METHOD AND APPARATUS FOR PROVIDING UNIQUE PER-COPY DIGITAL WATERMARKS

CROSS-REFERENCE TO RELATED APPLICATIONS


This application also claims the benefit of U.S. Nonprovisional Application Serial Number 13/069,036, “The Knowledge Transfer Tool: an Apparatus and Method for Knowledge Transfer”, filed 3/22/2011 by the present inventor, which is incorporated herein by reference. This application also claims the benefit of U.S. Nonprovisional Application Serial No. 13/307,695, “Method and Apparatus for Electronic Literary Macrame Component Referencing”, filed 3/22/2011 by the present inventor, also incorporated herein by reference.

FIELD OF THE INVENTION

1
This disclosure relates to the creation of texts readable on electronic displays, and more specifically to the creation of interconnected narratives and references readable using browser programs such as those adapted for use on the World Wide Web.

BACKGROUND OF THE INVENTION

Digital documents and records of all kinds suffer from certain disadvantages when compared to physical documents, stemming from the fact that they can be copied indiscriminately and undetectably regardless of copyright. Many copy-protection attempts have been made to overcome or at least offset these disadvantages. Most or all of these attempts have incurred new disadvantages, such as rejection by purchasers due to complexity and unreliability of the copy-protection software, or such as circumvention by skilled and unprincipled software analysts and developers. One consequence of confronting these disadvantages has been the increased attention to determining a document’s provenance, which appears to be a much-easier task.

Watermarking a document gives its holder a way to identify its provenance by embedding identifying information in a concealed form within the document in such a way as to make the concealed information available to those wishing to determine its source. Digital watermarking has become a conventional means of embedding and concealing identifying information in a digital document that compels considerable effort in its eradication, subversion, or replacement. Finding ways to increase the effort needed to subvert digital watermarks in digital documents would be desirable.

An electronic literary macramé, or ELM, is a tightly-linked and threaded form of electronic text, along with the software for building it. The concealment of sensitive texts, such as passages intended for mature readers only, answers to problems to be solved by students, and similar materials, is well served by encryption of their content. Encryption is also useful as a source of entertainment via the attraction of breaking the encryption of messages to reveal their content. Finally, and most importantly, encryption techniques may be used to enhance the value
of digital watermarks by making forgery or eradication more obvious to the producer of the watermark.

In the Web-enabled and network-enabled world, the continuing advent of increasing numbers of modes of communication, and increasing numbers of communication links within each mode, suggests the communication of cryptotext requiring at least two channels between the sender and the intended receiver. Assuming the availability of two or more channels for communication, at least one of which channels is known to be secure, eliminates the need for separate key management for at least portions of a cryptosystem. The availability of two or more channels can be considered a form of storage of information at two or more separate places. Here the term “channels” refers to a connection across time, space, or both time and space.

An ELM as published for its readers currently contains an embedded digital watermark produced when the ELM is synthesized, or compiled, from its textual and other components. See U.S. Patent No. 7,555,138, METHOD AND APPARATUS FOR DIGITAL WATERMARKING FOR THE ELECTRONIC LITERARY MACRAME”, a copy of which is incorporated herein by reference. The referenced form of watermark is stored in the published document only. “Secret-splitting”, also termed secret sharing, is a process well-known in the cryptographic art. For example, see U.S. Patent No. 7,606,769, “System and method for embedding user authentication information in encrypted data”, Yeung, et al. Secret-splitting, that is, the use of two or more separate places in which to conceal information along with a process for reconstituting said information, would constitute an improvement to the patented ELM invention, since any tampering with the watermark content in the published document would affect the appearance of any reconstitution of said watermark content with the unchanged watermark content in any other location.

SUMMARY OF THE INVENTION

The present method and apparatus provide a split embodiment of digital watermarks which contain literary information of interest to a reader of an electronic literary macramé
(ELM) or a knowledge transfer tool (KTT) document. The present method and apparatus change the nature of the watermark by an application of a simple form of “secret-sharing”: splitting the watermark content into two or more components, stored in separate repositories, which may be recombined to reproduce the original watermark content.

The present invention combines the ELM publishing process, the ELM watermarking process, the watermark-splitting process, a text-restoration process, and any of a wide range of electronic purchasing processes to customize a buyer’s copy of the ELM work at the time of purchase, embedding the buyer’s time/date/place of purchase, some dimensions of the buyer’s identity, and the ELM’s own per-work descriptive information into a form of per-copy watermark information. The proposed method and apparatus uses a secret-sharing technique to divide the per-copy watermark information into two or more shares, a first subset of which is furnished to the purchaser, a second and separate subset of which is furnished to the seller, and a third subset of which is furnished to a third party. The proposed method and apparatus also provides a means for recombining some or all subsets of the divided shares to extract and present the original per-copy watermark information for determination of provenance of both the work and the copy, or to extract and present other watermark information for other purposes.

DESCRIPTION OF DRAWINGS

Fig. 1 shows the derivation of multiple split files, using plain text or image files and a known watermark file, according to the present invention and stored in multiple separate locations.

Fig. 2 shows the reconstitution into a watermark of the multiple split files stored in multiple separate locations as shown in Fig. 1.

Fig. 3 shows an addition table for an alphabetic embodiment of the present invention.

Fig. 4 illustrates the derivation of a list of entries for a first addition result from the alphabetic addition table of Fig. 3.

Fig. 5 illustrates the use of the list of entries from Fig. 4 to select a sum from the list and separate the addends of the sum onto two separate outputs.
Fig. 6 illustrates the use of the table from Fig. 3 to combine the addends from the two separate outputs to reconstitute the original input as the sum.

Fig. 7 illustrates the use of the lists of entries from Figs. 4 and 6 to select sums from the lists and separate the addends of the sum onto three separate outputs.

Fig. 8 illustrates the reconstitution of the three separate output addends of Fig. 7 into the original sum using the table of Fig. 1.

Fig. 9 illustrates the derivation of an output comprising a first addend of a sum wherein a known second addend and the first addend sum to a known text.

Fig. 10 illustrates the reconstitution of the addends of Fig. 9 into the original sum.

Fig. 11 illustrates the derivation of a pair of output addends given a known sum and a known third addend.

Fig. 12 illustrates the reconstitution of the three addends of Fig. 11 into the original sum.

Fig. 13 shows a set of addition tables for a multiple-table alphabetic embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Given the existing ELM publishing process as presented in U.S. Patents __________ and __________, and the existing ELM watermarking method as presented in U.S. Patent No. 7,555,138, the present invention incorporates a digital text-splitting process to derive, incorporate, store, retrieve, and reconstitute one or more sets of watermark information in an electronic document such as an e-book as conventionally defined or an ELM or KTT as defined in the incorporated references.

The present method and apparatus provide a split embodiment of digital watermarks which contain literary information of interest to a reader of an electronic literary macramé (ELM) or a knowledge transfer tool (KTT) document. The present method and apparatus change the nature of the watermark by an application of a simple form of “secret-sharing”: splitting the watermark content into two or more components, stored in separate repositories, which may be
recombined to reproduce the original watermark content. The splitting of the watermark content is performed using a simple modular group operation applied with the use of a random or pseudorandom operand-pair-selection process which discards the random or pseudorandom value used. This process renders impossible the reconstruction of any split portion of the watermark content without access to all other split portions of the content.

The present method and apparatus provide a steganographic split embodiment of digital watermarks which introduces comprehensible components into the set of components split up and stored, thereby masking the use of the comprehensible components as components of the invention’s split digital watermark.

The present method and apparatus provide iterative embodiments of split digital watermarks which reapply the splitting and steganographic processes to generate greater numbers of components to be reconstituted into the original digital watermark.

The present method and apparatus provide embodiments of split digital watermarks which introduce false statistical information into the components of the split watermark, thereby rendering analysis by an adversary more difficult.

The present method and apparatus provide embodiments of split digital watermarks which require specific sequencings of reconstruction steps due to non-commutativity or non-associativity of its arithmetic operations, again rendering reconstruction by an adversary more difficult.

The separate repositories in which the split watermark content is stored comprise one or more components of the electronic literary macramé (ELM) or knowledge transfer tool (KTT) document itself, one or more file or digital data repositories accessible only to the publisher of the ELM or KTT, and one or more file or digital data repositories accessible only to one or more third parties.

In a second application of the present method and apparatus, the present invention divides portions of content of an ELM or KTT document into two or more components stored in different parts of the ELM or KTT document in order to restrict or delay reading of said portions of the content.
Stories describe the act of tearing a treasure map or other vital written instructions into pieces that can be reassembled, in such a way that without reassembly no possessor of a part of the map can derive the intended meaning. The present invention performs exactly such an act, and does it in such a way as to remove all information from the pieces except when they are all fully combined. In effect, it performs a digital "tearing apart" of an item of information: the process termed in the art “secret-splitting”. The present invention adapts secret-splitting to the purposes of the ELM and KTT.

The secret-splitting operation is already well-known in creating a key pair for two correspondents. In the conventional example, persons A (Alice) and B (Bob) both know the original text which is torn into the two parts. Alice gets a passphrase – her part – she can use in sending to Bob. Bob can then reconstruct Alice's passphrase by subtracting his own passphrase from the original text using the present method. Bob likewise uses his passphrase – his part of the split – in sending to Alice, who then subtracts hers from the original text to reconstruct Bob's. Since the digital output of the tearing-up can be as long as one likes, the keys amount to running keys for a series of messages.

Split Watermark Overview

For an overview of split processes 200, 300 and reconstruction process 400 for a watermark of the present invention see Figs. 1 and 2. For the splitting process according to the methods of the present invention, see Fig. 1. Original watermark 611 is split into intermediate files 548, 549 according to splitting process 200, intermediate file 549 and readable file 521 are combined according to process 300 to produce file 529 for retention by publisher 520, intermediate file 548 and readable file 511 from an ELM or KTT 510 are combined according to process 300 to produce file 539 for retention by a third party 530, and intermediate files 548, 549 are either retained for cross check or else deleted.

For the splitting process according to the methods of the present invention, see Fig. 2. File 529 and readable file 521 are combined according to process 400 to produce intermediate file 547, file 539 and readable file 511 are combined according to process 400 to produce intermediate file 546, and intermediate files 548, 549 are combined according to process 400 to produce reconstructed watermark 612 for comparison to original watermark 611. Intermediate
files 546, 547 are either cross checked against retained intermediate files 548, 549 respectively or else deleted.

The present invention may use any number and size of ELM or KTT components to produce watermark 611, up to and including all components in the ELM or KTT.

Numerical Illustration

The following illustrates arithmetic embodiments with an alphabet consisting of the integers 0-9, to simplify the presentation and clarify the relationship between the tabular and the arithmetic embodiments. Addition of pairs of these integers modulo 10 gives the following table (many other arrangements are possible):

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

There are ten ways (counting each of a commutative pair) in the above table to get a sum of 3: 0 + 3, 1 + 2, 2 + 1, 3 + 0, 4 + 9, 5 + 8, 6 + 7, 7 + 6, 8 + 5, and 9 + 4.

To encrypt a single character of text, here the character '3', in a 2-channel network, we simply choose randomly one of these pairs, and send the left character of the pair down one
channel, and the right character down the other. The intended recipient reconstructs the original plaintext character '3' by adding the two characters sent using the same table, and according to modular arithmetic, retaining only the remainder.

In the present invention, the “tearing-up” is done in its basic embodiment by splitting each character or other unit of text according to a modular addition table, and the reconstruction is done by “adding” the two characters of the split according to the same table. From an algebraic-group standpoint, the plaintext alphabet can be treated as a set for which the operation of modular addition is applicable, forming an addition group on the alphabet. The addition table for the alphabet then provides the results for each possible sum of two characters of the alphabet. If the alphabet contains 26 characters, there will be $26^2 = 676$ entries in the table, and for each of the 26 characters there will appear 26 different sums of character pairs equal to that character in the group.

See Fig. 3 for a diagram of the table for the 26-letter alphabet. An alphabet of any size may be used, up to and including an alphabet encompassing the entire Unicode set of characters, causing the resulting table for any N-character alphabet to have $N^2$ entries. In order that the results of encryption and decryption be consistent and complete, any arrangement of table entries must conform to rules of consistency and completeness for the encryption and decryption operations. For example, if the operation is $+$, and the table indicates that both $A + A = A$ and $A + B = A$, then $A + A = A + B$, meaning that $A = B$, which is inconsistent. Likewise, if $A + B$ does not equal any value in the table, then the table is incomplete. Since the table shown in Fig. 3 is only one of many possible arrangements conforming to such rules, different such arrangements may be made in different embodiments of the invention.

The splitting of text or other information according to the present invention permits an author or publisher of an electronic literary macramé (ELM) or knowledge transfer tool (KTT) to store a first digital watermark in the ELM or KTT according to the process described in U.S. Patent No. 7,555,138, construct a second digital watermark containing information different from that of the first digital watermark, derive a data file to be combined with the second digital watermark to produce the first digital watermark, and retain both the data file and the second digital watermark for use in generating the first digital watermark and comparing the generated watermark to a purported first digital watermark to evaluate the purported watermark’s
Basic Tabular or Symbolic Embodiment

To illustrate the invention’s basic embodiment, see Figs. 3, 4, and 5 for the process using a 26-character uppercase letter alphabet. Fig. 3 shows a typical table 100 for the 26-character English alphabet, with column headers 120 and row headers 110 for each character, and entries in each cell for each combination of row and column. The letter values in the table cell entries in table 100 of Fig. 3 are arranged in a simple staggered placement guaranteeing that no letter appears more than once in any row or column. Many other such arrangements of table cell entries are possible in other table embodiments of table 100. More specifically, any permutation of the sequence of letter value entries in any row or column, used for all rows or columns respectively, is acceptable, which means that for the 26-value set in the second illustration, there are 26! permutations - a 27-digit value.

To assist in references below, Fig. 3 also show all 26 entries for the letter ‘R’ in boldface italics. The entries for character 'R’ may be organized for use as in list 201 in Fig. 4. Each list entry identifies a pair of characters yielding ‘R’ as their sum according to the row labels 110 and column labels 120 of table 100.

The simple staggered placement of table entries in Fig. 3 exemplifies an addition operation with the commutative property, i.e., if the order of the addends is reversed for any sum in the table, the sum remains the same. To illustrate: F + M = R = M + F.

See Fig. 5 for a diagram of the splitting process 200. An input plain text 10 is to be split into two parts 11, 12. For the first character of input text 10, a uniformly-distributed random variable value, here 17, is selected from among the possible 26 index values for the list entries 201, and list entry 211 corresponding to that value is selected, here the 17th entry, which shows ‘R’ as the sum of ‘Q’ and ‘B’. Each subsequent character in input text 10 is split into sum in like manner using a different uniformly-distributed random variable value as shown in list 91, resulting in output texts 11 and 12. Output text 11 and output text 12 are separated onto different channels 240 and 260 for transmission on separate paths, storage in separate locations, or a combination of such transmission and storage patterns. Output text 11 may be stored in the watermark given to the possessor of the ELM, and output text 12 is retained by the ELM’s
publisher. List 91, the set of randomly-determined values used in the splitting process, is discarded.

See Fig. 6 for a diagram of the reconstitution process 400. Using outputs 11 and 12 of the process illustrated in Fig. 5, two of the output values, here ‘Q’ and ‘B’, are added using the ‘Q’ and ‘B’ row and column headers of the same table 100 as in Fig. 3 to produce ‘R’. Subsequent characters follow in the same way as shown to produce the complete original plain text 10. The process of reconstitution amounts to simple addition.

The order of entries in list 201 has no significance as long as said order is left unchanged throughout the process of splitting the input values in a message being processed.

The entire process is repeated for each character of the plain text input, using for each character a separately-determined value for the uniformly-distributed random variable. The result is a set of encrypted texts, no subset of which offers statistical information to a reader to suggest methods of decryption of the original text. Decryption requires access to all of the encrypted texts.

Having access to no more than a proper subset of the channels when a properly-conditioned source of entropy is driving the random selection of the pairs of addends equates to having access to a text encrypted with the Vernam cipher well-known in the art of cryptography. Under such conditions, the plaintext is impossible to recover. The plaintext is easily recovered if all encrypted texts are available. See Bruce Schneier, “Applied Cryptography”, 2nd Ed., pp 70-73, and Adi Shamir, “How to share a secret”, Communications of the ACM 22 (11): pp. 612-613, for references to secret splitting and secret sharing.

Generalized Tabular Embodiments

Table 100 of the present invention is herein presented with its contents organized as the values for an order-26 additive cyclic group (Fig. 3) in the mathematical sense. In the basic embodiments of the present invention, this additive cyclic group organization may be considered as a simple and comprehensible construction for general use, but the contents of table 100 are by no means restricted to such an organization. The only requirements for the organizations of the contents of table 100 are: 1) each input character, symbol or other token to be split must appear in at least one table entry; 2) each row header/column header combination must yield the same
table entry. Stated as a single requirement, this means that there must exist a bijective map between the set of all input characters, symbols, or tokens and the set of all row header/column header combinations.

This requirement may be further generalized to accommodate iterative splits of an input character, symbol, or token. In the general embodiment, each table entry is mapped bijectively to a set of three or more values that serve as the split version of the input represented by the table entry. In effect, this amounts to situating the input value in a multidimensional table, the coordinates of which serve to identify the unique split values for the input value.

The coordinates locating the input value comprise a “tuple” of values in the mathematical sense. Stated as for the row header / column header combinations described above, for each input character, symbol, or token there exists exactly one set of tuples from which one tuple may be chosen randomly according to the present invention. Each coordinate value of the tuple comprises a representation of one of the split values of the invention. An advantage of the use of tuples to split the input value is that the mapping of an input value to a set of tuples from which one will be randomly chosen accomplishes in one step what requires iterative splits in tabular processing. The realization of iterative embodiments is described hereinbelow.

Note that in these generalizations there exists no requirement for any split values to be equal arithmetically to any input values being split, i.e., closure of the split or reconstitution values is unnecessary. This means that an input value of a specific number of bits in length might map to a set of split values each of which is of a length of any number of bits.

Although the present disclosure describes and defines its inputs and outputs in terms of binary digital values, the characters, symbols, or tokens corresponding to each of such binary values also serve as terms having the same meanings as their binary representations in the contexts presented herein.

Finally, there exists no requirement for placement of specific table entries to satisfy group or other mathematical criteria such as associativity or commutativity, and no requirement for equal numbers of appearances for the same value in different table entries. The absence of such requirements enables the realization of alternative-distribution and sequence-sensitive algebraic embodiments as described hereinbelow.
Alternative-distribution Embodiment

In alternative-distribution random variable embodiments, the uniform distribution used for selection of a random variable value is replaced by any nonuniform distribution, for example, a binomial distribution, that generates statistically nonuniform selections from list entries 201, so that some entries are chosen more often than others for separation onto channels 240 and 260. Such embodiments inject into any analysis process statistical distribution information that serves to mislead the process and delay analysis.

Iterative Embodiments

In embodiments providing iterative application of the process, either or both of the output watermark values may be used as input to a repeated use of the table to generate another pair of characters as output. See Figs. 3 and 7, where output 12 of the process of Fig. 5, highlighted in the diagonal set of table entries 202 in boldface in Fig. 3, is used as input 12 to an identical process as shown in Fig. 7. This time a different uniformly-distributed random variable value, here 19, is selected, and the input ‘B’ is then expressed as the sum of ‘S’ and ‘J’ as found in entry 212 of list 202 from table 100. Each subsequent character in input text 11 is split into sum in like manner using a different uniformly-distributed random variable value as shown in list 92, resulting in output texts 13 and 14. Output text 13 and output text 14 are separated onto different channels 260 and 280 for transmission on separate paths, storage in separate locations, or a combination of such transmission and storage patterns. List 92, the set of randomly-determined values used in the second splitting process, is discarded as is list 91. All three outputs 11, 13, 14 are then produced on separate channels for transmission and/or storage independently. In this example, output 11 is stored in the watermark in the work, output 13 is retained by the publisher of the work, and output 14 is retained by a third party. Intermediate output 12 is discarded, since it can be reconstructed if necessary from outputs 13 and 14.

The reconstitution 400 of the original text value is diagrammed in Fig. 8. Using outputs 11, 13, 14 of the process illustrated in Figs. 3 and 7, two of the output values, here ‘Q’ and ‘S’, are added using the ‘Q’ and ‘S’ row and column headers of the same table 100 as in Fig. 3 to produce ‘I’. Subsequent characters from outputs 11, 13 follow in the same way as shown to produce intermediate output 15. Repeating the process, the ‘I’ character is then added to the ‘J’
character using the ‘I’ and ‘J’ row and column headers of the same table 100 as in Fig. 3 to produce the original character ‘R’. Subsequent characters from outputs 14, 15 follow in the same way as shown to produce original text 10. Intermediate output 15 is discarded. The process of reconstitution amounts to a series of simple additions.

In this reconstitution example the sequence in which the three encrypted characters are added does not matter. That is, \((Q + S) + J = Q + (J + S)\). Any order of selecting operands Q, S, or J and any order in which the + operation is applied will recover the original plaintext. This is due to the fact that the table 100 of Fig. 3 treats addition both as an associative process, meaning that, for example, \((Q + S) + J = Q + (S + J)\), and as a commutative process, meaning that, for example, \(S + J = J + S\). Thus intermediate output 15 is not necessarily the same as intermediate output 12 of Fig. 7. All usable tables in the present embodiment possess both the associative property and the commutative property.

Sequence-sensitive Algebraic Embodiments

Table 100 of Fig. 3 comprises a commutative group table in the mathematical sense. The commutative property of Table 100 is evident from its symmetry around the diagonal from the upper left corner to the lower right corner. By relaxing the restriction of commutativity, one or more sequence-sensitive embodiments of the present invention are derived.

In a noncommutative group embodiment a usable table lacking the commutative property may be used, in which case the order of addition of encrypted characters assumes significance. In such an embodiment, it is true that \(S + J \neq J + S\) for at least some S and J in the table.

In a nonassociative loop embodiment (the loop is a generalization of a group) a usable table lacking the associative property may be used, in which case the sequence of additions of encrypted characters performed in iterative applications of the process described above assumes significance. In such an embodiment, it is true that \((Q + S) + J \neq Q + (S + J)\) for at least some Q, S, and J in the table.

In an embodiment for which the use of the table’s entries lack both the commutative and associative properties, a table may be used for which both the order of addition of encrypted characters and the sequence of additions of encrypted characters performed in iterative applications of the process described above assume significance. In such an embodiment, it is
true that \( S + J \neq J + S \) and \( (Q + S) + J \neq Q + (S + J) \) for at least some \( Q, S, \) and \( J \) in the table.

Steganographic Embodiments

In steganographic embodiments, the present process employs a first innocuous plaintext \( A \), and a second plaintext \( B \) requiring concealment. The objective is to present to the reader and the world in general the innocuous text \( A \), thereby diminishing possible suspicion that there exists a concealed text \( B \). For a brief example, see the process 300 of Fig. 9, wherein the text “SECRETS” \( 21 \) requiring concealment is to be combined with the innocuous text “HUMDRUM” \( 22 \). The text \( 22 \) is to be transmitted over or stored on a first output channel, and the combination 23 of texts \( 21 \) and \( 22 \) according to the present process is to be transmitted over or stored on a second (and presumably more-secure) output channel. In Fig. 9, for the first character (‘H’) of text \( 22 \) and the first character (‘S’) of text \( 21 \), the present process 302 of this embodiment is to solve the equation \( S = H + x \), where \( x \) represents the combination of \( H \) and \( S \) according to the table. Since both inputs are determined, and one input (‘H’) is to be used also as output on one channel, no random selection process is used. Instead, the table entry 213 which satisfies the conditions of the equation is selected as shown in process 302, giving the character ‘L’ as the output on the second channel. In effect, the present embodiment arrives at its result through a form of subtraction, that is, when the equation \( S = H + x \) is solved arithmetically, it is written as, and is equivalent to, \( x = S - H \). The subtraction operation “–” constitutes an inverse of addition, so that when “\( x \)” is known value \( X \), the original value of \( S \) can be determined from computing \( H + X \). Each subsequent pair of corresponding characters in input texts \( 21, 22 \) is processed in like manner, resulting in output text 23. Text 22 and output text 23 are separated onto different channels 270 and 290 for transmission on separate paths, storage in separate locations, or a combination of such transmission and storage patterns.

See Fig. 10 for reconstitution 400 of the concealed text \( 21 \) from text \( 22 \) and output text 23. The process is identical to that of Fig. 6. Inputs 22, 23 from channels 270, 290 respectively are added character by character to reconstitute the original concealed text \( 21 \), beginning with the addition of ‘H’ and ‘L’ to produce ‘S’. Subsequent characters are processed in the same way as shown, producing the original concealed text \( 21 \).

A limitation of the steganographic embodiment is the possible lack of addition inverses
for specific character pairs in some character-subset embodiments. This means that in a character-subset embodiment having vowels in one subset and consonants in another, the equation ‘O’ - ‘B’ = s has no solution, and therefore no usable combination text can be produced for such combinations.

As with other embodiments, this steganographic embodiment does not reduce or eliminate vulnerability to decryption if all encrypted texts are available. The purpose of this embodiment is to reduce the likelihood of searching for a combination text ZZZ to combine with an ordinary text XXX to produce concealed text YYY.

Steganographic Iterative Embodiments

Combined embodiments using both steganographic and iterative processes as described above furnish the advantages of both processes, at the cost and exposure of increasing the number of texts to be handled and communicated. See Figs. 11 and 12 for an example. The concealed text 21, “SECRETS”, is combined with innocuous text 22, “HUMDRUM”, according to the steganographic procedure 302 described above to produce the combination 23, here “LKQONZG”. Combination text 23 is then split according to the process of the basic embodiment shown in Fig. 5 to produce the split-text pair 24, 25, “ICZFKDG” and “DIRJDWA” respectively. List 93, the set of randomly-determined values used in the splitting process 301, is discarded. Combination text 23 is then discarded, and texts 24 and 25 are individually disposed either as transmissions or stored keys.

See Fig. 12 for the process of reconstituting the concealed text 21. First, texts 24 and 25 are reconstituted into combination text 23 according to the basic embodiment of the invention, and then combination text 23 is used in combination with innocuous text 22 to reconstitute concealed text 21 as shown earlier in Fig. 10.
Arithmetic Embodiments

An arithmetic embodiment of the present invention in a computer-based implementation comprises an instance of a tabular or symbolic embodiment that exploits the computational advantages of the computer in which the embodiment is operating. In an arithmetic embodiment, the table of values is replaced by a calculation using random or pseudorandom numeric values selected from a range. For example, an 8-bit arithmetic embodiment uses generated values in the range from 0 to 255, 256 values in all, to compute the split values from the original text, as follows. Given an 8-bit character or other value CH, an 8-bit random value RN between 0 and 255 inclusive is generated. Using these two values, a first 8-bit value C1 is computed as C1 = (CH + RN) mod 256, and a second 8-bit value C2 is computed as C2 = (CH – RN) mod 256. C1 is then put out on a first channel, and C2 is put out on a second channel. RN is discarded. To reconstitute the value CH using C1 and C2 simply requires the calculation CH = ((C1 + C2) mod 256) / 2.

Any integer numeric base may be used in arithmetic embodiments. The above example uses a base of 256. If a base of 26 is used, all of the examples shown in Figs. 5 through 12 may be used to illustrate the base-26 arithmetic embodiment by substituting for each letter its numeric position in the Roman alphabet minus 1.

The arithmetic embodiment is especially useful for splitting binary data into two or more channels of output, where the input to be split is not textual. In general, an N-bit arithmetic embodiment exploiting the advantages of binary computation uses generated values RR in the range from 0 to 2^N – 1, 2^N values in all, and selects N successive bits BB at a time from its input. The two outputs B1 and B2 are then computed as B1 = (BB + RR) mod 2^N and B1 = (BB – RR) mod 2^N respectively, and reconstituted through the calculation BB = ((B1 + B2) mod 2^N) / 2.

Steganographic Arithmetic Embodiment

In a steganographic arithmetic embodiment, the process works in the same manner as in the steganographic embodiment described above and shown in Figs. 9, 10, 11, and 12, with the substitution of a steps of calculation for the corresponding step 302 of lookup in a list. Given an 8-bit arithmetic embodiment integer base, the calculation step using a concealed value CO and an innocuous value IN as inputs to produce a restoration output RE is performed as RE = ((2 *
CO) - IN) mod 256. The reconstitution of the concealed value is computed as \( CO = ((RE + IN) \mod 256) / 2 \), just as in the reconstitution process for any arithmetic embodiment.

Alternative-distribution Arithmetic Embodiment

In alternative-distribution random variable arithmetic embodiments, as with embodiments using specific character sets, the uniform distribution used for selection of a random variable value RN or RR is replaced by any nonuniform distribution, for example, a binomial distribution, that generates statistically nonuniform selections from the range 0 through \( 2^N \), so that some values are chosen more often than others for separation onto the output channels. Such embodiments inject into any analysis process statistical distribution information that lacks purpose-related significance, thereby prolonging analysis by consuming an analyst’s time.

Multiple-Table Embodiment

The ELM and KTT use the invention both for assuring watermark integrity and for enhancing reader engagement. For readers, the present invention must produce and present readable text or symbols from which the readers may derive ELM and KTT content by reconstructing said content from the presented text and symbols. The time and effort needed for derivation of content serves to delay premature reader viewing of answers or supporting material in a KTT, and to engage reader interest in solving puzzles in an ELM. In multiple-table embodiments, the invention’s addition table is separated into two or more addition tables for character subsets to make the output resemble readable text, or encrypted text in a simpler mode. See Fig. 13. In the tables in Fig. 13, all the uppercase consonants form one table 101, the uppercase vowels another table 102, and the numbers another table 103, with additional tables (not shown in Fig. 13) similarly arranged for lowercase letters and other symbols as desired. Using said tables to split a text produces two texts that present the general appearance of words and sentences by preserving the spacing, capitalization, punctuation, and consonant-vowel patterns of the text to be split while substituting different letter, number, and symbol values. Readers attempting decryption using only one of the split texts derived from a plain text can find the task considerably more challenging and entertaining than doing the daily newspaper cryptogram.
Embodiment Combinations

The embodiments described hereinabove may be combined to produce additional embodiments as shown in the following list of alternatives, which represents a broad taxonomy of the possible combinations.

- Tabular vs. Arithmetic
- Uniform-Distribution vs. Nonuniform-Distribution
- Single-Pass vs. Multiple-Pass
- Commutative Split vs. Noncommutative Split
- Associative Split vs. Nonassociative Split
- Steganographic vs. Non-steganographic

Certain combinations are omitted in the preceding list due to inconsistency of attributes, e.g., the steganographic embodiments are only possible when in the realm of multiple-pass embodiments, since at least two passes of encryption or encoding are required to implement the invention’s steganographic embodiments. Likewise, in arithmetic embodiments, the commutativity and associativity of arithmetic are assumed, eliminating embodiments lacking those properties.

Graphical Embodiments

Graphical applications of arithmetic embodiments of the present invention utilize digital images instead of text to conceal watermark and other information in ELM and KTT documents. This process, called “visual cryptography” in the art, operates at the level of bits, bytes, or pixels rather than at the level of characters, but produces similar results. See Moni Naor and Adi Shamir, “Visual Cryptography”, EUROCRYPT 1994, pp. 1–12. Practical ELM and KTT embodiments combining graphical, steganographic, and iterative processes as described above, either pairwise or with all three, furnish the advantages of the combined processes for both watermarks and content for which presentation is to be delayed or obstructed.

A Simple Everyday Example
A husband has given his wife his ATM card to use while they are on vacation. He decides to take a side trip with a his friend Joe, and while they are away, she calls him.

"You forgot to give me the PIN number for your card," she says. "I have to buy some gas."

"Oh, yeah," he responds. "Well, look, I don't want to say it on the cell network. Let me give you half of the sum for it."

Since both are amateur cryptographers, they both understand. He says, "9234. Just add that to the first four digits on the card I gave you when I left with Joe. It's where you keep your change."

She says, "Thanks," opens her change purse, finds the card, and the first four digits are 7881. Adding these digits modularly to the number he gave her, she gets $9234 + 7881 = 6015$, the PIN number of his card.

Admittedly, this illustrates the use of a full-length stored key, Vernam-style, but the husband might have forgotten to give his wife the card. In that case, he arranges with her another call or a message via another medium in order to give her the number needed. The giving of the card constitutes the use of a communication channel in the broader sense. He might just as easily have whispered '7881' to her as he left, trusting to her memory. The principle is the same. Increasing the number of distinct channels used to transmit the cryptotext components increases the adversary's problem sharply.

Customized Watermarking

The splitting methods and results disclosed hereinabove and the structural and processing specifications disclosed in the hereinabove-referenced applications offer a powerful tool for enhancing the customization and provenance determination for an electronic (digital) document. The original ELM/KTT or other electronically-published work may optionally contain its own watermark information embedded digitally in said work in any of a variety of ways both conventional and unconventional. By applying the splitting process hereinabove disclosed to the embedded watermark information, the present invention creates shares of the watermark
information that may be distributed among purchasers, publisher, author, and other legal entities. See Fig. 14.

From a base ELM/KTT or other digital document 510, a base watermark 611 may be derived, stored, and extracted. Using splitting process 200, the present invention creates a publisher watermark share intermediate file 549 and a third-party watermark share intermediate file 548 as shown also in Fig. 1. At the time of purchase of a published copy of digital document 510, the present invention solicits and obtains digital buyer data 551 from the buyer and sources of digital information concerning said buyer, applies combining process 300 to generate buyer watermark 613, and applies embedding process 700 to embed buyer watermark 613 in digital document copy 501.1.

The process of Fig. 14 may be reapplied multiple times in various arrangements to provide a unique watermark 613 in each published copy of base ELM/KTT or other digital document 510. For an exemplary arrangement of splitting and combining watermark data, see Fig. 15. Splitting process 200 is applied in this exemplary arrangement to produce a watermark share intermediate file 548.1, 548.2, 548a, 549 for each copy. In combining process 300, the present invention combines each watermark intermediate share file 548, 549 with digital buyer data 551.1, 551.2, author data 553, or publisher data 555 to produce buyer watermark 613.1, 613.2, author watermark 615, or publisher watermark 617 respectively. The present invention then uses embedding process 700 as shown in Fig. 14 to embed the respective watermark in its own copy 510.1, 510.2, 510a, 510b of base ELM/KTT or other digital document 510.

The present invention performs reconstitution of watermark intermediate share files and the original base watermark as shown in Fig. 16. Using reconstitution process 400, the present invention combines buyer watermark 613.1 with buyer data 551.1 to produce reconstituted buyer watermark share file 548.1. In like manner, reconstituted watermark files 548.2, 548a, 549 are created from their respective sources as shown. If desired, the present invention may then use reconstitution process 400 to recreate base watermark 611.

The exemplary process outlined hereinabove with reference to Figs. 14, 15, and 16 may be varied to provide disjoint or merged intermediate files in one or more distinct additional stages of splitting, recombining, and reconstituting watermark patterns as intermixed with other digital materials held by and identifiable by individuals and groups comprising a wide range of
parties to the original base ELM/KTT or other digital document or to its derivative copies.

Conclusions

The present invention is in part distinguished from others in the art by its symmetry: it uses no separately-generated or separately-stored key to produce the encrypted texts, but instead generates randomly the text-splitting criterion at the point in space and time at which the split takes place, thereby minimizing both temporal and spatial exposure to compromise of the content being encrypted. The generated values used to split the text are discarded immediately, making them inaccessible for all later analysis, a feature constituting an advantage over the use of stored and/or transmitted keys arising directly out of a random-value-generation process.

The present invention’s methods of splitting its input use an input-to-tuple bijective mapping process which generalizes and subsumes the conventional processes well-known in the art of secret splitting: 1) XOR of input at a bit level to derive a pair of outputs, 2) other modular arithmetic operations. For mappings not corresponding to conventional arithmetic processing, such as those required for multiple-table embodiments or certain of the generalized embodiments described hereinabove, the reconstruction process requires the use of the same tabular information as the splitting process, either in the form of tables explicitly stored and accessed, or in the form of processing which represents such tables through computation.

Both electronic literary macramé output works and knowledge transfer tool output works make use of the encryption and decryption processes described herein to assure the integrity of digital watermarks stored in each copy of such a work. Both classes of works also make use of the encryption and decryption processes described herein to conceal selected textual components from casual reader access, for the purposes of delaying access to answers to questions directed to the reader, obstructing access to adult or controversial content, and providing sources of entertainment and mental challenge to readers in finding and decrypting the encrypted texts presented.

Since its principal purpose is the splitting and recombining of digital watermarks, the
The present invention is further distinguished from others in the art by its lack of requirement for high-performance splitting or recombining of the watermark, as would be found in the XOR-based methods used in conventional data-splitting applications. The absence of such requirements teaches instead preference for the use of the invention’s generalized splitting and reconstruction processes described herein.

When the present invention’s input-to-tuple bijective mapping process takes a conventional fixed form not varied by its users, the mapping may be compromised. Even in such circumstances, the present invention may be characterized as a kind of "keyless cryptosystem", since the key to decryption – the random value used to select one of the tuples – is discarded at the point at which it is first used. But since the present invention’s key information can be considered to be distributed in the messages produced by the use of the key, perhaps the term "all-key cryptosystem" might do just as well. The problem of key management has not disappeared, but instead has become a part of the problem of channel management. As long as an adversary has access only to an insufficient number of channels to decrypt messages, this system works quite well.

For an adversary, the channel-access problem is simply a more-difficult form of the key-access problem. The added difficulty arises from the fact that access for each channel must take place within a limited range of time and space, down to a period of microseconds not necessarily synchronous for all channels, and over a range of possible classes of channels limited only by the ingenuity of the sender and receiver. Also, before and after the receiver has the sender's message, there is no key storage to consider or defend.

In effect, the conventional "man-in-the-middle" attack on encrypted messages is changed to a "man-in-all-the-middles" attack. As shown above, the sender and receiver can complicate matters by sending encrypted components which, when summed with certain subsets of the other components transmitted, will produce plausible-looking plaintexts.

As a tradeoff for the difficulties of channel access, an adversary gains the advantage of complete access to the plaintext when all channels are accessible. This advantage is offset by the convenience of combining the present invention with other systems. Padding, transposition, temporal shifts, block encryption, and other methods and techniques all work through the present invention transparently, and add their conventional advantages.
In addition, an encrypted form of data which has been split using the present invention offers no statistical information concerning its content, thereby presenting an additional obstruction to analysis. For example, once a plaintext has been split into two or more parts according to the present system, the sender and receiver can use a public-key cryptosystem to encrypt each of the split message parts, say, with a different prearranged passphrase for each one. Similarly, DES could be used on the split parts, or the parts could be encrypted with different techniques. The use of such approaches would erase any appearance of pattern in the parts, and prevent trivial matching of the parts to recover the plaintext.

Current trends showing the proliferation of both channels and modes of communication suggest that the present invention’s utility increases as a sender’s possible numbers and types of communication links to a receiver increase.

The use of the present invention with respect to digital documents presents significant added capability to determine the provenance of said documents, along with the ability to customize individual copies or sets of copies to contain data relating the owners of said copies to the originators of the digital document or to one another.

It will be apparent to those of ordinary skill in the art that the practice of the present invention as delineated in the present disclosure encompasses numerous possible alterations, modifications, and combinations not explicitly recited hereinabove.
Claims

What is claimed:

1. An apparatus for verifying the digital watermark of a length of a first number of binary bits in an electronic document, comprising:

   a computer system, further comprising one or more processors, a user display interface component, one or more user input interface components, and one or more memory components for holding an operating system, one or more software applications, and one or more electronic documents each comprising a plurality of components;

   a first software application for splitting one or more components of the digital watermark of a length of a first number of binary bits of a first electronic document into two or more components of watermark information stored in the first electronic document and in one or more second electronic documents; and

   a second software application for reconstructing said one or more components of the digital watermark of a length of the first number of binary bits of the first electronic document using said two or more components of watermark information stored in said first electronic document and in one or more second electronic documents.

2. The apparatus of claim 1, wherein the first electronic document comprises an electronic literary macramé (ELM) component.

3. The apparatus of claim 1, wherein the first electronic document comprises a knowledge transfer tool (KTT) component.

5. [secret-splitting (general)] The apparatus of claim 1, in which the first software application for splitting one or more components of the digital watermark of a length of a first number of binary bits of a first electronic document into two or more components of watermark information stored in the first electronic document and in one or more second electronic documents comprises:
a software program for selecting a second number of bits from the digital watermark less than or equal to the first number of bits;

a software program for expressing the value determined by the second number of bits as a set of two or more values;

a software program for storing each value of the set of two or more values in a separate output corresponding with the order of the values of the set [MAY NEED HELP WITH CLAIM HERE];

a software program for repeating the previous four steps for unselected bits of the digital watermark until all bits of the digital watermark have been selected and all resulting sets of two or more values have been stored.

6. [secret-splitting (modular sum)] The apparatus of claim 1, in which the first software application for splitting one or more components of the digital watermark of a length of a first number of binary bits of a first electronic document into two or more components of watermark information stored in the first electronic document and in one or more second electronic documents comprises:

a software program for selecting a second number of bits from the digital watermark less than or equal to the first number of bits;

a software program for expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number;

a software program for storing the first value in a first output;

a software program for storing the second value in a second output; and

a software program for repeating the previous four steps for unselected bits of the digital watermark until all bits of the digital watermark have been selected and all resulting first values and second values have been stored.

7. [non-commutative modular sum] The apparatus of claim 6, wherein the software program for expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number further comprises
a software program for expressing the value determined by the second number of bits as a non-
commutative modular sum of a first value and a second value each having the same number of
bits as the second number.

8. [non-associative modular sum] The apparatus of claim 6, wherein the software program for
expressing the value determined by the second number of bits as a modular sum of a first value
and a second value each having the same number of bits as the second number further comprises
a software program for expressing the value determined by the second number of bits as a non-
associative modular sum of a first value and a second value each having the same number of bits
as the second number.

11. [looking up split parts of watermark component (general)] The apparatus of claim 5, wherein
the first software program for expressing the value determined by the second number of bits as a
set of two or more values further comprises a software program for looking up the value
determined by the second number of bits in a table to locate the set of two or more values.

12. [computing split parts of watermark component (general)] The apparatus of claim 5, wherein
the first software program for expressing the value determined by the second number of bits as a
set of two or more values further comprises a software program for computing the set of two or
more values using the value determined by the second number of bits as input to the
computation.

21. [secret sharing (general)] The apparatus of claim 1, wherein the second software application
for reconstructing said one or more components of the digital watermark of a length of a first
number of binary bits of the first electronic document using said two or more components of
watermark information stored in the first electronic document and in one or more second
electronic documents comprises:

  a software program for retrieving a series of values from each of the said two or more
  components of watermark information;

  a software program for determining a watermark value comprising a component of the
digital watermark using the retrieved series of values;
   a software program for storing the watermark value in a third output; and
   a software program for repeating the previous four steps for the said two or more
components of watermark information until the third output comprises the digital watermark.

22. [looking up watermark component] The apparatus of claim 21, wherein the software
program for determining a watermark value comprising a component of the digital watermark
using the retrieved series of values comprises a software program for looking up the watermark
value in a table using the retrieved series of values as the lookup key.

23. [computing watermark component] The apparatus of claim 21, wherein the software
program for determining a watermark value comprising a component of the digital watermark
using the retrieved series of values comprises a software program for computing the watermark
value using the retrieved series of values as the inputs to computation.

25. [secret sharing (modular sum)] The apparatus of claim 1, wherein the second software
application for reconstructing said one or more components of the digital watermark of a length
of a first number of binary bits of the first electronic document using said two or more
components of watermark information stored in the first electronic document and in one or more
second electronic documents comprises:
   a software program for selecting the second number of bits from a first input;
   a software program for retrieving a first value of a length of the second number of bits
from a first input that comprises the first of the two outputs;
   a software program for retrieving a second value of a length of the second number of bits
from a second input that comprises the second of the two outputs;
   a software program for computing the modular sum of the second number of bits of the
first value and the second value;
   a software program for storing the modular sum of the second number of bits of the first
value and the second value in a third output; and
   a software program for repeating the previous four steps for the first input and the second
input until the third output comprises an output of the length of the first number of bits.

26. [final watermark output] The apparatus of claim 25, wherein the software program for repeating the previous four steps for the first input and the second input until the third output comprises an output of the length of the first number of bits further comprises a software program for repeating the previous four steps for the first input and the second input until the third output comprises an output to be matched to the original digital watermark.

27. [customized watermark] The apparatus of claim 1, further comprising:
   a third software application for customizing the digital watermark of the first electronic document using data provided by a third party to generate a custom digital watermark in a copy of the first electronic document to produce a second electronic document containing said custom watermark; and
   a fourth software application for reconstructing the digital watermark of the first electronic document using data provided by a third party and a custom digital watermark in a second electronic document to produce said digital watermark of the first electronic document.

101. A method for verifying the content of an original digital watermark of a length of a first number of binary bits, said digital watermark comprising a component of an electronic document, comprising the steps of:
   composing an original digital watermark of the length of a first number of bits;
   splitting the content of the original digital watermark into one or more first outputs and one or more second outputs;
   storing the one or more first outputs in an electronic document;
   storing the one or more second outputs in one or more repositories separate from the electronic document;
   retrieving the one or more first outputs from the electronic document;
   retrieving the one or more second outputs from the repositories separate from the electronic document;
computing the content of a reconstructed digital watermark from the one or more first outputs and the one or more second outputs; and
comparing the original digital watermark with the reconstructed digital watermark.

102. [ELM secret-splitting] The method of claim 101, in which the step of storing the one or more first outputs in an electronic document comprises the step of storing the one or more first outputs in an electronic literary macramé.

103. [ELM secret-splitting] The method of claim 101, in which the step of retrieving the one or more first outputs from the electronic document comprises the step of retrieving the one or more first outputs from the electronic literary macramé.

106. [KTT secret-splitting] The method of claim 101, in which the step of storing the one or more first outputs in an electronic document comprises the step of storing the one or more first outputs in a knowledge transfer tool.

107. [KTT secret-splitting] The method of claim 101, in which the step of retrieving the one or more first outputs from the electronic document comprises the step of retrieving the one or more first outputs from the knowledge transfer tool.

111. [secret-splitting (modular sum)] The method of claim 101, in which the step of splitting the content of an original digital watermark of the length of a first number of bits into two or more outputs comprises the steps of:
selecting a second number of bits from the digital watermark less than or equal to the first number of bits;
expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number;
storing the first value in a first output;
storing the second value in a second output; and
repeating the previous four steps for unselected bits of the digital watermark until all bits
of the digital watermark have been selected and all resulting first values and second values have been stored.

112. The method of claim 111, in which the step of expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number comprises the step of expressing the value determined by the second number of bits as a non-commutative modular sum of a first value and a second value each having the same number of bits as the second number.

113. The method of claim 111, in which the step of expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number comprises the step of expressing the value determined by the second number of bits as a non-associative modular sum of a first value and a second value each having the same number of bits as the second number.

114. The method of claim 111, in which the step of selecting a second number of bits from the digital watermark less than or equal to the first number of bits comprises the step of selecting adjoining bits from the digital watermark.

114a. The method of claim 111, in which the step of selecting a second number of bits from the digital watermark less than the first number of bits comprises the step of selecting eight adjoining bits from the digital watermark.

114b. The method of claim 111, in which the step of selecting a second number of bits from the digital watermark less than the first number of bits comprises the step of selecting sixteen adjoining bits from the digital watermark.

114c. The method of claim 111, in which the step of selecting a second number of bits from the digital watermark less than or equal to the first number of bits comprises the step of selecting permuted bits from the digital watermark.
115. The method of claim 111, in which the step of expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number comprises the steps of:

- determining the set of all possible pairs of modular addend values yielding the value determined by the second number of bits;
- selecting at random one pair of modular addend values from the set of all possible pairs of modular addend values yielding the value determined by the second number of bits; and
- expressing the value determined by the second number of bits as the selected modular sum of the selected pair of modular addend values.

115a. [CRITICAL!] The method of claim 115, in which the step of selecting at random one pair of modular addend values from the set of all possible pairs of modular addend values yielding the value determined by the second number of bits comprises the steps of:

- selecting a random numeric value from a range that indexes the set of all possible pairs of modular addend values yielding the value determined by the second number of bits;
- using the selected random numeric value to retrieve its indexed pair of modular addend values; and
- discarding the selected random value [critical step].

115b. The method of claim 115, in which the step of selecting at random one pair of modular addend values from the set of all possible pairs of modular addend values yielding the value determined by the second number of bit comprises the step of selecting one pair of modular addend values from the set of all possible pairs of modular addend values according to a random distribution selected from the group consisting of:

- a uniform random distribution; and
- a general nonuniform random distribution.

116. [secret-splitting multiple-pass] The method of claim 111, further comprising the steps of:

- selecting an output to be split from the first output and the second output;
selecting a second number of bits from the output to be split less than or equal to the first number of bits;
expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number;
storing the first value in a third output;
storing the second value in a fourth output; and
repeating the previous four steps for unselected bits of the second output until all bits of the output to be split have been selected and all resulting first values and second values have been stored.

118. The method of claim 111, in which the step of expressing the value determined by the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number comprises the step of expressing the second number of bits as a modular sum of a first value and a second value each having the same number of bits as the second number wherein the modulus of the sum is equal to two raised to the power of the second number of bits.

121. [secret sharing multiple-pass] The method of claim 101, in which the step of reconstructing the content of the digital watermark from the two outputs comprises the steps of:
selecting the second number of bits from a first input;
retrieving a first value of a length of the second number of bits from a first input that comprises the first of the two outputs;
retrieving a second value of a length of the second number of bits from a second input that comprises the second of the two outputs;
computing the modular sum of the second number of bits of the first value and the second value;
storing the modular sum of the second number of bits of the first value and the second value in a third output; and
repeating the previous four steps for the first input and the second input until the third output comprises an output of the length of the first number of bits.
122. [secret sharing] The method of claim 121, in which the step of repeating the previous four steps for the first input and the second input until the third output comprises an output of the length of the first number of bits comprises the step of repeating the previous four steps for the first input and the second input until the third output comprises an output of the length of the digital watermark.

131. [false watermark splitting multiple-pass] The method of claim 101, in which the step of splitting the content of an original digital watermark of the length of a first number of bits into two or more outputs comprises the steps of:

- providing a first input of the length of the first number of bits;
- providing a second input of the length of the first number of bits;
- selecting a second number of bits from the first input less than the first number of bits to produce an original bit selection;
- selecting the second number of bits from the second input to produce a second bit selection;
- computing the modular difference of the original bit selection and the second bit selection by subtracting modularly the second bit selection from the original bit selection;
- storing the modular difference of the original bit selection and the second bit selection in a first output; and
- repeating the previous four steps for unselected bits of the first input and the second input until all bits of the first input and the second input have been selected and all resulting modular differences have been stored in the first output.

131. [false watermark splitting] The method of claim 101, in which the step of splitting the content of an original digital watermark of the length of a first number of bits into two or more outputs comprises the steps of:

- providing a second digital watermark of the same length as the original digital watermark and having one or more bits different in value from the corresponding bits of the original watermark;
selecting a second number of bits from the original digital watermark less than the first number of bits to produce an original bit selection;
selecting the second number of bits from the second digital watermark to produce a second bit selection;
computing the modular difference of the original bit selection and the second bit selection by subtracting modularly the second bit selection from the original bit selection;
storing the modular difference of the original bit selection and the second bit selection in a first output; and
repeating the previous four steps for unselected bits of the original digital watermark until all bits of the original digital watermark have been selected and all resulting modular differences have been stored.

151. [secret-splitting (general)] The method of claim 101, in which the step of splitting the content of an original digital watermark of the length of a first number of bits into two or more outputs comprises the steps of:
selecting a second number of bits from the digital watermark less than or equal to the first number of bits;
expressing the value determined by the second number of bits as a set of two or more values;
storing each value of the set of two or more values in a separate output corresponding with the order of the values of the set [MAY NEED HELP WITH CLAIM HERE]; and
repeating the previous four steps for unselected bits of the digital watermark until all bits of the digital watermark have been selected and all resulting first values and second values have been stored.

152. [secret-splitting (general)] The method of claim 151, in which the step of splitting one or more components of the digital watermark of a length of a first number of binary bits of a first electronic document into two or more components of watermark information stored in the first electronic document and in one or more second electronic documents comprises the steps of:
selecting a second number of bits from the digital watermark less than or equal to the first
number of bits;
expressing the value determined by the second number of bits as a set of two or more values;
storing the first value in a first output;
storing the second value in a second output; and
repeating the previous four steps for unselected bits of the digital watermark until all bits of the digital watermark have been selected and all resulting first values and second values have been stored.

152. [looking up split parts of watermark component (general)] The method of claim 151, wherein the step of expressing the value determined by the second number of bits as a set of two or more values further comprises the step of looking up the value determined by the second number of bits in a table to locate the set of two or more values.

153. [computing split parts of watermark component (general)] The method of claim 151, wherein the step of expressing the value determined by the second number of bits as a set of two or more values further comprises the step of computing the set of two or more values using the value determined by the second number of bits as input to the computation.

175. The method of claim 101, further comprising the steps of:
recombining each of the one or more first outputs and one or more second outputs of the split content of the original digital watermark of a first electronic document with a unique digital document to produce a custom digital watermark;
storing said custom digital watermark in a copy of the first electronic document; and
providing said copy of the first electronic document to the provider of the unique digital document.

176. The method of claim 101, further comprising the steps of:
retrieving the custom digital watermark from a copy of a first electronic document; retrieving the unique digital document from the provider of said digital document; and reconstituting the original digital watermark of a first electronic document by combining each of said custom digital watermarks with its corresponding unique digital document.

177. The method of claim 176, further comprising the steps of:
   combining each of said custom digital watermarks with its corresponding unique digital document to reconstitute a split component of an original base digital watermark;
   reconstituting said original digital watermark by modular addition of its split components to produce a copy of said original digital watermark; and
   comparing the original digital watermark with the reconstituted digital watermark.