



- (51) International Patent Classification:
G09C 5/00 (2006.01)
- (21) International Application Number:
PCT/MY2014/000187
- (22) International Filing Date:
24 June 2014 (24.06.2014)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
PI 2013003670 11 October 2013 (11.10.2013) MY
- (71) Applicant: MIMOS BERHAD [MY/MY]; Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).
- (72) Inventor: ALWYN, Goh; c/o Technology Park Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).
- (74) Agent: MANIAM, Mahalingam; IP Rights (M) Sdn Bhd, No. 7-M, Biz Avenue, Neo Cyber, Lingkaran Cyber Point Barat, 63000 Cyberjaya, Selangor Darul Ehsan (MY).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

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

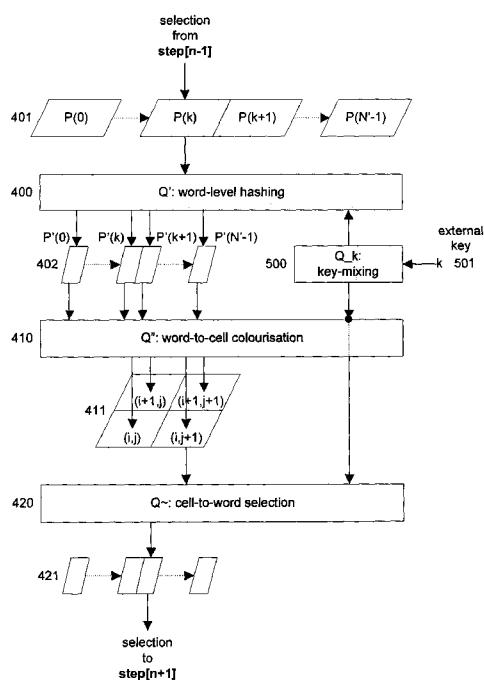
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,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

Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- of inventorship (Rule 4.17(iv))

[Continued on next page]

- (54) Title: A METHOD FOR MULTI-STEP PROGRESSIVE VISUAL AUTHENTICATION OF HIGH-ENTROPY PARAMETERS

**Figure 4**

- (57) Abstract: The present invention relates to a method for visual authentication of high-entropy parameters by means of multi-step progressive visualization on a receiving application by a user, more particularly to allow machine-to-human authentication, which is unaddressed in existing solutions and security protocol frameworks. One of the advantages of the present invention is that it provides for representation of long high-entropy codewords as perceptually significant visual images on graphical displays. These codewords occur in the context of cryptographic protocols, and typically range in length from 128 to 1024-bits. By computing representation at more detailed scales of resolution in progressive steps, this allows human visual inspection which is both secure, effective and ergonomic. Another advantage of the method of the present invention is that it computes visually simple (and therefore ergonomic) representations at each step of progressive computation, with the complexity of visualization process (as would necessarily arise from entropy content of cryptographic codewords) dispersed over the multiple steps of progression. This provides for the user to determine whether visualised cryptographic input is authentic by means of a process which can range from simple to exhaustive, with the level of thoroughness proportional to number of user interactions with the particular visualization object. Authentication of the input codeword would be accomplished by means of comparing test visualization against reference visualization at each progressive step, the latter of which is executed on platform deemed to be trustworthy by the user.



Published:

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

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

A METHOD FOR MULTI-STEP PROGRESSIVE VISUAL AUTHENTICATION
OF HIGH-ENTROPY PARAMETERS

5 FIELD OF THE INVENTION

The present invention relates to a method for authentication of high-entropy parameters by means of multi-step progressive visualization of a receiving application by a user more particularly to allow machine-to-human authentication, which is unaddressed in existing
10 solutions and security protocol frameworks.

BACKGROUND OF THE INVENTION

Standard cryptographic frameworks for client-server security are based on computation and
15 exchange of high-entropy codewords. Client and server-side components of distributed applications should not be regarded as independent of one another from the security viewpoint, especially if developed and/or operated by the same party. Verification that codewords are correct requires user to presume client or server-side applications are trustworthy. Codeword correctness as determined by client or server-side components in
20 the context of transactions executed on the same application is hence not entirely in satisfactory in terms of establishment of trustworthiness.

In addition, visual inspection of codewords (in symbolic or visual representations) is neither effective nor ergonomic. This is because of the complexity of codeword representations, in
25 the form of symbols (as base-16/32/64 strings), or images (ie optical barcode). Codeword digests (ie public-key hashes) are shorter (i.e. of order 2^{160} complexity) but still not sufficiently conducive for effective and ergonomic visual inspection. Hashing indeed allows for simpler representations, but cannot be applied repeatedly for cumulative effect. Visual inspection of codewords is hence still excessively taxing, and therefore not ergonomic.
30 Therefore, there is a need to overcome the above drawbacks.

The present invention introduces a method for visual authentication of high-entropy parameters of a receiving application by a user in multiple progressive steps. The present invention further computes representation at more detailed scales of resolution in
35 progressive steps, so as to allow human visual inspection which is both secure and

ergonomic. Moreover, the present invention allows machine-to-human authentication, which is unaddressed in existing solutions and security protocol frameworks.

SUMMARY OF THE INVENTION

5

The present invention provides to a method for visual authentication of high-entropy parameters of a receiving application on a user terminal executing the receiving application as a test visualization, and concurrently generating a reference visualization from an application deemed to be trusted by the user; displaying the test visualization and the
10 reference visualization on the respective graphical displays; and determining the authenticity of the test visualization by comparing the test visualization against the reference visualization.

In one aspect of the present invention, high-entropy parameters are cryptographic
15 codewords of variable length and effective duration.

In yet another aspect of the present invention, the receiving application executes processing of a visual representation of high-entropy parameters into progressive scales of resolution.

20 In another of aspect of the present invention, a visual representation is provided for visual authentication of high-entropy parameters of a receiving application on a user terminal with a graphical display.

In one aspect of the present invention, the visual representation transformed from gross to
25 fine resolution in discrete steps by a controlled system, up to visualization limit computed from length of high-entropy parameter

In yet another one aspect of the present invention, the visual representation is generated by dependant on input key.
30

In one of the embodiment of the present invention, the visual representation is generated by independant on input key.

In one of the embodiment of the present invention, the visual representation is computed on
35 multiple segments of a parameter at each step and the visual representation is executed as

colour value computed from numerical or symbolic value of the parameter on each segment at each step.

In yet another embodiment of the present invention, segmentation of visual representation displayed on the user terminal is of equal degree to segmentation of parameter segment represented, at each progressive step of computation.

A cryptographic hash function is used to compute the colour corresponding to each segment.

A hash-based message authentication code (HMAC) is used to compute the colour corresponding to each segment with hash-based message authentication code (HMAC) key as operative secret parameter.

In another of the embodiment of the present invention, the trusted application executes on a trusted device.

The receiving application executes a visualization comprising word-to-cell visualization of the high-entropy parameter into a visual-map in iterative steps comprising partitioning of visual object [i] of particular step n into N' sub-cells, where N' is the degree to which display object is partitioned for mapping process;

providing a segmentation of input codeword $P[i]$ of same step n into N' sub-words, with equal degree N' of codeword segmentation;

providing a computation of visualization value $Q[i]$ for each sub-word $P[i]$,

for $i = 0 \dots N' - 1$; and

displaying visualization value $Q[i]$ by means of colour assignment $Q[i]$ for each cell [i].

In one aspect of the present invention, a cell colourisation $Q(P)$ corresponding to codeword segment P is executed in ZK manner.

In another aspect of the present invention, visualization limit is provided if a range of all possible values of input codeword P at step n is less than encoding capacity N'' of single visualization step and visualization is terminated where N'' is encoding capacity of visualization output from geometry and colourisation of display object.

The receiving application executes subsequent visualization comprising word-to-cell visualization of the high-entropy input codeword into a visual-map; subject to user option of 1-of-N' visual segment corresponding to sub-word of said input codeword, or alternatively system random option of 1-of-N' visual segment corresponding as aforesaid, or alternatively system option of all N' visual segments corresponding to entirety of said input codeword; and furthermore subject to condition that visualization process has not exceeded visualization limit.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of the specification, illustrate embodiments of the invention and, together with the description, serve to explain the principles of the invention.

Figure 1 illustrates a flow chart of a method for visual authentication of high-entropy parameters of a receiving application on a user terminal in accordance with the present invention.

Figure 2 illustrates a partition of visual object of visualization process into N' constituent cells at each step [n] of multi-step progression, as part of method for visual authentication of high-entropy parameters of a receiving application on a user terminal in accordance with the present invention.

Figure 3 illustrates a segmentation process in which input codeword of visualization process is divided into N' constituent sub-words at each step [n] of multi-step progression, as part of method for visual authentication of high-entropy parameters of a receiving application on a user terminal in accordance with the present invention.

Figure 4 illustrates a computation of visual representation Q for codeword P of interest at each step [n] of multi-step progression, as part of method for visual authentication of high-entropy parameters of a receiving application on a user terminal in accordance with the present invention.

DETAILED DESCRIPTIONS OF THE INVENTION

The present invention will now be described in detail in connection with specific embodiments, and with reference to the accompanying drawings.

5

The method of the present invention provides interactions conducted using cryptographic codewords in internal representations and external exchange parameters which are of length excessive for easy or effective visual inspection by human users. This method is applicable to computerised entities or application processes engaged in interactions using cryptographic mechanisms and protocols, and in which it is useful for human as users to have a means for assessment, on external entities and processes.

The present invention relates to a method for visual authentication of high-entropy parameters of a receiving application by means of a multi-step progressive method on a graphical display on a user terminal. The general method of the present invention is illustrated in **Figure 1**. Visualization process **100** begins by executing two or more entities or applications which have engaged in such interactions, in which at least one device or application is deemed to be trustworthy by the user of interest. Visualization outcomes **110** as iteratively computed on this trusted device or application is provided to be the reference visualization. The equivalent outcomes on the other entities and/or applications previously engaged are provided as the test visualizations. User then determines authenticity **112** of the test visualization by comparing the test visualization against the reference visualization.

For instance, if the outcome of the comparison is similar, this indicates satisfactory authentic conclusion for prior interaction as characterised by input codeword P. To the contrary, if the outcome of the comparison is dissimilar, this indicates an unsatisfactory inauthentic conclusion.

Visualization process **110** is computed on the basis of a N-dimensional hyper-cubic representation, with each axial component $[i] = 0 \dots N_i - 1$ partitioned to degree N_i . Visualization process **110** requires specification of visual mapping field Q over hyper-cube $[i]$; and consequent to aforesaid specification, computation of field value $Q[i]$ for each cell, with cell index $i = 1 \dots N'$ for $N' = \prod_i N_i (= 1 \dots N)$ as the product of all axial partitions, spanning entirety of aforesaid N-dimensional representation.

35

Each field valuation $Q[i]$ would be in range $0 \dots N_0 - 1$, with N_0 being the range of the colour representation scheme used for particular instance of visualization 100. Encoding capacity of each visualization step 110 can therefore be established as $N'' = N_0 * N' = \pi_i$ ($= 0 \dots N$) N_i , as the product of colour map range N_0 and hyper-cubic geometric partition N' of visualization object 112.

Exemplary embodiments of the visualization geometry of display object 112 allows assumption of values as follows:-

- $N = N_i = 2$ for two-dimensional binary-square;
- $N = 3, N_i = 2$ for three-dimensional binary-cube;
- $(N, N_1, N_2) = (2, 2, 2)$ for tetrahedron, with $N' = 4$ triangular surfaces;
 $(2, 2, 3)$ for cube, with $N' = 6$ square surfaces;
 $(2, 2, 4)$ for octahedron, with $N' = 8$ triangular surfaces;
 $(2, 2, 6)$ for dodecahedron, with $N' = 12$ pentagonal surfaces;
 $(2, 4, 5)$ for icosahedron, with $N' = 20$ triangular surfaces.

Exemplary embodiments of the colour value for each cell of display object 112 allows assumption of values as follows:-

- $N_0 = 2^{**8} = 256$ for 8-bit colour or greyscale representations
- $N_0 = 2^{**16} =$ for 16-bit representations

When executing word-to-cell visualization 110, of particular cryptographic input 111 into visual-map 112, the iterative steps comprise partitioning of visual object $[i]$ of particular step n into N' sub-cells, where N' is the degree to which display object is partitioned for mapping process. Then, segmentation of input codeword $P[i]$ 111 of same step n into N' sub-words is provided, with equal degree N' of codeword segmentation. Subsequently, computation of visualization value $Q[i]$ for each sub-word $P[i]$, for $i = 0 \dots N' - 1$ is provided. Finally, display of visualization $Q[i]$ 112 by means of colour assignment $Q[i]$ for each cell $[i]$.

In one aspect of the method of the present invention, the cell colourisation $Q(P)$ corresponding to codeword segment P is executed in zero knowledge (ZK) manner such that deduction of input segment P from output visualization $Q(P)$ is infeasible, discovery of alternative segment P' such that $Q(P') = Q(P)$ is infeasible; and discovery of random segments (P', P'') such that $Q(P') = Q(P'')$ is infeasible.

This specification is equivalent to that associated with the inputs and outputs of cryptographic hash functions, and ensures that minor differences between dissimilar segments (P, P') such that strictly unequal $P \neq P'$ results in major differences in corresponding visualizations (Q, Q') which are clearly and unambiguously perceptible to user. Therefore, the use of hash functions is provided to accomplish the outcomes necessary for visualization step **110**.

Visualization **110** can progress to subsequent step at more detailed resolution of cryptographic codeword **111**, provided that information content of visualization input P as aforesaid exceeds encoding capacity N'' of visualization output **112**, as applicable from geometry and colourisation of display object. Visual limit **120** is therefore attained if the range of all possible values of input codeword P at step [n] is less than encoding capacity N'' of single visualization step. Visualization process cannot then be continued in meaningful terms at step [n+1], and is consequently terminated at **121**.

In one aspect of the method of the present invention, user compares test and reference visualization objects **112**, and undertake determination **130** as to whether computations of additional visualizations are required. If the outcomes for which the aforesaid visualizations are clearly dissimilar, no further computation is required, and this implies that the corresponding input codewords **111** are dissimilar. User therefore chooses to undertake termination **130** of the visualization process **110**, and to conclude that prior cryptographic interaction did not result in satisfactory authentic completion. User might alternatively conclude that comparison of visualizations at this step is sufficient to allow for conclusion that aforesaid interaction concluded in satisfactory manner, and correspondingly engage in elective termination **130** of visualization process **110**.

A preferred embodiment of the present invention, provides for use of a trusted device equipped with a camera to capture visual object resulting from test visualization, and additionally graphical screen to display object resulting from reference visualization; and simultaneously test object as overlay on reference object.

The continuation **140** of visualization process **100** to subsequent iteration [n+1] of visualization **110** is executed based on the user selection of sub-cell [i] from N' partitions of visual object at present step [n] of visualization, or alternatively automatic selection by system of all partitions of aforesaid object, or alternatively automatic random selection by

system of one or more partitions; and consequently selection of corresponding singular or plural sub-words $P[i]$ from N' segments of input codeword at present step to be used as input into subsequent step $[n+1]$ of visualization **110**.

5

Partition process in which visual object of visualization step **110** is divided into N' constituent cells is illustrated in **Figure 2**. A particular cell **200** of dimensionality N from preceding step $[n-1]$ is presented as input into present step $[n]$. Partition process **201** divides input cell **200** into N' equal partitions, each of which might be used as input into subsequent step $[n+1]$.

10

Cell **200** can subsequently be described in terms of internal index $[i] = [i_1, \dots, i_N]$ of dimensionality N , with each axial component i_k is furthermore segmented into N_k divisions, with values in range $0 \dots N_k - 1$; resulting in partition **201** of cell into $N' = \pi_{i_k} (= 1 \dots N) N_k$ sub-cells; and subsequent selection **202** of one or more sub-cells $[i]$ from range of N' possible partitions of input cell at present step.

15

Partition process is subsequently repeated, if not terminated as specified by visualization limit **121** or user action **131**, at step $[n+1]$ of visualization **110**, with selected partitions **210** from step $[n]$, subject to partitioning **211** identical to equivalent process **201** at previous step; and selection **212** similarly identical to equivalent **202** at previous step.

20

Segmentation process in which input codeword into visualization step **110** is divided into N' constituent words is illustrated in **Figure 3**. Particular segment **300** from preceding step $[n-1]$ is presented as input into present step $[n]$. Segmentation process **201** divides input cell **200** into N' equal segments, each of which might be used as input into subsequent step $[n+1]$. Degree of segmentation N' for each codeword is identical to degree of partitioning for each visual object. Segmentation **201** might furthermore insert bits of random value into alternating segments to ensure that all segments are of uniform length. Segmentation process is subsequently repeated, if not terminated as specified by visualization limit **121** or user action **131**, at step $[n+1]$ of visualization **110**, with selected segments **310** from step $[n]$, subject to segmentation **311** identical to equivalent process **301** at previous step and selection **312** similarly identical to equivalent **302** at previous step.

25

Computation of visual representation Q for codeword P of interest at each step $[n]$ is as illustrated in **Figure 4**. Codeword segment of interest $P[k]$ **401** for $k = 0 \dots N' - 1$ from previous step $[n-1]$ is presented as input to hash function Q' **400**, resulting in internal

30

- representation $P'[k]$ **402** of hash output, with equivalent segment index. In one aspect of the method of the present invention, the hash Q' on codeword segment P is executed in zero knowledge (ZK) manner such that deduction of P from $Q'(P)$ is infeasible; discovery of alternative segment P_1 such that $Q'(P_1) = Q'(P)$ is infeasible and discovery of random segments (P_1, P_2) such that $Q'(P_1) = Q'(P_2)$ is infeasible. Hash output P' **402** is subsequently presented as input to colourisation function Q'' **410**, resulting in visual representation $Q[i]$ **411** with N-dimensional spatial partition index $[pi_i] = [i_1, ..., i_N]$ of equivalent representational dimensionality to segment index of P' .
- 10 In one aspect of the present invention, colourisation $Q''(P')$ on codeword digest P' is executed in zero knowledge (ZK) manner such that deduction of P' from $Q''(P')$ is infeasible, discovery of alternative segment P'_1 such that $Q''(P'_1) = Q''(P')$ is infeasible; and discovery of random segments (P'_1, P'_2) such that $Q''(P'_1) = Q''(P'_2)$ is infeasible.
- 15 Colour map Q'' **411** is then presented to human user for inspection, and possible selection of portion $[i]$ with multi-dimensional index $pi_i = 0 \dots N' - 1$, for visualization of corresponding codeword segment $P'[k]$ of equivalent index. Map index $[i]$ of chosen partition is subsequently presented as input to association function $Q\sim$ **420**, enabling selection of corresponding codeword segment $P'[k]$ with $k = Q\sim(i)$. The association $k = Q\sim(i)$ of codeword
- 20 index with selected map index i is executed in a zero knowledge (ZK) manner such that deduction of i from $k(i)$ is infeasible, with the effectiveness of any such deduction equivalent to random selection from all possible index associations.
- Hash $Q'(P)$ **400**, colourisation $Q''(P')$ **410**, and index association $Q\sim(i)$ **420** are furthermore
- 25 specified with input dependency on step index $[n]$, with a zero knowledge (ZK) relationship between equivalent parameters in successive steps, such that deduction of parameters at previous step $[n-1]$ from equivalent parameters at present step $[n]$ is infeasible, deduction of alternative parameters at step $[n-1]$ resulting in equal value of equivalent parameters at step $[n]$ is infeasible and deduction of two distinct sets of random parameters at step $[n-1]$
- 30 resulting in equal value at step $[n]$ is infeasible.
- Hash Q' **400**, colourisation Q'' **410** and index association $Q\sim$ **420** are additionally specified with input dependency on external key **501**, such dependence resulting from modification of Q' , Q'' and $Q\sim$ functions by means of key mixing function Q_k **500**. This mixing function **500**
- 35 is specified with a zero knowledge (ZK) relationship with respect to key input k **501**, such

that deduction of k from output of mixing function used as inputs in Q' , Q'' and $Q_{\sim}$ is infeasible; and deduction of k from resultant outputs of Q' , Q'' and $Q_{\sim}$ is infeasible.

Visual representation of the present invention is generated so as to be dependant on input key, or independant thereof. This applies to cryptographic codewords deemed to have either short or long-term effective duration. Representations of visual object used in the present invention is as a two-dimensional planar map or three-dimensional volumetric solid, with distinct colour value assigned to each cell in representation, and with cells of visual object furthermore subject to user interaction at each progressive step of visualization.

Comparison of test and reference visualizations is undertaken by comparison, at each of multiple progressive steps, of test visual object against reference visual object at particular step of interest, with reference object as it appears on graphical display of application deemed to be trustworthy by user. Alternatively, comparison is undertaken by means of superposition of test visual object, as captured by camera on application deemed to be trustworthy by user, and reference visual object on graphical display of said trusted application. A cryptographic hash function is used to compute colour corresponding to each input segment, corresponding to key-independant visualization.

EXEMPLARY EMBODIMENTS

General representation comprising N -dimensional hypercube: with

- Segmentation into $N' = N_1 * \dots * N_N$ cells.
- Visual map Q specified over hypercube.
- Value $Q[i]$ in encoding range $0 \dots (N_0 - 1)$ with:-
- (*) $[x] = (x_1, \dots, x_i, \dots, x_N)$ denoting vector index denoting cell location in hypercube,
- (*) $x_i = 0 \dots (N_i - 1)$ denoting index component value, and
- (*) N_0 denoting colour depth, with
- Encoding range of $N'' = N_0 * N'$ for Q at initial step, and also at each subsequent progressive step.

Important special representations are inclusive of:-

- $N = N_i = 2$ for planar binary square.

- $N = 3$, $N_i = 2$ for volumetric binary-cube.
- $N_0 = 2^{**8} / 16$ for 8/16-bit colour depth.

Representations are also inclusive of non-cartesian constructions, as exemplified by the five regular solids. These constructions can be represented as planar projections, or as volumetric objects, as follows:-

- Tetrahedron: equivalent to $(N, N_1, N_2) = (2, 2, 2)$ cube, with $N' = 4$ triangular surfaces per step.
- Cube: $(2, 2, 3)$ representation, with $N' = 6$ square surfaces.
- Octahedron: $(2, 2, 4)$ representation, with $N' = 8$ triangular surfaces.
- Dodecahedron: $(2, 2, 6)$ representation, with $N' = 12$ pentagonal surfaces.
- Icosahedron: $(2, 4, 5)$ representation, with $N' = 20$ triangular surfaces.

The basic concept of present invention is to repeat visualization, as represented by visual object colourisation, on progressively smaller segments of the input codeword, or alternatively to stop at visualization limit.

Method of present invention requires execution at n-th step: $n=1, 2, \dots$ of

- Partition of cell-of-interest $[i, n]$ into N' sub-cells.
- Segmentation of input-word $P[i, n]$ into N' sub-words, each associated with corresponding sub-cell.
- Compute visualization by colour $Q[i, n] = Q(P[i, n])$ for each sub-word mapped to corresponding sub-cell.
- Test limit condition: as to whether information content of next cell-of-interest $[i, n+1]$ less than encoding range N'' of visualization
- If limit condition has been attained then stop, else progress to subsequent $(n+1)$ -th step.

Method of invention furthermore requires at initial step comprising:-

- Segmentation of input codeword P into N' words $P[i, n(=1)]$, each corresponding to cell $[i, n(=1)]$ at initial step $n=1$; based on premise that
- P has value range greater than encoding range N'' of Q , and hence that
- $P[i]$ value range is greater than colour representation at location $[i]$; Such that
- Specification of visual map $Q[i, n(=1)]$ can be undertaken at $[i]$, by means of

- Application of – colour map $Q = Q[i](P)$ such that $P[i]$ is represented as colour $Q[i]$ at $[i]$.

Method of invention then requires progressive (n-th) step comprising:-

- 5 • 1-of- N' selection of cell $[i,n]$, with associated word $P[i,n]$, from cell $[i',n-1]$ of previous step.
- Segmentation of cell-of-interest $[i]$ into N' sub-cells as per previous steps.
- Corresponding and equivalent segmentation of word $P[i]$ into N' sub-words.
- Application of colour map $Q = Q(P)$ for particular internal index values.
- 10 • Test of limit condition as to whether information content of $P[i]$ exceeds encoding range of Q at present step, with repetition of progressive step for negative test outcome, or termination for positive test outcome.

Method of invention has additional aspect of progressive steps which can be executed in one of the following modes :-

- Local progression: in which single 1-of- N' selection is undertaken at each step, resulting in additive visualization of $O(n*N')$ after n steps.
- Global progression: in which all N' cells are selected at each step, resulting in multiplicative visualization of $O(N'^{**}n)$ after n steps, and therefore faster convergence to full information content of input codeword.
- 20

Method of invention has additional aspect of key-dependant variation, which requires:-

- Key-dependant map $Q'_k(P)$, with external input k , in lieu of key-independant map $Q(P)$, and furthermore
- 25 • ZK re-mapping of base-step input and/or output into key-dependant map $Q'(P) = (Z_k \circ Q \circ Z'_k)(P)$.

$[i,n]$ respectively denote the internal spatial and step indices for the visualization object, which are transparent to external observation. Cell $[i,n]$ is of smaller spatial extent for progressive step values n . Word $P[i,n]$ is of correspondingly shorter bit-length.

$Q[i,n]$ is specified so as to be subject to spatial -and step-wise variation.

Q should assume the zero knowledge (ZK) irreversibility and collision-resistive properties of cryptographic hash functions, such that codeword segment $P[i]$ cannot be deduced from

colour assignment $Q[i]$, and furthermore such that it is infeasible to generate collisions – of form $Q(P) = Q(P')$ for $P \neq P'$. Q can therefore be constructed from hashing primitives.

Key-dependency can be implemented in various ways, inclusive of - step-specific key schedules of form $k[n]$ and key-specific cell permutations of form $i'_k[i] = i'_k[i, n]$. Simple implementation of key-dependance of form $Z_k = Z'_k = h_k$ can be implemented via a hash message authentication code (HMAC) block on either or both sides of the base-step colorization function. Cell selection for progressive computation could be by means of point-and-click (via mouse) or touch (via touch-screen).

Configurations of the method of the present invention may be implemented by hardware, software, firmware, middleware, microcode, or a combination thereof. When implemented in software, firmware, middleware, or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine-readable medium such as a storage medium or other storage means. A processor may perform the necessary tasks. A code segment may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or a combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, and the like, may be passed, forwarded, or transmitted via a suitable means including memory sharing, message passing, token passing, and network transmission, among others.

One of the advantages of the present invention is to provide for representation of long high-entropy codewords as perceptually significant visual images on graphical displays. These codewords occur in the context of cryptographic protocols, and typically range in length from 128 to 1024-bits. By computing visual representations at more detailed scales of resolution in each progressive step-, this allows human visual inspection which is secure, effective and ergonomic.

Another advantage of the method of the present invention is that it computes visually simple (and therefore ergonomic) representations at each step of progressive computation, with the complexity of the visualization process (as would necessarily arise from the entropy content of cryptographic codewords) dispersed over the multiple steps of progression. This provides

for the user to determine whether visualised cryptographic input is authentic by means of a process which can range from simple to exhaustive, with the level of thoroughness proportional to number of user interactions with the particular visualization object. Authentication of the input codeword would be assessed by means of comparing test
5 visualization against reference visualization at each progressive step, the latter of which is executed on a platform deemed to be trustworthy by the user.

In addition, the method of the present invention is able to compute representation as dependent on explicit (key-specific) and/or implicit (context-sensitive) system inputs. These
10 keyless and key-dependent modes are respectively analogous to hash functions and hashed message authentication codes (HMAC). Existing solutions based on standard protocol frameworks (inclusive of SSL, TLS and IPsec) are primarily concerned with the security of machine-to-machine (inclusive of server-to-client/browser and client-to-server) interactions. User-to-machine security elements (inclusive of passwords and/or physical tokens) are
15 usually implemented external to the protocol frameworks, but would still not address the issue of reciprocal system-to-user authentication. This problem is addressed by the method of the present invention.

The foregoing embodiment and advantages are merely exemplary and are not to be
20 construed as limiting the present invention. The description of the embodiments of the present invention is intended to be illustrative and not to limit the scope of the claims and many alternatives, modifications and variations will be apparent to those skilled in the art.

25

30

35

CLAIMS

1. A method for visual authentication of high-entropy parameters by a receiving application
5 on the graphical display of a user terminal, comprising

generating a test visualization on receiving application;

generating a reference visualization on application deemed to be trustworthy by the
user; and

10 displaying the test visualization and the reference visualization on the graphical
displays of receiving and trusted application; and

determining the authenticity of the tested visualization by comparing the test
visualization against the reference visualization

15 wherein a visual representation is provided for visual authentication of high-entropy
parameters of a receiving application on the graphical display of a user terminal,
wherein high-entropy parameters are cryptographic codewords of variable length and
effective duration, with the visual representation undertaken in discrete progressive
steps resulting in visualization progressing from gross to fine resolution, by a
controlled system.

- 20 2. The method as claimed in Claim 1 wherein the receiving application processes
visualization on progressive scales of resolution, from gross to fine visual resolution in
progressive steps.

- 25 3. The method as claimed in Claim 1 wherein the visual representation is generated by
dependant on input key.

- 30 4. The method as claimed in Claim 1 wherein the visual representation is generated by
independant on input key.

- 35 5. The method of as claimed in Claim 1 in which comparison of test and reference
visualizations is undertaken by means of superposition of test visual object, as captured
by camera on application deemed to be trustworthy by user, and reference visual object
on graphical display of said trusted application.

6. The method as claimed in Claim 1 wherein the visual representation is computed on a segment of the input high-entropy parameter at each progressive step.

7. The method as claimed in Claim 1 wherein the visual representation is executed as colour value computed from the numerical or symbolic value of the input high-entropy parameter on the segment at each progressive step.

8. The method of as claimed in Claim 6 wherein representations of visual object is as a two-dimensional planar map or three-dimensional volumetric solid, with distinct colour value assigned to each cell in representation, and with cells of visual object furthermore subject to user interaction at each progressive step of visualization.

9. The method as claimed in Claim 6 wherein segmentation of visual representation displayed on the graphical display of a user terminal is of equal degree to segmentation of input parameter segment represented, at each progressive step of computation.

10. The method as claimed in Claim 8 wherein a cryptographic hash function is used to compute colour corresponding to each input segment, corresponding to key-independent visualization.

11. The method as claimed in Claim 8 wherein a hash-based message authentication code (HMAC) is used to compute colour corresponding to each segment with hash-based message authentication code (HMAC) key as key parameter, which is presumed to be secret.

12. The method as claimed in Claim 1 wherein the receiving application executes as a test visualization comprising word-to-cell visualization of high-entropy input parameter into a visual-map in iterative steps, further comprising

providing a partition of visual object [i] of particular step n into N' sub-cells, where N' is the degree to which display object is partitioned for mapping process;

providing a segmentation of input codeword P[i] of same step n into N' sub-words, with equal degree N' of codeword segmentation;

providing a computation of visualization value Q[i] for each sub-word P[i],

for $i = 0 \dots N' - 1$; and

displaying visualization value $Q[i]$ by means of colour assignment $Q[i]$ for each cell $[i]$.

13. The method as claimed in Claim 12 wherein a cell colourisation $Q(P)$ corresponding to codeword segment P is executed in a zero knowledge (ZK) manner.

5

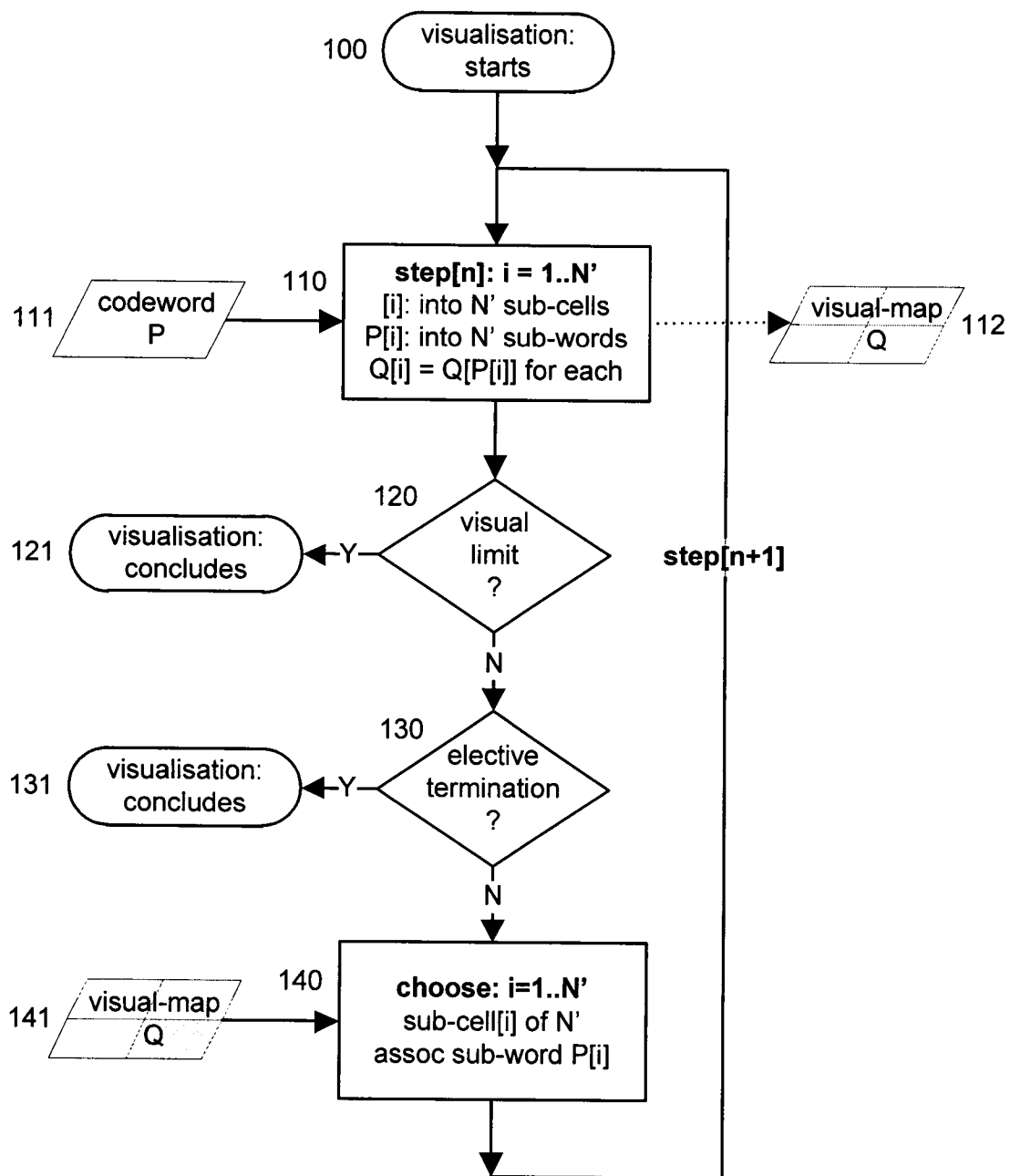
14. The method as claimed in claim 12 in which next step of visualization is undertaken on the basis of user or random system selection of one or more partitions on visualization object, or alternatively system selection of all partitions on visualization object.

10 15. The method as claimed in Claim 13 wherein visualization limit is provided if a range of all possible values of input codeword P at step n is less than encoding capacity N'' of single visualization step, where N'' is encoding capacity of visualization output from geometry and colourisation of display object, and to also provide for termination of visualization if such limit is attained in visualization computation.

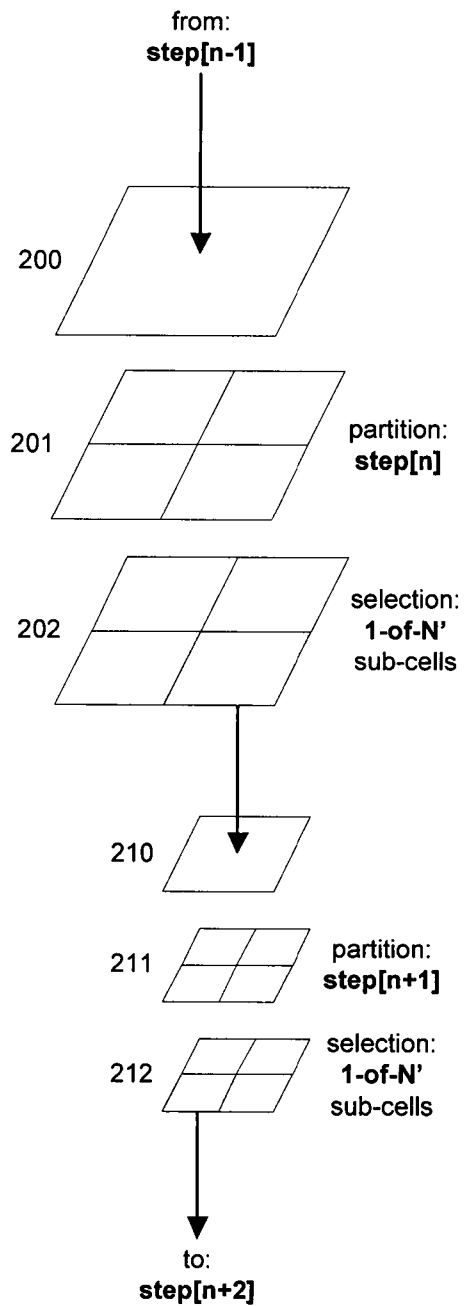
15

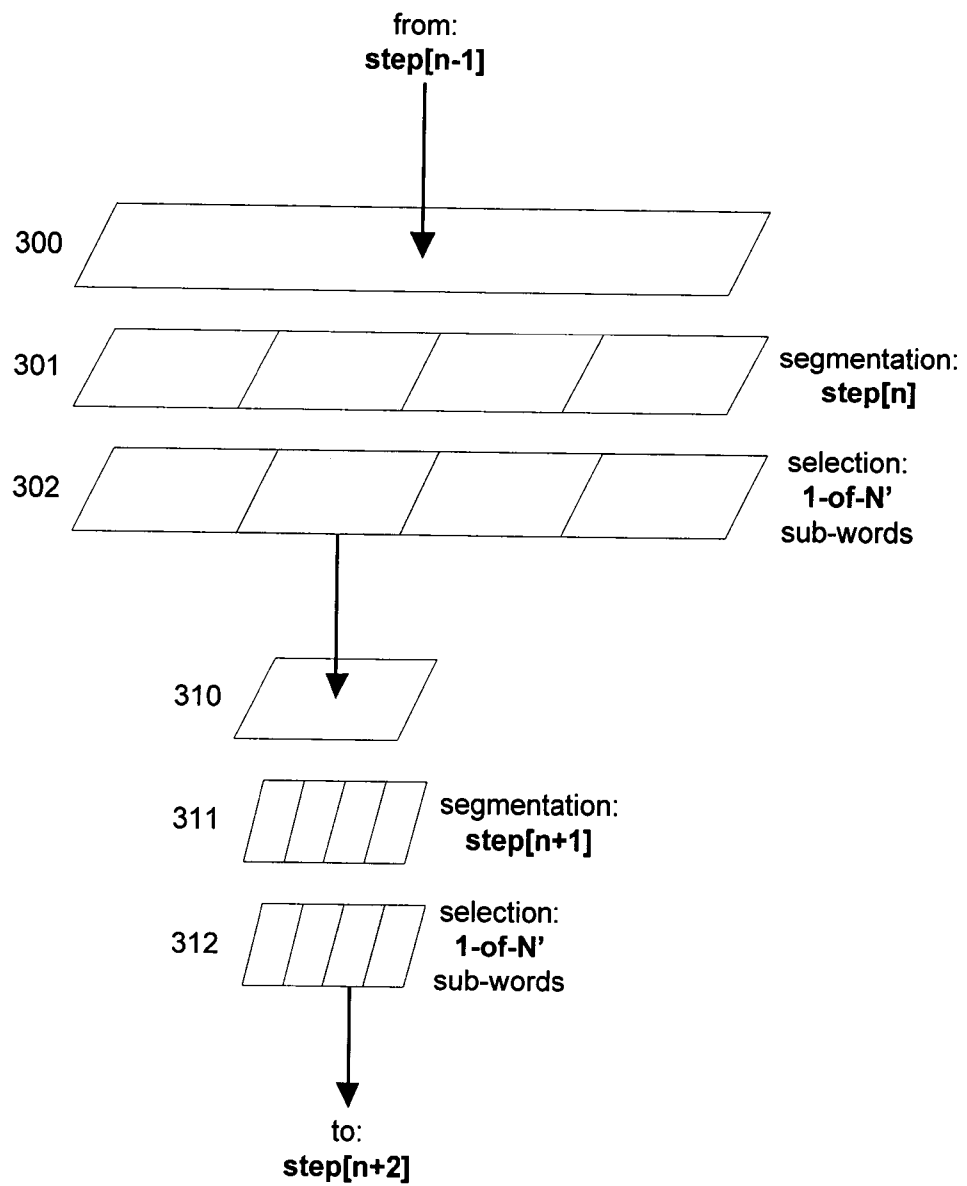
20

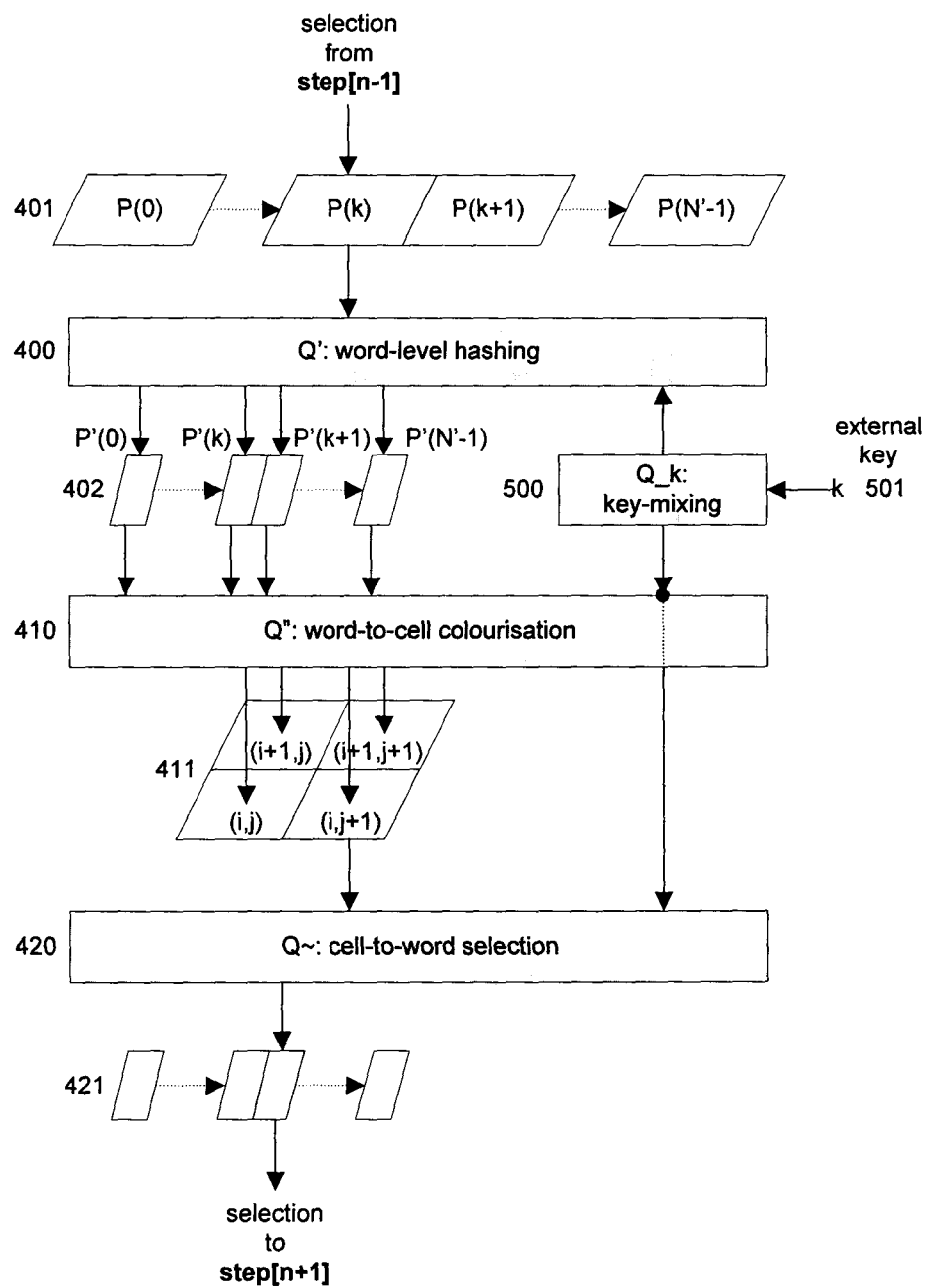
25

**Figure 1**

2/4

**Figure 2**

**Figure 3**

**Figure 4**

INTERNATIONAL SEARCH REPORT

International application No

PCT/MY2014/000187

A. CLASSIFICATION OF SUBJECT MATTER

INV. G09C5/00

ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G09C G06F

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, PAJ, WPI Data, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	Sea Chong Seak ET AL: "A Centralized Multimodal Unified Authentication Platform for Web-based Application", Proceedings of the World Congress on Engineering and Computer Science 2014 Vol I WCECS 2014, 22 October 2014 (2014-10-22), XP055164373, San Francisco, USA ISBN: 978-9-88-192520-6 Retrieved from the Internet: URL: http://www.iaeng.org/publication/WCECS2014/WCECS2014_pp227-232.pdf [retrieved on 2015-01-23] paragraph [00IV] ----- -/-	1-15



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 but published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

26 January 2015

Date of mailing of the international search report

03/02/2015

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Bec, Thierry

INTERNATIONAL SEARCH REPORT

International application No

PCT/MY2014/000187

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Dwaine Clarke ET AL: "The Untrusted Computer Problem and Camera-Based Authentication" In: "LECTURE NOTES IN COMPUTER SCIENCE", 1 January 2002 (2002-01-01), Springer Berlin Heidelberg, Berlin, Heidelberg, XP055164018, ISSN: 0302-9743 ISBN: 978-3-54-045234-8 vol. 2414, pages 114-124, DOI: 10.1007/3-540-45866-2_10, paragraph [0005] -----	1-15
Y	Mohammad Mannan ET AL: "Leveraging Personal Devices for Stronger Password Authentication from Untrusted Computers *", , 1 January 2011 (2011-01-01), XP055164011, Retrieved from the Internet: URL:http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.158.5942&rep=rep1&type=pdf [retrieved on 2015-01-21] paragraph [6.2f)] -----	1-15
Y	Sonia Chiasson ET AL: "Graphical Password Authentication Using Cued Click Points" In: "LECTURE NOTES IN COMPUTER SCIENCE", 1 January 2007 (2007-01-01), Springer Berlin Heidelberg, Berlin, Heidelberg, XP055164014, ISSN: 0302-9743 ISBN: 978-3-54-045234-8 vol. 4734, pages 359-374, DOI: 10.1007/978-3-540-74835-9_24, paragraph [0003] -----	1-15
Y	ABDULLAH M JAAFAR ET AL: "Visual Zero-Knowledge Proof of Identity Scheme: A New Approach", COMPUTER RESEARCH AND DEVELOPMENT, 2010 SECOND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 7 May 2010 (2010-05-07), pages 205-212, XP031692829, ISBN: 978-0-7695-4043-6 paragraph [00IV] ----- -/--	12-15

INTERNATIONAL SEARCH REPORT

International application No

PCT/MY2014/000187

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
T	MONI NAOR ET AL: "Visual Authentication and Identification", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH,, 26 August 2000 (2000-08-26), pages 1-19, XP061000022, [retrieved on 2000-08-26] paragraphs [03.4], [0004] -----	
T	INKOO KANG ET AL: "Color Extended Visual Cryptography Using Error Diffusion", IEEE TRANSACTIONS ON IMAGE PROCESSING, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 20, no. 1, 1 January 2011 (2011-01-01), pages 132-145, XP011328680, ISSN: 1057-7149, DOI: 10.1109/TIP.2010.2056376 -----	