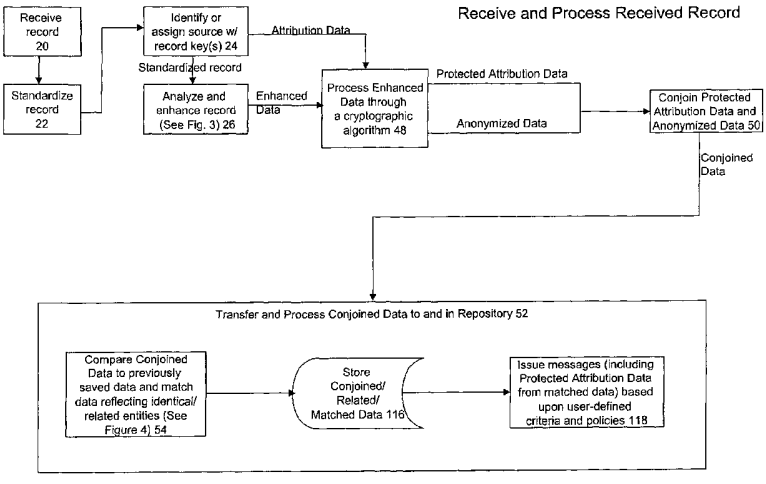
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CONFIDENTIAL DATA SHARING AND ANONYMOUS ENTITY RESOLUTION



(57) Abstract: A method, program and system for processing data is disclosed. The data comprises identifiers of a plurality of entities. The method, program and system comprising the steps of: (a) receiving one or more records, each record having a plurality of identifiers, each record corresponding with at least one entity [20], (b) utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record [48], (c) sometimes after transmitting the processed record to a separate system or database, comparing the processed record to previously stored data [54]; (d) matching the processed record with previously stored data that is determined to reflect the entity, the previously stored data that is determined to reflect the entity comprising at least a portion of at least two previously stored data that is determined to reflect the entity comprising at least a portion of at least two previously received records and/or based upon another identifier [54]; and/or (e) associating the processed record with previously stored data that is determined to reflect a relationship with the entity [54].

WO 2004/045123 A1

CONFIDENTIAL DATA SHARING AND ANONYMOUS ENTITY RESOLUTION

CROSS-REFERENCE TO RELATED APPLICATION

[0001] The present application claims the benefit of provisional application number 60/424,240, filed in the United States Patent Office on November 6, 2002.

FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] Not Applicable.

TECHNICAL FIELD:

[0003] This invention relates to processing and retrieving data in a database and, more particularly, to a submission, comparison and matching/associating of data in a confidential and anonymous manner.

BACKGROUND OF THE INVENTION:

[0004] In the wake of September 11, 2001 events, various parties (e.g., corporations, governmental agencies or natural persons) face a common dilemma: how can parties share specific information (e.g., a terrorist watch list, black list or a list of actual or potential problematic entities) that would assist the same or separate parties in detecting the presence of potential terrorists or other problematic parties, while maintaining the security and confidentiality of such information and separating any information that is not relevant to the matter?

[0005] Hesitation to contribute or otherwise disclose, as well as laws governing the use and disclosure of, certain information is predicated upon a concern that the information could be used in a manner that would violate privacy or otherwise cause damage to the party. Such damage could include identity theft, unauthorized direct marketing activities, unauthorized or intrusive governmental activities, protected class (e.g., racial, religious, gender, ethnic) profiling and discrimination, anti-competitive practices, defamation and/or credit or economic damage.

[0006] In response to this dilemma, or any situation requiring the sharing of confidential data, it would be beneficial to have a system wherein various parties may contribute data to an internal or external process or repository in a manner that: (a) sufficiently identifies each record in the data (e.g., a source and record number) without disclosing any entity-identifiable data (e.g., name or social security number); (b) prepares the data so: (i) identical unique value(s) results from same data regardless of source and (ii) such data can be transmitted in a standard, but confidential, format to protect the confidentiality and security of the data, (c) compares the data to previously contributed data while the data is still in the confidential format, (d) constructs an identifiable entity (such as by utilizing a persistent key and analyzing and enhancing the record with confidential representations of potential aliases, addresses, numbers and/or other identifying information) through matching of the compared data, (e) constructs related entities through an association of the compared data, and/or (f) generates messages for appropriate parties (such as with relevant record identifying elements – e.g., a source and record number), such messages sometimes sent in a confidential manner, such as: (i) on an interval basis and/or wherein at least one message is noise (e.g., a message that does not correspond with a match or relation, but is issued to minimize certain vulnerabilities corresponding with traffic pattern analysis) and (ii) after such message has been processed through a reversible cryptographic algorithm (e.g., encoding, encryption or other algorithm used to engender a level of confidentiality, but can be reversed, such as by using decoding or decryption).

[0007] Current systems use various means to transfer data in a relatively confidential manner within or between parties. For example, some current systems use a reversible cryptographic algorithm, which modifies the data in order to engender some level of confidentiality and lower the risk of losing data during transmission, prior to transmitting data with the understanding that the recipient will use a comparable

decoding or decryption method (i.e., an algorithm that reverses, returns or modifies the encoded/encrypted data to a format representative of the original data) in order to decipher and understand the data. However, once the data is deciphered, such data is subject to analysis and use in a manner that could cause the very damage that the encoding/encryption process was intended to protect against.

[0008] Other current systems use irreversible cryptographic algorithms (e.g., a one-way functions, such as MD-5 or other algorithm used to engender a level of confidentiality, but is irreversible) often as a document signature to make unauthorized document alteration detectable when the document is being shared across parties. Indeed, several existing irreversible cryptographic algorithms cause data to: (a) result in an identical unique value for same data regardless of source and (b) be undecipherable and irreversible to protect the confidentiality and security of the data. Any minor alteration (such as an extra space) in the data results in a different value after the use of the irreversible cryptographic algorithm as compared with data that does not have the minor alteration, even if the data is otherwise the same. Some current systems utilize an irreversible cryptographic algorithm to process a portion of the data and then match and merge records on a one-to-one basis based upon identical processed data. For example, current systems in a hospital may process the social security numbers in electronic patient records through a one-way function and then match and merge records on a one-to-one basis in a database based upon the processed social security numbers.

[0009] However, there are no existing systems that, at a minimum: (a) match received data – after at least a portion of such received data is processed through a cryptographic algorithm (e.g., reversible cryptographic algorithm, such as encoding or decryption, or an irreversible cryptographic algorithm, such as a one-way function) – with data previously stored in a database on a one-to-many or many-to-

many basis (i.e., received data consists of one or more records that matches data previously stored in a database, the matched data previously stored in a database comprising more than one previously received record), limiting the ability in current systems to build upon identifiable entities while the data is still in a confidential format, (b) move beyond the initial match process to analyze whether any additional information is gained in the initial match and then match other data previously stored in a database based upon the additional information, further limiting the current systems ability to construct identifiable entities, (c) utilizing all or part of those functions identified in (a) and (b) in this paragraph, to match not only same entities, but associate various entities that are determined to be related in some manner (e.g., a passenger on an airline reservation list is a roommate of a natural person on an airline watch list) and/or (d) issue a plurality of messages wherein at least one of the plurality of messages is merely noise.

[0010] As such and in addition, there are no existing systems that can use the cryptographic algorithm to share and compare confidential data (including, without limitation, by leaving personally identifiable information in a cryptographic format), construct identifiable or related entities and message the appropriate entities in a manner that maintains security and confidentiality of the original data.

[0011] The present invention is provided to address these and other issues.

SUMMARY OF THE INVENTION:

[0012] It is an object of the invention to provide a method, program and system for processing data in a database. The method, program and system preferably comprise the steps of: (a) receiving one or more records, each record having a plurality of identifiers (e.g., a plurality of data values of known types, such as two (2) data values of "John" corresponding with a known "first name" type and "Smith"

corresponding with a known "last name" type, which is sometimes emanating from one data value which is parsed into separate values corresponding with separate known types, such as when an original data value of John Smith corresponding with a known "name" type is parsed into two (2) data values of John corresponding with a "first name" type and Smith corresponding with a "last name" type), each record corresponding with at least one entity, (b) utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record, (c) sometimes, after transmitting the processed record to a separate system or database, comparing the processed record to previously stored data; and (d) matching the processed record with previously stored data that is determined to reflect the entity, the previously stored data that is determined to reflect the entity comprising at least a portion of at least two previously received records.

[0013] It is yet further contemplated that the method, program and system further comprise the steps of: (a) assigning or identifying a source to the record (e.g., an organization providing the record, a particular system within the organization, and a unique identifier representing the record in the particular system), (b) adding salt (i.e., additional data used to pad, modify, skew, or coat the processed data) to the record prior to the use of the cryptographic algorithm, and (c) sometimes deciphering at least a portion of the processed record (such as the source) after the step of matching the processed record with the previously stored data that is determined to reflect the entity.

[0014] It is further contemplated that the method, program and system further comprise the step of analyzing the record prior to the step of utilizing a cryptographic algorithm, which may include: (a) comparing the identifier against a user-defined criterion (such as a user-defined standard) or one or more data sets in a secondary database (such as querying the secondary database for a secondary identifier) or list and

(b) enhancing the record, such as by: (i) generating at least one variant to at least one identifier and including the variant(s) with the record and (ii) supplementing the record with the secondary identifier(s).

[0015] It is further contemplated that the method, program and system further comprise the steps of converting the record into a standard message format. For example, the method, program and system may convert the record into a standard message format by utilizing a type indicator (e.g., a designation, variable, tag or other indicator corresponding with a type, such as an XML tag corresponding with a type, such as name or phone number) for each of the identifiers. By way of further example, where the record contains three (3) identifiers corresponding with one (1) last name type and two (2) phone number types, a standardized record, utilizing <2> as the type indicator for the last name type and <3> as the type indicator for the phone number type, may result in the following: <2>Smith</2><3>111-222-3333</3><3>222-111-3131</3>. It is further contemplated that the type indicator may be discernable after the step of utilizing the cryptographic algorithm. For example, the standardized record set forth above in this paragraph, may result in the following after being processed in the cryptographic algorithm:

<2>23ff0ad398gl3ef82kcks83cke821apw</2><3>bcke39sck30cvk1002ckwlAeMn301L3b</3><3>23kaPek309cwf319oc3f921ldks8773q</3>.

[0016] It is further contemplated that the step of matching the processed record includes the steps of: (a) retrieving the previously stored data having the identical identifier(s), (b) evaluating whether another identifier is included in the processed record that does not exist in the previously stored data, (c) analyzing the previously stored data for a match to the processed record based on the another identifier; (d) repeating the steps until the previously stored data is analyzed for a match to the processed record based upon the another identifier; and (e) assigning a persistent key (i.e., a unique numeric or alphanumeric

identifier that, at a minimum, may be used to distinguish one or more records corresponding with a particular entity from other records corresponding with a different entity) associated with at least a portion of the previously stored data to the matched processed record. To the extent that the persistent key of the previously stored data is changed as a result of any matching, the system may save any prior persistent key(s) with a reference to the changed persistent key.

[0017] It is further contemplated that the method, program and system includes the steps of: (a) issuing one or more messages based upon a user-defined rule, such as: (i) wherein the message includes the source of the record and/or the source(s) of the previously stored data, which could be used to identify the relevant information in the other source(s), (ii) wherein at least one of the messages is noise, and/or (iii) in user-defined intervals and/or (b) storing the processed record in a database.

[0018] It is further contemplated that the method, process and system include the steps of: (a) receiving a record having a plurality of identifiers, the record corresponding with an entity, (b) utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record (sometimes analyzing the record prior to utilizing the cryptographic algorithm), (c) comparing the processed record to previously stored data, (d) matching the processed record with previously stored data that is determined to reflect the entity based upon at least one of the plurality of identifiers, (e) analyzing whether another identifier is included in the processed record that is not included in the matched previously stored data; and (f) matching the matched data with secondary previously stored data that is determined to reflect the entity based upon the another identifier (sometimes storing the processed record in a database).

[0019] It is yet further contemplated that the method, system and program further comprise the steps of: (a) receiving a record having a plurality of

identifiers, the record corresponding with an entity, (b) utilizing a cryptographic algorithm to process at least a portion of the record (sometimes analyzing and enhancing the record prior to utilizing the cryptographic algorithm), (c) comparing the processed record to previously stored data, and (d) associating the processed record with the previously stored data that is determined to reflect a relationship with the entity, and (e) storing the relationships with the entity in a database.

[0020] It is yet further contemplated that the method, system, and program further comprise the step of assigning a persistent key to the processed record.

[0021] It is yet further contemplated that the method, system, and program further comprise the steps of: (a) receiving a record having a plurality of identifiers, the record corresponding with an entity and at least one of the plurality of identifiers having previously been processed utilizing a cryptographic algorithm; (b) comparing the record to previously stored data, at least a portion of the previously stored data having been processed utilizing the cryptographic algorithm; (c) matching the record with the previously stored data that is determined to reflect the entity and/or associating the record with the previously stored data that is determined to reflect a relationship with the entity; and (d) issuing a plurality of messages wherein at least one of the plurality of messages is noise.

[0022] These and other aspects and attributes of the present invention will be discussed with reference to the following drawings and accompanying specification.

BRIEF DESCRIPTION OF THE DRAWINGS:

[0023] FIGURE 1 is a functional block diagram of the system in accordance with the invention.

[0024] FIGURE 2 is a flowchart of the receive and process the record steps.

[0025] FIGURE 3 is a flowchart of the Analyze record block in FIGURE 2.

[0026] FIGURE 4 is a flowchart of the Compare Conjoined Data block in FIGURE 2.

[0027] FIGURES 5-7 are flowcharts further illustrating the Compare Conjoined Data block in FIGURE 2.

DETAILED DESCRIPTION OF THE INVENTION:

[0028] While this invention is susceptible of embodiment in many different forms, there is shown in the drawing, and will be described herein in a detailed, specific embodiment thereof with the understanding that the present disclosure is to be considered as an exemplification of the principles of the invention and is not intended to limit the invention to the specific embodiment illustrated.

[0029] A data processing system 10 for processing data prior to, and in, a database is illustrated in FIGURES 1 through 7. The system 10 includes at least one conventional computer 12 having a processor 14 and memory 16. The memory 16 is used both for storage of the executable software to operate the system 10 and for storage of the data in a database and random access memory. All or part of the software may be embodied within various applications and equipment, depending upon the relevant confidentiality and security requirements. For example, the software may be embodied, stored or provided on any computer readable medium utilizing any of the following, at a minimum: (a) an installed software application on the source system, (b) a box unit that self-destroys the unit upon any tampering, and/or (c)

a CD, DVD or floppy disc. The computer 12 may receive inputs from one or more sources 18_1 - 18_n.

[0030] The data comprises one or more records having a plurality of identifiers. Each record corresponds with one or more entities. The one or more entities may be natural persons, organizations, personal property, real property, proteins, chemical or organic compounds, biometric or atomic structures, or other items that can be represented by identifying data. For example, a record that contains identifiers for name, employer name, home address, work address, work telephone number, home telephone number, car license plate number, car type and social security number may correspond with, at a minimum, the following entities: (a) natural person, (b) organization (e.g., employer or airline), and/or (c) property (e.g., car).

[0031] The system 10 receives the data from the one or more sources 18_1 - 18_n and processes each of the received records as illustrated in FIGURE 2. The software is stored in the memory 16 and is processed or implemented by the processor 14.

[0032] As illustrated in FIGURE 2, the system 10 receives the received record in step 20 and processed the received record in a manner that comprises the following steps: (a) if the received record is not in a standard format (e.g., XML), converts the received record into a standard format in step 22 and (b) identifies, assigns or otherwise attributes the record to a source (e.g., one or more identifiers that identifies the record in or to the source 18_1 - 18_n -- such as one or more primary keys of the record such as organization ID, system ID and record ID) in step 24 (the identifiers attributed to the source of the received record being "Attribution Data"). Alternatively, a coded cross-reference table is sometimes used whereby the Attribution Data is represented by an attribution key and the attribution key is used to locate the Attribution Value when necessary.

[0033] The system 10 further processes the received record in step 20 by analyzing and enhancing one or more of the plurality of identifiers of the received record in step 26 (the analyzed and enhanced identifiers of the record being "Enhanced Data") through: (a) comparing at least a portion of the identifiers of the received record 20 to a user-defined criteria and/or rules to perform several functions, such as: (i) name standardization in step 28 (e.g., comparing to a root names list), (ii) address hygiene in step 30 (e.g., comparing to postal delivery standards), (iii) geo-coding in step 32 (e.g., determining geographic locations, such as latitude and longitude coordinates), (iv) field testing or transformations in step 34 (e.g., comparing the gender field to confirm M/F or transforming Male to M), (v) user-defined formatting in step 36 (e.g., formatting all social security numbers in a 999-99-9999 format) and/or (vi) variant generation and inclusion in step 38 (e.g., common value alternatives or misspellings), (b) supplementing the received record in step 40 by causing the system 10 to access one or more databases in step 42 (which may contain the processing previously identified, thus causing the system to access additional databases in a cascading manner) to search for additional data (which may by submitted as new record(s) for receipt and processing in step 20) which can be added to the received record in step 44, and (c) building and including hash keys (e.g., a combination of certain data in the received record, such as the first three letters of a rooted first name, first four letters of last name and last five numbers of a social security number) in step 46. Any new, modified or enhanced data can be stored in newly created fields to maintain the integrity of the original data. By analyzing and enhancing the identifiers in each record, identifiers corresponding with the same entity are more likely to match (either through the original identifiers or through the new, modified or enhanced data).

[0034] Thereafter, all or part of the Enhanced Data is processed through a cryptographic algorithm and all or part of the Attribution Data is

sometimes processed through a cryptographic algorithm in step 48, which may include adding salt to the Enhanced Data or the Attribution Data, for protection and confidentiality, such as: (a) utilizing an irreversible cryptographic algorithm (e.g., one-way function) to process the entity-identifiable Enhanced Data (the irreversible processed data being "Anonymized Data") and (b) sometimes utilizing a reversible cryptographic algorithm (e.g., encryption or encoding) to process the Attribution Data (the reversible processed data being "Protected Attribution Data").

[0035] The Anonymized Data and the Protected Attribution Data are then conjoined in step 50 (and sometimes further processed through a reversible cryptographic algorithm) (the conjoined Anonymized Data and the Protected Attribution Data being the "Conjoined Data") and transferred, processed and saved in a repository ("Repository") in step 52.

[0036] The location of the Repository in step 52 is less critical because the Conjoined Data in the Repository in step 52 will be in a confidential format. Furthermore, in this example, only the Attribution Data is susceptible to being reversed (e.g., decrypted or decoded) from the Conjoined Data. As such, even if an unauthorized party was able to reverse the Attribution Data, such party would be unable to access, read or otherwise evaluate the Enhanced Data. However, the entirety of the Conjoined Data may be used for comparison and identity recognition or correlation purposes, while maintaining confidentiality.

[0037] The system in the Repository in step 52 compares the Conjoined Data with previously stored data (such as from other sources and potentially a warehouse of stored data) and matches any data reflecting the same or related entities in step 54. As illustrated in FIGURE 4, which is similarly exemplified in an invention by the inventor submitted under the title Real Time Data Warehousing, Application Number 10/331,068, and published on August 14, 2003 with

publication number 2003/0154194A1, the system in the Repository analyzes the first identifier of the Conjoined Data in step 56 and determines whether such identifier is a candidate list builder identifier (e.g., an identifier that may help in differentiating between and across entities) in step 58. For example, an identifier representing the social security number for a natural person type entity is helpful in differentiating between and across entities and would be used to build a list of potential candidates that would be used for matching or relationship building. If the identifier is a candidate list builder identifier, the system would determine whether the identifier is generally distinctive across entities in step 60, such as by comparing the identifier to a list of common identifiers and determining whether such identifier is on the list. The system would determine whether there are any additional uncompared identifiers in the Conjoined Data in step 62 if the identifier is: (a) not a candidate list builder identifier or (b) a candidate list builder identifier, but not generally distinctive across entities.

[0038] If the identifier is a candidate list builder and a generally distinctive identifier, the system would retrieve all occurrences of the identical identifier in the previously stored data in step 64, unless the system, based upon a user-defined criterion, determines that the identifier ought not to be considered a generally distinctive identifier in step 66. For example, if: (a) the identifier represented a social security number and the processed value corresponded with the value of 999-99-9999 (e.g., a value used in the source system as a default in the event the social security number was unknown), and (b) the user-defined criteria corresponding with the social security number identifiers was to stop retrieving occurrences if the number of identical social security numbers reached fifty (50) (or some other set amount), at the point when the same social security number reached 51, the system would determine that the social security number is not a generally distinctive identifier and would stop retrieving occurrences.

[0039] If the identifier is still considered to be a generally distinctive identifier in step 66, the retrieved occurrences are updated or added to a candidate list and relationship records in step 68. However, if the system determines that the identifier is not to be considered a generally distinctive identifier in step 66, the system stops matching based upon the common identifier (such as by adding the identifier to the list of common identifiers) in step 70 and may un-match previous records that were matched based upon the common identifier in step 72. Finally, the system determines whether there are any additional uncompared identifiers in the Conjoined Data in step 62.

[0040] Once the system determines that there are no more uncompared identifiers in step 62, the system retrieves all of the identifiers used for confidence and/or identity recognition (whether or not such identifiers are candidate building identifiers) corresponding to the candidate list in step 74 and compares the Conjoined Data with the candidate list in step 76 to enable the system to create confidence indicators (such as a likeness indicator and a related indicator) and update the candidate list and relationship records with the confidence indicators in step 78. The system then determines whether there are any matches based upon the likeness indicator in step 80 and if a match is identified, evaluates whether the matched record(s) contains any new or previously unknown identifiers in step 82 that may be candidate list builder identifiers to add or update the candidate list/relationship records. This process is repeated in step 84 until no further matches can be discerned. The system would then assign all of the matched records the same persistent key in step 86. If no matches were found for any record, the Conjoined Data would be assigned a new persistent key in step 88. Throughout the entire process, the system retains full attribution of the Conjoined Data and the matching process does not lose any data through a merge, purge or delete function.

[0041] Another example of the step of comparing Conjoined Data to previously stored data to find matches of same entities is illustrated in FIGURES 5 – 7 (and although not specifically identified, FIGURES 5-7 identifies several functions used with respect to identifying associations of related entities). Starting from an empty database 90, Conjoined Data record one 92 (emanating from company AAA, reservations system, record 21 within the reservation system, or AAA-Res-0021, and after being standardized, analyzed and enhanced, anonymized and conjoined) is received in the Repository. Given no records in the database 90, the system would find no occurrences of identical candidate list and generally distinctive identifiers (which may be based upon variants and/or hash keys to enable "fuzzy logic"-like capabilities) in the stored data, resulting in an empty candidate list in step 94. Given the empty candidate list, no identifiers corresponding with the candidate list would be retrieved in step 96, no confidence indicators would be created, and therefore no likeness matches would occur. As such, the system would assign a new persistent key to the Conjoined Data record one and add the record to the database in step 98.

[0042] As further illustrated in FIGURE 6, the same process would occur when Conjoined Data record two is received in the Repository in step 100, such as emanating from Company BBB, Dining system, record 0486 in the dining system (or BBB-Din-0486). The system would retrieve all occurrences of identical candidate list and generally distinctive identifiers in the stored data, identifying the same phone number (along with the persistent key) to be added to the candidate list in step 102. The system retrieves all identifiers corresponding to the candidate list, resulting in the data corresponding with the first record being retrieved in step 104. Based solely on a matched phone number, the system would create a relationship confidence indicator (such as indicating that the two individuals are roommates), but the telephone number match would not indicate a high confidence likeness match absent additional information confirming the likeness, such as

same name or social security number. As such, without a likeness confidence indicator indicating a match, the system would assign the Conjoined Data record two a new persistent key and add the record to the database in step 106.

[0043] As further illustrated in FIGURE 7, upon receipt of a Conjoined Data record three in step 108, such as emanating from company CCC, car rental system, record 0356 in the car rental system (or CCC-Car-0356), the system would retrieve all occurrences of identical candidate list and generally distinctive identifiers in the stored data, resulting in a candidate list identifying the social security number from Conjoined Data record one (along with the persistent key of Conjoined Data record one) and driver's license number from Conjoined Data record two (along with the persistent key of Conjoined Data record two) in step 110. The system would then retrieve all identifiers corresponding with the candidate list showing all identifiers from the two previously stored records in step 112. The system could then create confidence indicators based upon Conjoined Data record three and the retrieved data enabling likeness confidence indicators to be created indicating a match. Based upon the likeness matches, the system would assign the same persistent key to all of the records and add the Conjoined Data record three to the database in step 114. Sometimes, the prior persistent key corresponding with Conjoined Data record two, PK: 00000002, would be saved with a reference to the new persistent key, PK: 00000001, in order for the system to recognize at a later time that persistent key PK: 00000002 has since been changed to persistent key PK: 00000001.

[0044] Furthermore, as illustrated on FIGURE 2, the Conjoined Data and any resulting relations and/or matches will be stored in step 116 and a series of messages, sent based upon user-defined rules in step 118, such as: (i) on a set interval basis, (ii) sometimes including a message that is merely noise to minimize a traffic analysis attack, and/or (iii) with

respect to the true messages, identifying Protected Attribution Data from matched data. For example, relevant parties may be given the Protected Attribution Data (e.g., AAA-Res-0021, BBB-Din-0486 and/or CCC-Car-0356) which may be deciphered, although not the original data corresponding with the Attribution Data (which is unknown to the Repository), thus enabling such organization to request or share specific records corresponding with the Attribution Data from or with other relevant parties. By way of further example, in circumstances when a match or relation has not been determined within the intervals, a message of noise will be sent. Appropriate procedures would be established to maintain the confidentiality and security of the underlying Attribution Data.

[0045] From the foregoing, it will be observed that numerous variations and modifications may be effected without departing from the spirit and scope of the invention. It is to be understood that no limitation with respect to the specific apparatus illustrated herein is intended or should be inferred. It is, of course, intended to cover by the appended claims all such modifications as fall within the scope of the claims.

WHAT IS CLAIMED IS:

1. A method for processing data comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding to an entity;

utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record to form a processed record;

comparing the processed record to previously stored data; a

matching the processed record with the previously stored data that is determined to reflect the entity, the previously stored data that is determined to reflect the entity comprising at least a portion of at least two previously received records.

2. The method of claim 1 further comprising the step of one of assigning and identifying a source to the record.

3. The method of claim 2 further comprising the step of deciphering at least a portion of the processed record after the step of matching the processed record with the previously stored data that is determined to reflect the entity.

4. The method of claim 3 wherein the deciphered at least a portion of the processed record is the source.

5. The method of claim 1 further comprising the step of adding salt to the record.

6. The method of claim 1 further comprising receiving a plurality of received records.

7. The method of claim 1 further comprising the step of analyzing the record prior to the step of utilizing the cryptographic algorithm to process at least a portion of the record.

8. The method of claim 7 wherein the step of analyzing the record includes comparing at least one of the plurality of identifiers against one of:

a user-defined criterion; and

a data set in one of a secondary database and a list.

9. The method of claim 8 further comprising the step of enhancing the record.

10. The method of claim 9 wherein the step of enhancing the record includes formatting the at least one of the plurality of identifiers in accordance with a user-defined standard.

11. The method of claim 9 wherein the step of enhancing the record includes generating a variant to the at least one of the plurality of identifiers and including the variant with the record.

12. The method of claim 9 wherein the step of enhancing the record includes:

querying the data set for a secondary identifier relating to the record; and

supplementing the record with the secondary identifier.

13. The method of claim 1 further comprising the step of converting the record into a standardized message format.

14. The method of claim 13 wherein the step of converting the record into a standardized message format includes the step of utilizing a type indicator corresponding with each of the plurality of identifiers.

15. The method of claim 14 wherein the type indicator is discernable after the step of utilizing the cryptographic algorithm.

16. The method of claim 1 wherein the step of matching the processed record with the previously stored data that is determined to reflect the entity includes the steps of:

retrieving the previously stored data having at least one of the plurality of identifiers;

evaluating whether another identifier is included in the processed record that is not included in the previously stored data having the at least one of the plurality of identifiers; and

analyzing the previously stored data having the at least one of the plurality of identifiers for a match to the processed record based on the another identifier.

17. The method of claim 16 wherein the step of matching the processed record further comprises the step of retrieving a secondary previously stored data having the another identifier and including the secondary previously stored data with the previously stored data having the at least one of plurality of identifiers.

18. The method of claim 1 wherein the step of matching the processed record with the previously stored data that is determined to reflect the entity includes the step of assigning a persistent key associated with at least a portion of the previously stored data that is determined to reflect the entity to the matched processed record.

19. The method of claim 2 further comprising the step of issuing a message based upon a user-defined rule.

20. The method of claim 19 wherein the message includes one of the source of the record and at least one source of the previously stored data.

21. The method of claim 19 wherein the step of issuing a message based upon a user-defined rule includes the step of issuing a message in user-defined intervals.

22. The method of claim 1 further comprising the step of storing the processed record in a database.

23. A method for processing data comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding to an entity;

utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record to form a processed record;

comparing the processed record to previously stored data;

determining matched data by matching the processed record with the previously stored data that is determined to reflect the entity based upon the plurality of identifiers;

analyzing whether another identifier is included in the processed record that is not included in the previously stored data that is determined to reflect the entity based upon the plurality of identifiers; and

matching the matched data with the previously stored data that is determined to reflect the entity based upon the another identifier.

24. The method of claim 23 further comprising the step of one of assigning and identifying a source to the record.

25. The method of claim 24 further comprising the step of deciphering at least a portion of the processed record after the step of matching the matched data.

26. The method of claim 25 wherein the deciphered at least a portion of the processed record is the source.

27. The method of claim 23 further comprising the step of adding salt to the record.

28. The method of claim 23 wherein the received record comprises a plurality of received records.

29. The method of claim 23 further comprising the step of analyzing the record prior to the step of utilizing the cryptographic algorithm to process at least a portion of the record.

30. The method of claim 29 wherein the step of analyzing the record includes the step of comparing at least one of the plurality of identifiers against one of:

a user-defined criterion and

a data set in one of a secondary database and a list.

31. The method of claim 30 further comprising the step of enhancing the record.

32. The method of claim 31 wherein the step of enhancing the record includes formatting the at least one of the plurality of identifiers in accordance with a user-defined standard.

33. The method of claim 31 wherein the step of enhancing the record includes generating a variant to the at least one of the plurality of identifiers and including the variant with the record.

34. The method of claim 31 wherein the step of enhancing the record includes:

querying the data set for a secondary identifier relating to the record; and

supplementing the record with the secondary identifier.

35. The method of claim 23 further comprising the step of converting the record into a standardized message format.

36. The method of claim 35 wherein the step of converting the record into a standardized message format includes the step of utilizing a type indicator corresponding with each of the plurality of identifiers.

37. The method of claim 36 wherein the type indicator is discernable after the step of utilizing the cryptographic algorithm.

38. The method of claim 23 wherein the step of matching the matched data includes the step of assigning a persistent key associated with at least a portion of the previously stored data that is determined to reflect the entity to the processed record.

39. The method of claim 24 further comprising the step of issuing a message based upon a user-defined rule.

40. The method of claim 39 wherein the message includes one of the source of the record and at least one source of the previously stored data.

41. The method of claim 40 wherein the step of issuing a message based upon a user-defined rule includes the step of issuing a message in user-defined intervals.

42. The method of claim 23 further comprising the step of storing the processed record in a database.

43. A method for processing data comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding to an entity;

utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record to form a processed record;

comparing the processed record to previously stored data; and

associating the processed record with the previously stored data that is determined to reflect a relationship with the entity.

44. The method of claim 43 further comprising the step of one of assigning and identifying a source to the record.

45. The method of claim 44 further comprising the step of deciphering at least a portion of the processed record after the step of associating the processed record with the previously stored data that is determined to reflect a relationship with the entity.

46. The method of claim 45 wherein the deciphered at least a portion of the processed record is the source.

47. The method of claim 43 further comprising the step of adding salt to the record.

48. The method of claim 43 wherein the received record comprises a plurality of received records.

49. The method of claim 43 wherein the previously stored data that is determined to reflect the relationship with the entity comprises at least a portion of two previously received records.

50. The method of claim 43 further comprising the step of analyzing the record prior to the step of utilizing the cryptographic algorithm to process at least two of the plurality of identifiers in the record.

51. The method of claim 50 wherein the step of analyzing the record includes comparing at least one of the plurality of identifiers against one of:

a user-defined criterion; and

a data set in one of a secondary database and a list.

52. The method of claim 51 further comprising the step of enhancing the record.

53. The method of claim 52 wherein the step of enhancing the record includes formatting the at least one of the plurality of identifiers in accordance with a user-defined standard.

54. The method of claim 52 wherein the step of enhancing the record includes generating a variant to the at least one of the plurality of identifiers and including the variant with the record.

55. The method of claim 52 wherein the step of enhancing the record includes:

querying the data set for a secondary identifier relating to the record; and

supplementing the record with the secondary identifier.

56. The method of claim 43 further comprising the step of converting the record into a standardized message format.

57. The method of claim 56 wherein the step of converting the record into a standardized message format includes the step of utilizing a type indicator corresponding with each of the plurality of identifiers.

58. The method of claim 57 wherein the type indicator is discernable after the step of utilizing the cryptographic algorithm.

59. The method of claim 44 further comprising the step of issuing a message based upon a user-defined rule.

60. The method of claim 59 wherein the message includes one of the source of the record and the source of the previously stored data.

61. The method of claim 59 wherein the step of issuing the message based upon the user-defined rule includes the step of issuing a message in user-defined intervals.

62. The method of claim 43 further comprising the step of storing the processed record in a database.

63. The method of claim 43 further comprising the step of storing the relationships with the entity in a database.

64. A method for processing data comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding with an entity and at least one of the plurality of identifiers having previously been processed utilizing a cryptographic algorithm;

comparing the record to previously stored data, at least a portion of the previously stored data having previously been processed utilizing the cryptographic algorithm;

matching the record with the previously stored data that is determined to reflect the entity; and

issuing a plurality of messages wherein at least one of the plurality of messages is noise.

65. The method of claim 64 wherein the step of issuing a plurality of messages occurs in user-defined intervals.

66. The method of claim 64 wherein at least one of the plurality of messages includes a source of the record.

67. The method of claim 64 further comprising the step of storing the record in a database.

68. A method for processing data comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding with an entity and at least one of the plurality of identifiers having previously been processed utilizing a cryptographic algorithm;

comparing the record to previously stored data, at least a portion of the previously stored data having previously been processed utilizing the cryptographic algorithm;

associating the record with the previously stored data that is determined to reflect a relationship with the entity; and

issuing a plurality of messages wherein at least one of the plurality of messages is noise.

69. The method of claim 68 wherein the step of issuing a plurality of messages occurs in user-defined intervals.

70. The method of claim 68 wherein at least one of the plurality of messages includes a source of the record.

71. The method of claim 68 further comprising the step of storing the record in a database.

72. The method of claim 68 further comprising the step of storing the relationships with the entity in a database.

73. For a system for processing data and a computer readable medium containing program instructions for execution by a computer for performing the method comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding to an entity;

utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record to form a processed record;

comparing the processed record to previously stored data; and

matching the processed record with the previously stored data that is determined to reflect the entity, the previously stored data that is determined to reflect the entity comprising at least a portion of at least two previously received records.

74. The computer readable medium for performing the method of claim 73 further comprising the step of one of assigning and identifying a source to the record.

75. The computer readable medium for performing the method of claim 74 further comprising the step of deciphering at least a portion of the processed record after the step of matching the processed record with the previously stored data that is determined to reflect the entity.

76. The computer readable medium for performing the method of claim 75 wherein the deciphered at least a portion of the processed record is the source.

77. The computer readable medium for performing the method of claim 73 further comprising the step of adding salt to the record.

78. The computer readable medium for performing the method of claim 73 further comprising receiving a plurality of received records.

79. The computer readable medium for performing the method of claim 73 further comprising the step of analyzing the record prior to the step of utilizing the cryptographic algorithm to process at least a portion of the record.

80. The computer readable medium for performing the method of claim 79 wherein the step of analyzing the record includes comparing at least one of the plurality of identifiers against one of:

a user-defined criterion; and

a data set in one of a secondary database and a list.

81. The computer readable medium for performing the method of claim 80 further comprising the step of enhancing the record.

82. The computer readable medium for performing the method of claim 81 wherein the step of enhancing the record includes formatting the at least one of the plurality of identifiers in accordance with a user-defined standard.

83. The computer readable medium for performing the method of claim 81 wherein the step of enhancing the record includes generating a variant to the at least one of the plurality of identifiers and including the variant with the record.

84. The computer readable medium for performing the method of claim 81 wherein the step of enhancing the record includes:

querying the data set for a secondary identifier relating to the record; and

supplementing the record with the secondary identifier.

85. The computer readable medium for performing the method of claim 73 further comprising the step of converting the record into a standardized message format.

86. The computer readable medium for performing the method of claim 85 wherein the step of converting the record into a standardized message format includes the step of utilizing a type indicator corresponding with each of the plurality of identifiers.

87. The computer readable medium for performing the method of claim 86 wherein the type indicator is discernable after the step of utilizing the cryptographic algorithm.

88. The computer readable medium for performing the method of claim 73 wherein the step of matching the processed record with the previously stored data that is determined to reflect the entity includes the steps of:

retrieving the previously stored data having at least one of the plurality of identifiers;

evaluating whether another identifier is included in the processed record that is not included in the previously stored data having the at least one of the plurality of identifiers; and

analyzing the previously stored data having the at least one of the plurality of identifiers for a match to the processed record based on the another identifier.

89. The computer readable medium for performing the method of claim 88 wherein the step of matching the processed record further comprises the step of retrieving a secondary previously stored data having the another identifier and including the secondary previously stored data with the previously stored data having the at least one of plurality of identifiers.

90. The computer readable medium for performing the method of claim 73 wherein the step of matching the processed record with the previously stored data that is determined to reflect the entity includes the step of assigning a persistent key associated with at least a portion of the previously stored data that is determined to reflect the entity to the matched processed record.

91. The computer readable medium for performing the method of claim 74 further comprising the step of issuing a message based upon a user-defined rule.

92. The computer readable medium for performing the method of claim 91 wherein the message includes one of the source of the record and at least one source of the previously stored data.

93. The computer readable medium for performing the method of claim 91 wherein the step of issuing a message based upon a user-defined rule includes the step of issuing a message in user-defined intervals.

94. The computer readable medium for performing the method of claim 73 further comprising the step of storing the processed record in a database.

95. For a system for processing data and a computer readable medium containing program instructions for execution by a computer for performing the method comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding to an entity;

utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record to form a processed record;

comparing the processed record to previously stored data;

determining matched data by matching the processed record with the previously stored data that is determined to reflect the entity based upon the plurality of identifiers;

analyzing whether another identifier is included in the processed record that is not included in the previously stored data that is determined to reflect the entity based upon the plurality of identifiers; and

matching the matched data with the previously stored data that is determined to reflect the entity based upon the another identifier.

96. The computer readable medium for performing the method of claim 95 further comprising the step of one of assigning and identifying a source to the record.

97. The computer readable medium for performing the method of claim 96 further comprising the step of deciphering at least a portion of the processed record after the step of matching the matched data

98. The computer readable medium for performing the method of claim 97 wherein the deciphered at least a portion of the processed record is the source.

99. The computer readable medium for performing the method of claim 95 further comprising the step of adding salt to the record.

100. The computer readable medium for performing the method of claim 95 wherein the received record comprises a plurality of received records.

101. The computer readable medium for performing the method of claim 95 further comprising the step of analyzing the record prior to the step of utilizing the cryptographic algorithm to process at least a portion of the record.

102. The computer readable medium for performing the method of claim 101 wherein the step of analyzing the record includes the step of comparing at least one of the plurality of identifiers against one of:

a user-defined criterion and

a data set in one of a secondary database and a list.

103. The computer readable medium for performing the method of claim 102 further comprising the step of enhancing the record.

104. The computer readable medium for performing the method of claim 103 wherein the step of enhancing the record includes formatting the at least one of the plurality of identifiers in accordance with a user-defined standard.

105. The computer readable medium for performing the method of claim 103 wherein the step of enhancing the record includes generating a variant to the at least one of the plurality of identifiers and including the variant with the record.

106. The computer readable medium for performing the method of claim 103 wherein the step of enhancing the record includes:

querying the data set for a secondary identifier relating to the record; and

supplementing the record with the secondary identifier.

107. The computer readable medium for performing the method of claim 95 further comprising the step of converting the record into a standardized message format.

108. The computer readable medium for performing the method of claim 107 wherein the step of converting the record into a standardized message format includes the step of utilizing a type indicator corresponding with each of the plurality of identifiers.

109. The computer readable medium for performing the method of claim 108 wherein the type indicator is discernable after the step of utilizing the cryptographic algorithm.

110. The computer readable medium for performing the method of claim 95 wherein the step of matching the matched data includes the step of assigning a persistent key associated with at least a portion of the previously stored data that is determined to reflect the entity to the processed record.

111. The computer readable medium for performing the method of claim 96 further comprising the step of issuing a message based upon a user-defined rule.

112. The computer readable medium for performing the method of claim 111 wherein the message includes one of the source of the record and at least one source of the previously stored data.

113. The computer readable medium for performing the method of claim 112 wherein the step of issuing a message based upon a user-defined rule includes the step of issuing a message in user-defined intervals.

114. The computer readable medium for performing the method of claim 95 further comprising the step of storing the processed record in a database.

115. For a system for processing data and a computer readable medium containing program instructions for execution by a computer for performing the method comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding to an entity;

utilizing a cryptographic algorithm to process at least two of the plurality of identifiers in the record to form a processed record;

comparing the processed record to previously stored data; and

associating the processed record with the previously stored data that is determined to reflect a relationship with the entity.

116. The computer readable medium for performing the method of claim 115 further comprising the step of one of assigning and identifying a source to the record.

117. The computer readable medium for performing the method of claim 116 further comprising the step of deciphering at least a portion of the processed record after the step of associating the processed record with the previously stored data that is determined to reflect a relationship with the entity.

118. The computer readable medium for performing the method of claim 117 wherein the deciphered at least a portion of the processed record is the source.

119. The computer readable medium for performing the method of claim 115 further comprising the step of adding salt to the record.

120. The computer readable medium for performing the method of claim 115 wherein the received record comprises a plurality of received records.

121. The computer readable medium for performing the method of claim 115 wherein the previously stored data that is determined to reflect the relationship with the entity comprises at least a portion of two previously received records.

122. The computer readable medium for performing the method of claim 115 further comprising the step of analyzing the record prior to the step of utilizing the cryptographic algorithm to process at least two of the plurality of identifiers in the record.

123. The computer readable medium for performing the method of claim 122 wherein the step of analyzing the record includes comparing at least one of the plurality of identifiers against one of:

a user-defined criterion; and

a data set in one of a secondary database and a list.

124. The computer readable medium for performing the method of claim 123 further comprising the step of enhancing the record.

125. The computer readable medium for performing the method of claim 124 wherein the step of enhancing the record includes formatting the at least one of the plurality of identifiers in accordance with a user-defined standard.

126. The computer readable medium for performing the method of claim 124 wherein the step of enhancing the record includes generating a variant to the at least one of the plurality of identifiers and including the variant with the record.

127. The computer readable medium for performing the method of claim 124 wherein the step of enhancing the record includes:

querying the data set for a secondary identifier relating to the record; and

supplementing the record with the secondary identifier.

128. The computer readable medium for performing the method of claim 115 further comprising the step of converting the record into a standardized message format.

129. The computer readable medium for performing the method of claim 128 wherein the step of converting the record into a standardized message format includes the step of utilizing a type indicator corresponding with each of the plurality of identifiers.

130. The computer readable medium for performing the method of claim 129 wherein the type indicator is discernable after the step of utilizing the cryptographic algorithm.

131. The computer readable medium for performing the method of claim 116 further comprising the step of issuing a message based upon a user-defined rule.

132. The computer readable medium for performing the method of claim 131 wherein the message includes one of the source of the record and the source of the previously stored data.

133. The computer readable medium for performing the method of claim 131 wherein the step of issuing the message based upon the user-defined rule includes the step of issuing a message in user-defined intervals.

134. The computer readable medium for performing the method of claim 115 further comprising the step of storing the processed record in a database.

135. The computer readable medium for performing the method of claim 115 further comprising the step of storing the relationships with the entity in a database.

136. For a system for processing data and a computer readable medium containing program instructions for execution by a computer for performing the method comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding with an entity and at least one of the plurality of identifiers having previously been processed utilizing a cryptographic algorithm;

comparing the record to previously stored data, at least a portion of the previously stored data having previously been processed utilizing the cryptographic algorithm;

matching the record with the previously stored data that is determined to reflect the entity; and

issuing a plurality of messages wherein at least one of the plurality of messages is noise.

137. The computer readable medium for performing the method of claim 136 wherein the step of issuing a plurality of messages occurs in user-defined intervals.

138. The computer readable medium for performing the method of claim 136 wherein at least one of the plurality of messages includes a source of the record.

139. The computer readable medium for performing the method of claim 136 further comprising the step of storing the record in a database.

140. For a system for processing data and a computer readable medium containing program instructions for execution by a computer for performing the method comprising the steps of:

receiving a record having a plurality of identifiers, the record corresponding with an entity and at least one of the plurality of identifiers having previously been processed utilizing a cryptographic algorithm;

comparing the record to previously stored data, at least a portion of the previously stored data having previously been processed utilizing the cryptographic algorithm;

associating the record with the previously stored data that is determined to reflect a relationship with the entity; and

issuing a plurality of messages wherein at least one of the plurality of messages is noise.

141. The computer readable medium for performing the method of claim 140 wherein the step of issuing a plurality of messages occurs in user-defined intervals.

142. The computer readable medium for performing the method of claim 140 wherein at least one of the plurality of messages includes a source of the record.

143. The computer readable medium for performing the method of claim 140 further comprising the step of storing the record in a database.

144. The computer readable medium for performing the method of claim 140 further comprising the step of storing the relationships with the entity in a database.

Figure 1

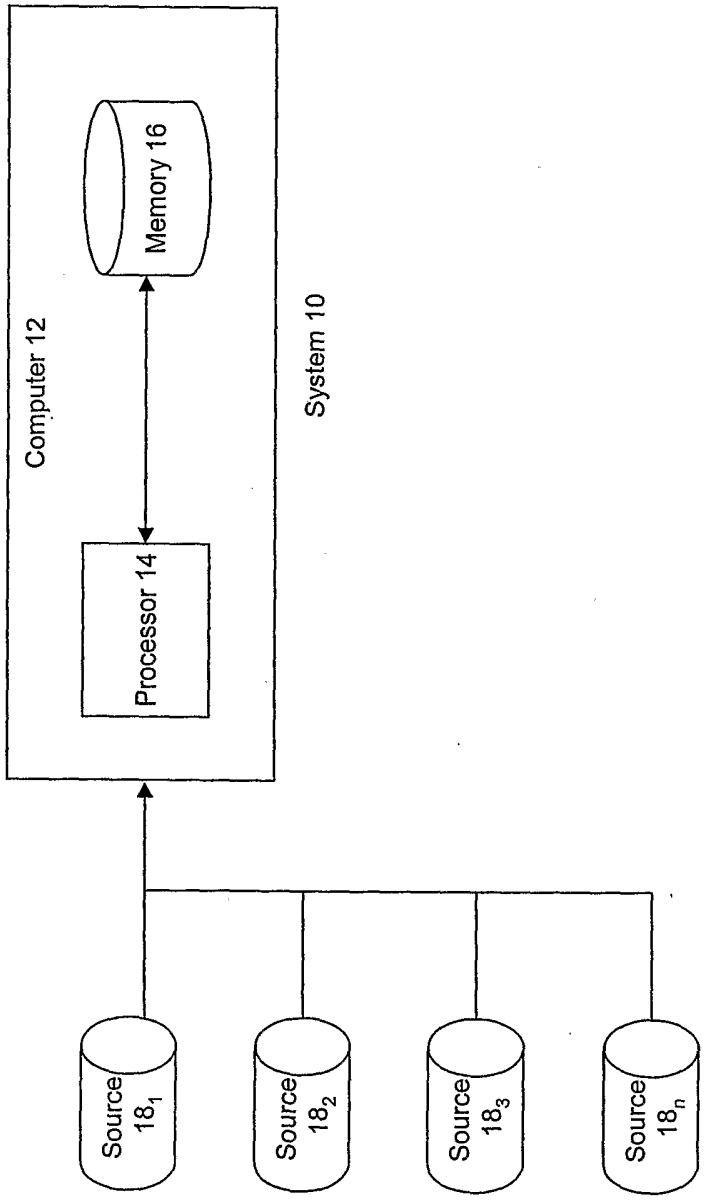

Memory 16
Computer 12
System 10
Processor 14
Source 18$_1$
Source 18$_2$
Source 18$_3$
Source 18$_n$

Figure 2 – Receive and Process Received Record

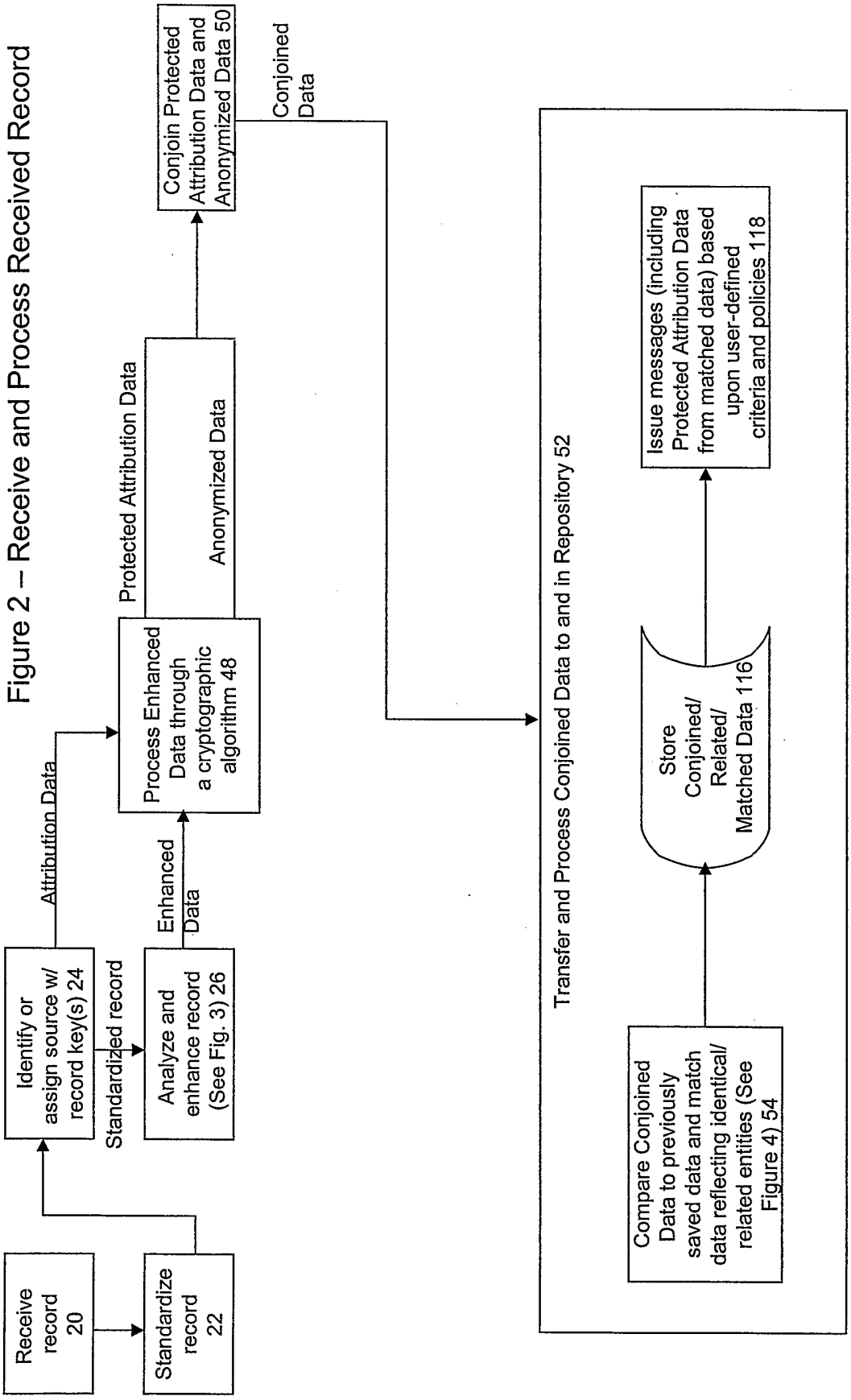


Figure 3 – Analyze and Enhance Record 26

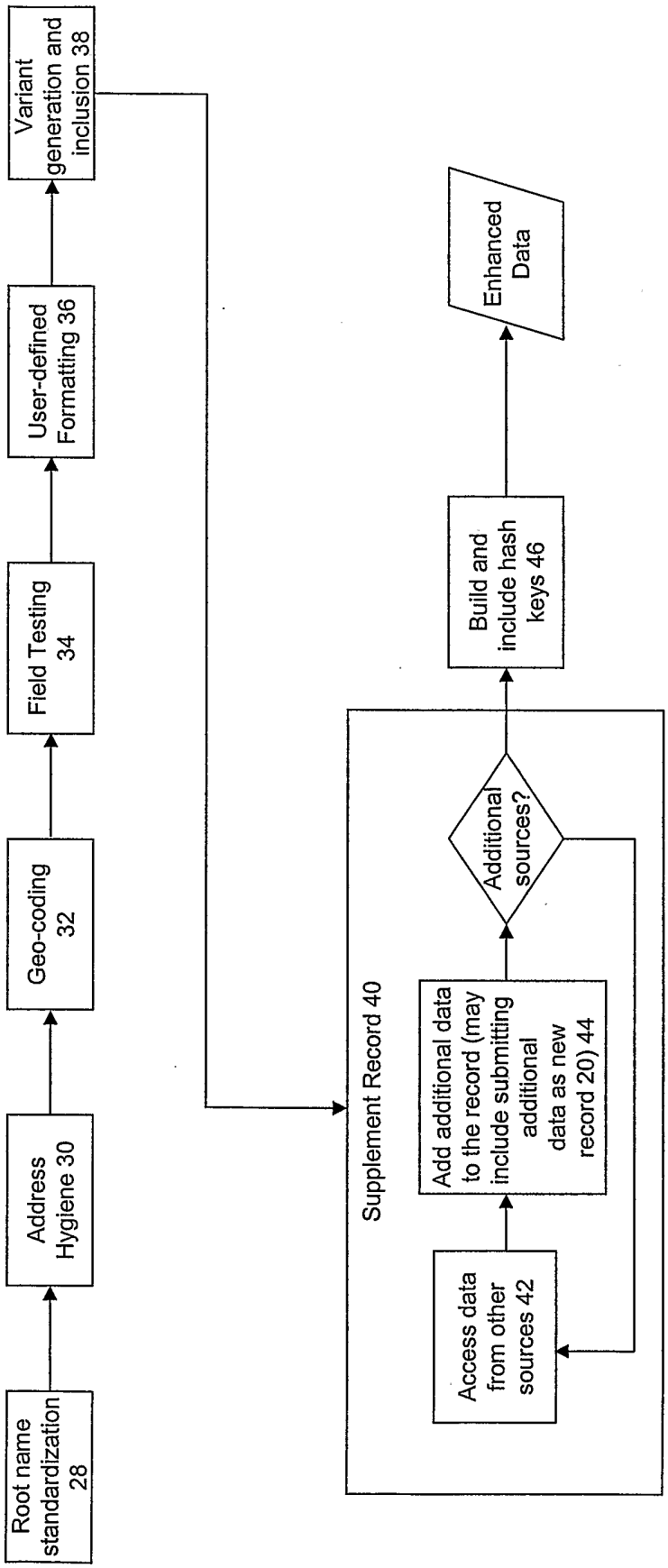


Figure 4 – Compare Conjoined Data to Previously Stored Data 58

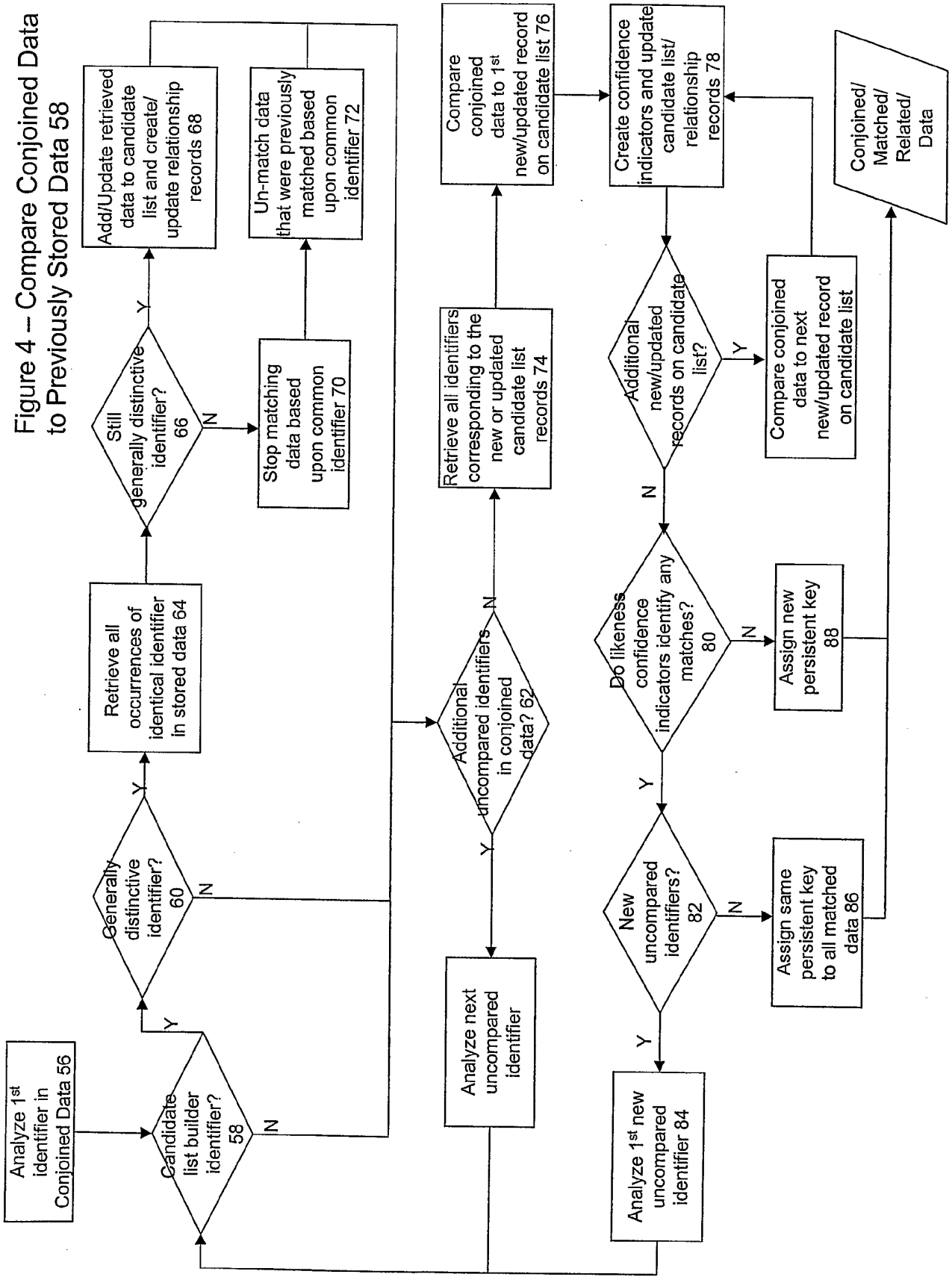
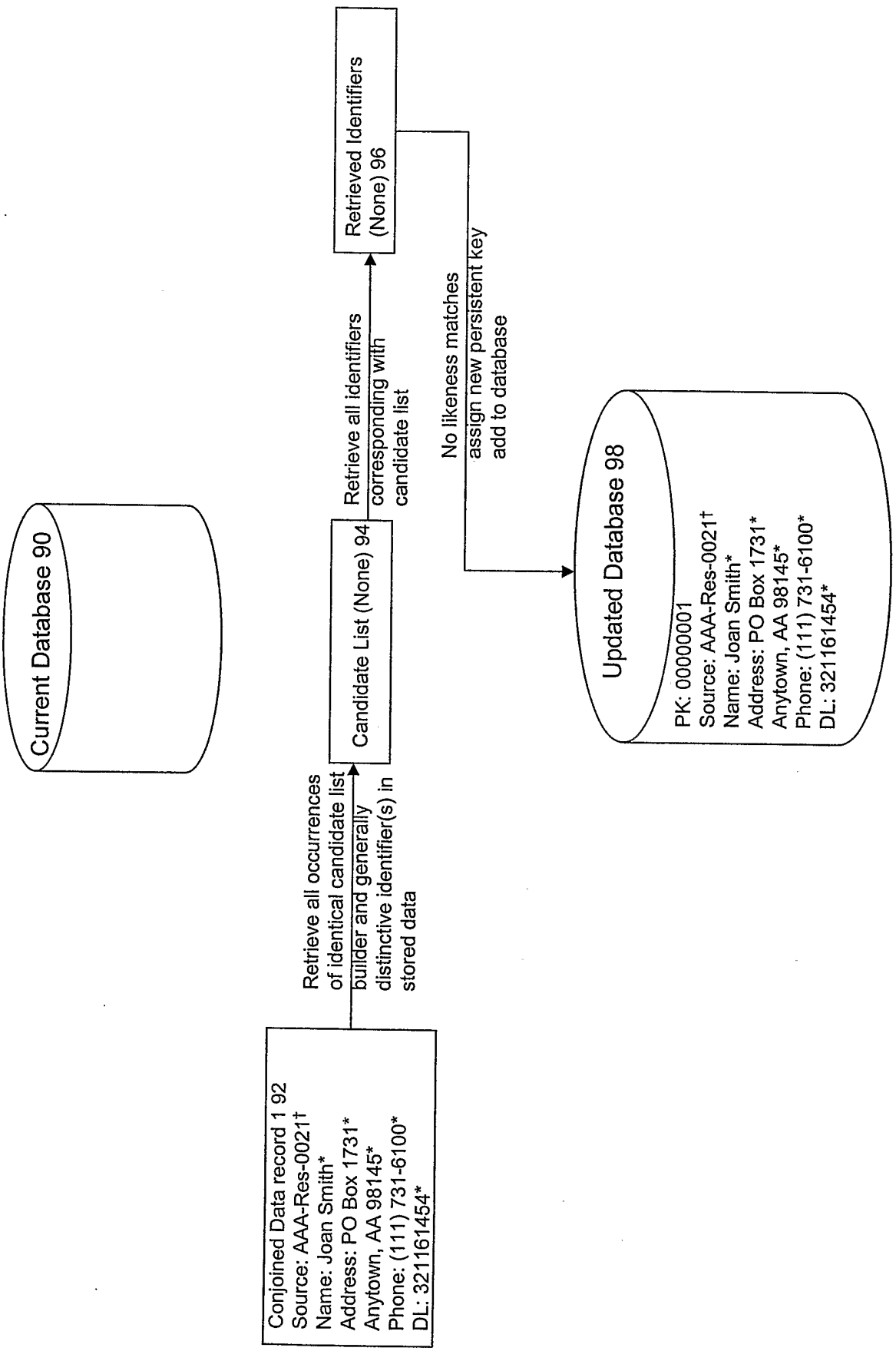
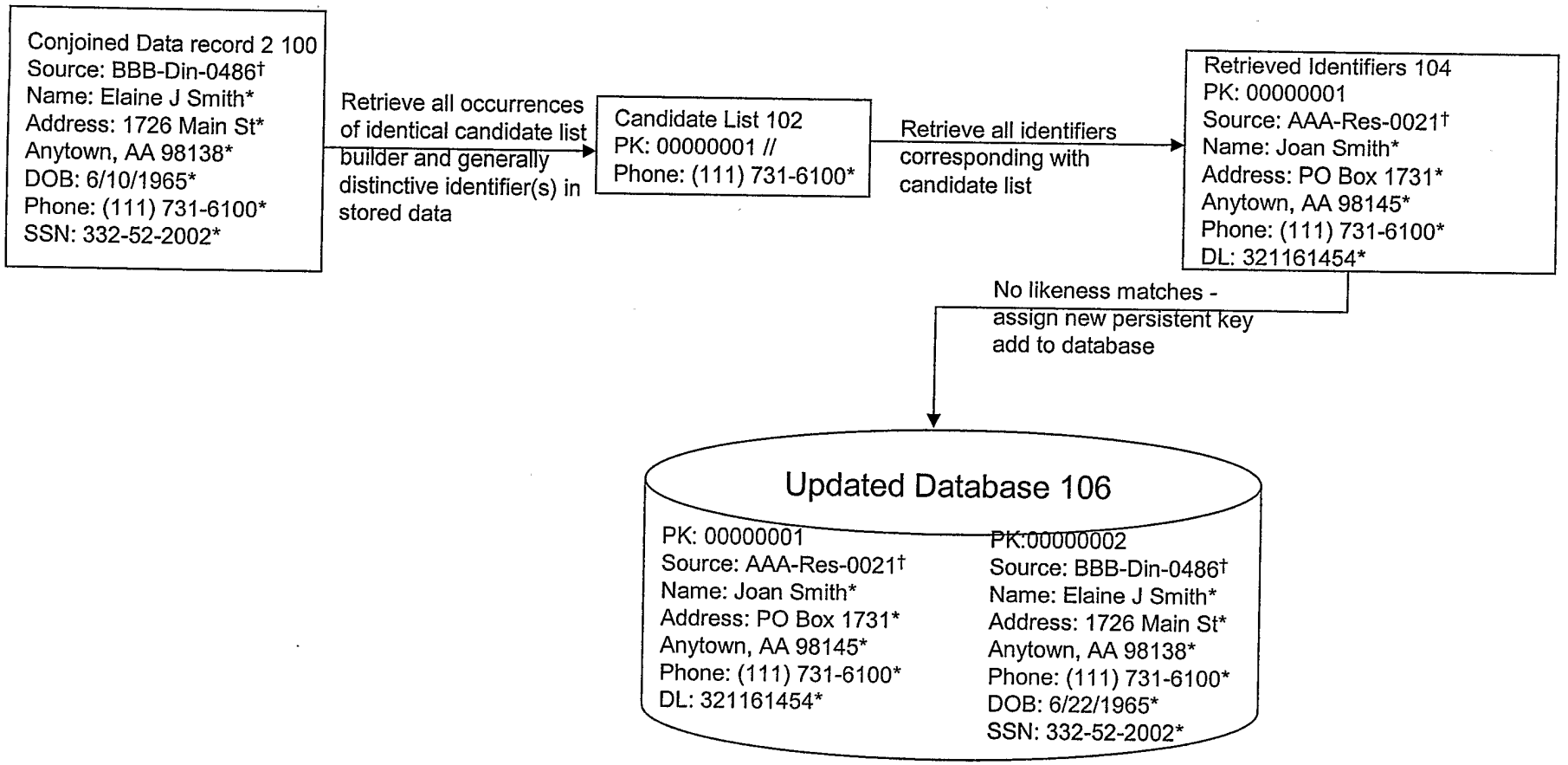


Figure 5 – Initial Record



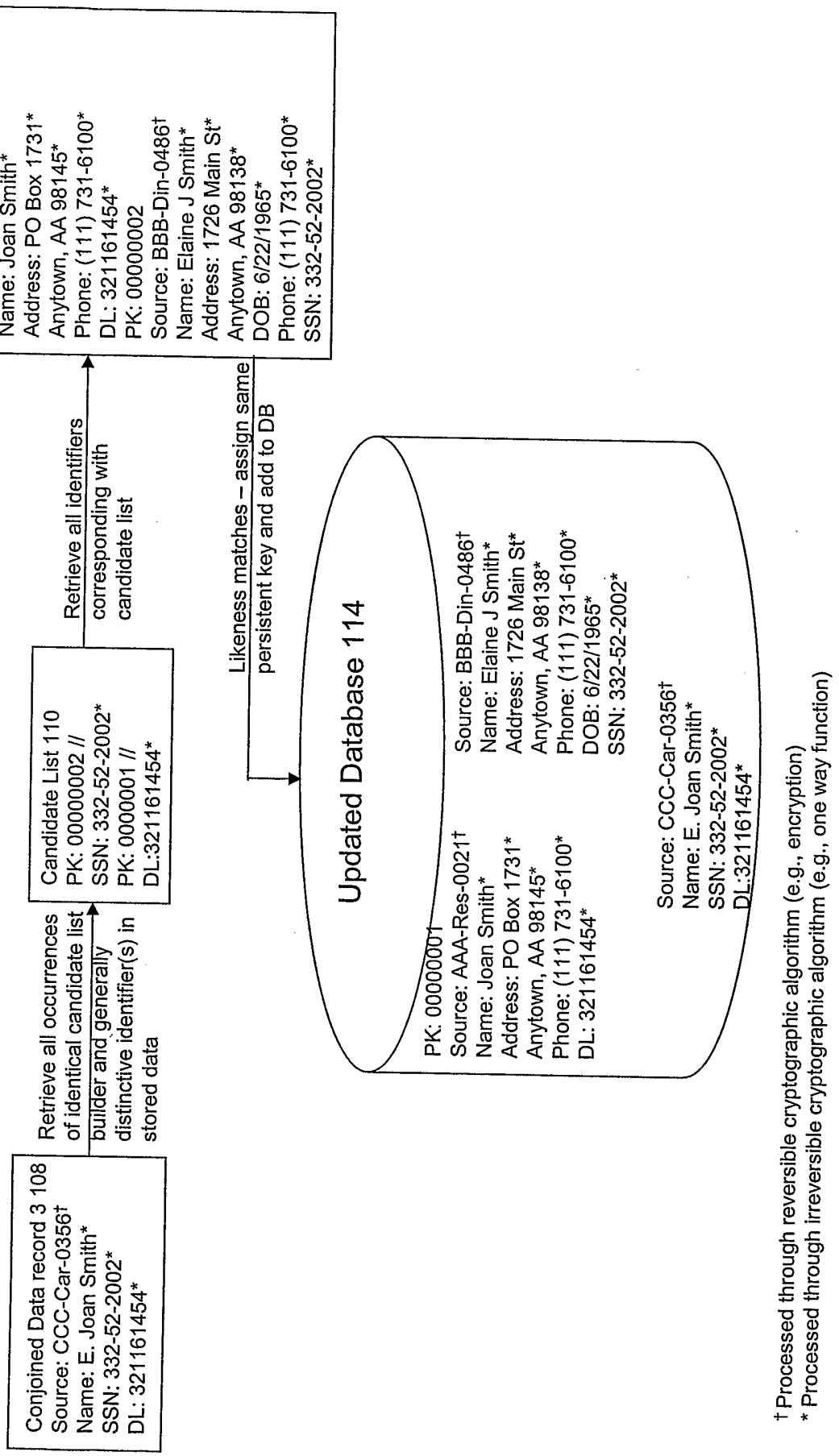
† Processed through reversible cryptographic algorithm (e.g., encryption)
* Processed through irreversible cryptographic algorithm (e.g., one way function)

Figure 6 – Subsequent Record



† Processed through reversible cryptographic algorithm (e.g., encryption)
* Processed through irreversible cryptographic algorithm (e.g., one way function)

Figure 7 – Third Record



† Processed through reversible cryptographic algorithm (e.g., encryption)
* Processed through irreversible cryptographic algorithm (e.g., one way function)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US03/35607

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04K 1/00; H04L 9/00, 9/32; G06F 11/30, 12/14

US CL : 713/185, 202

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)

U.S. : 713/185, 202

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)

Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,446,210 B1 (BORZA) 03 September 2002 (03.09.2002), column 2, lines 13 to column 3, line 23; column 7, lines 7-44; column 8, lines 28-38; column 11, lines 43-55; column 11, line 65 to column 12, line 48.	1-63; 73-135 ---------- 64-72; 136-144
Y	US 6,317,834 B1 (GENNARO et al.) 13 November 2001 (13.11.2001), column 2, line 28 to column 3, line 3; column 8, lines 8-48; column 9, line 47 to column 10, line 35.	64-72; 136-144
A,T	US 6,697,947 B1 (MATYAS, JR. et al.) 24 February 2004 (24.02.2004), column 1, line 39 to column 5, line 3.	1-144
A	US 5,991,408 A (PEARSON et al.) 23 November 1999 (23.11.1999), column 1, line 55 to column 5, line 9.	1-144
A	US 6,076,167 A (BORZA) 13 June 2000 (13.06.2000), column 2, line 10 to column 3, line 18.	1-144
A	US 5,534,855 A (SHOCKLEY et al.) 09 July 1996 (09.06.1996), column 3, line 13 to column 4, line 41.	1-144
A	US 6,167,517 A (GILCHRIST et al.) 26 December 2000 (26.12.2000), column 2, line 25 to column 3, line 7.	1-144
A	US 6,041,410 A (HSU et al.) 21 March 2000 (21.03.2000), column 1, line 51 to column 3, line 58.	1-144

☒ Further documents are listed in the continuation of Box C. ☐ 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 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

13 April 2004 (13.04.2004)

Date of mailing of the international search report

23 APR 2004

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Facsimile No. (703)305-3230

Authorized officer

Michelle L. Eason
for
Ayaz Sheikh

Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

PCT/US03/35607

INTERNATIONAL SEARCH REPORT

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,092,199 A (DUTCHER et al.) 18 July 2000 (18.07.2000), column 2, line 26 to column 3, line 13.	1-144
A	US 6,058,477 A (KUSAKABE et al.) 02 May 2000 (02.05.2000), column 1, line 66 to column 5, line 42.	1-144
A	US 5,784,464 A (AKIYAMA et al.) 21 July 1998 (21.07.1998), column 2, line 11 to column 4, line 47.	1-144
A	US 5,229,764 A (MATCHETT et al.) 20 July 1993 (20.07.1993), column 3, lines 10-57.	1-144
A	US 6,160,903 A (HAMID et al.) 12 December 2000 (12.12.2000), column 4, line 3 to column 5, line 13.	1-144

Continuation of B. FIELDS SEARCHED Item 3:
EAST, IEEE, ACM
search terms: user authentication; biometric authorization, comparing encrypted