US 20070294770A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2007/0294770 A1**

CUENOD et al. (43) **Pub. Date: Dec. 20, 2007**

(54) **METHOD TO PROTECT SOFTWARE AGAINST UNWANTED USE WITH A VARIABLE PRINCIPLE**

(75) Inventors: **Jean-Christophe Emanuel CUENOD**, Montesson (FR); **Gilles Jean SGRO**, Bourg de Peage (FR)

Correspondence Address:
SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037 (US)

(73) Assignee: **SAS VALIDY**, Romans (FR)

(21) Appl. No.: **11/835,204**

(22) Filed: **Aug. 7, 2007**

Related U.S. Application Data

(63) Continuation of application No. 10/178,834, filed on Jun. 25, 2002, now Pat. No. 7,269,740.

(60) Provisional application No. 60/308,824, filed on Aug. 1, 2001.

Publication Classification

(51) **Int. Cl.**
G06F 11/00 (2006.01)

(52) **U.S. Cl.** **726/25**

(57) **ABSTRACT**

The invention concerns a process to protect a vulnerable software working on a data processing system against its unauthorized usage using a memorizing unit. The process comprises creating a protected software by choosing in the source of the vulnerable software at least one variable and by producing the source of the protected software by modifying the source of the vulnerable software, so that the chosen variable resides in the memorizing unit.

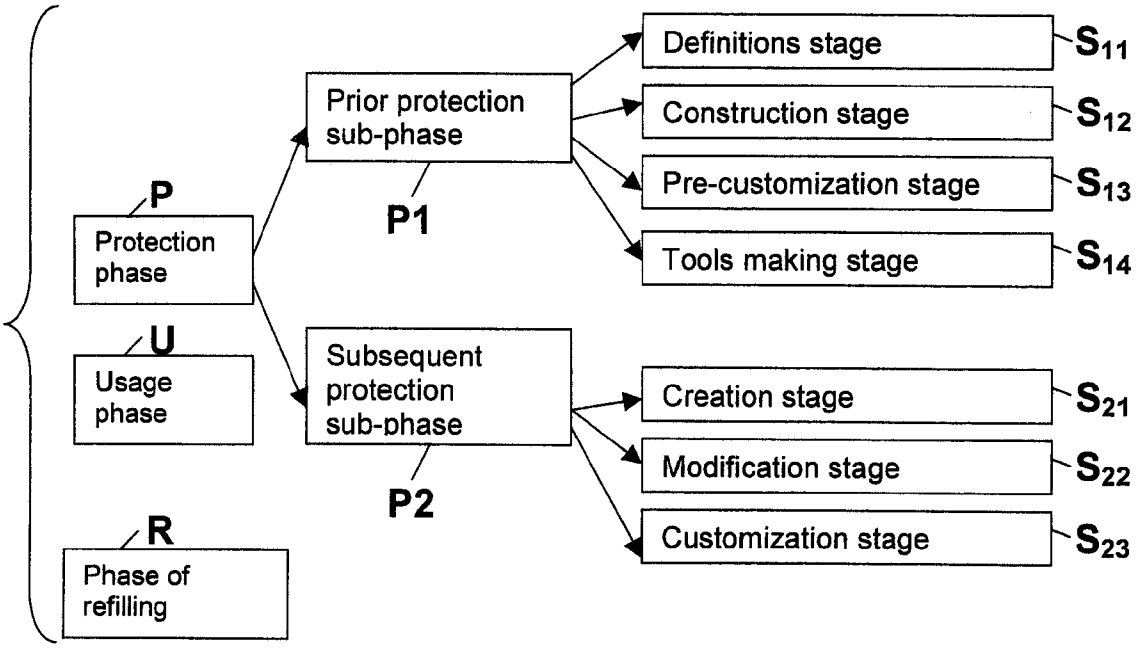


FIG. 10

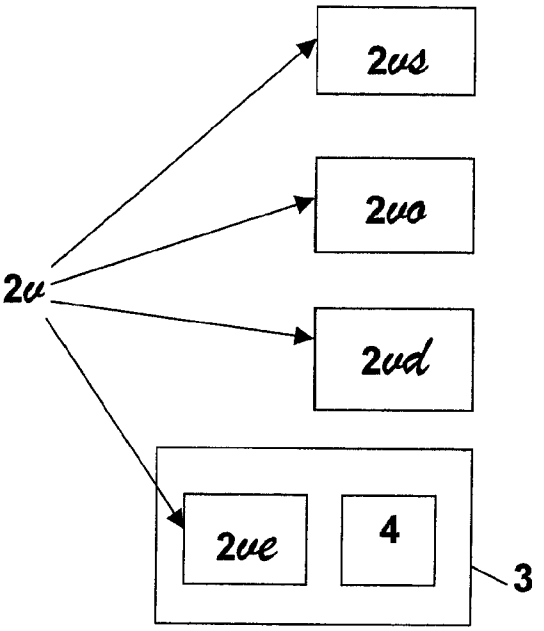

2vs
2vo
2v
2vd
2ve
4
3

FIG. 11

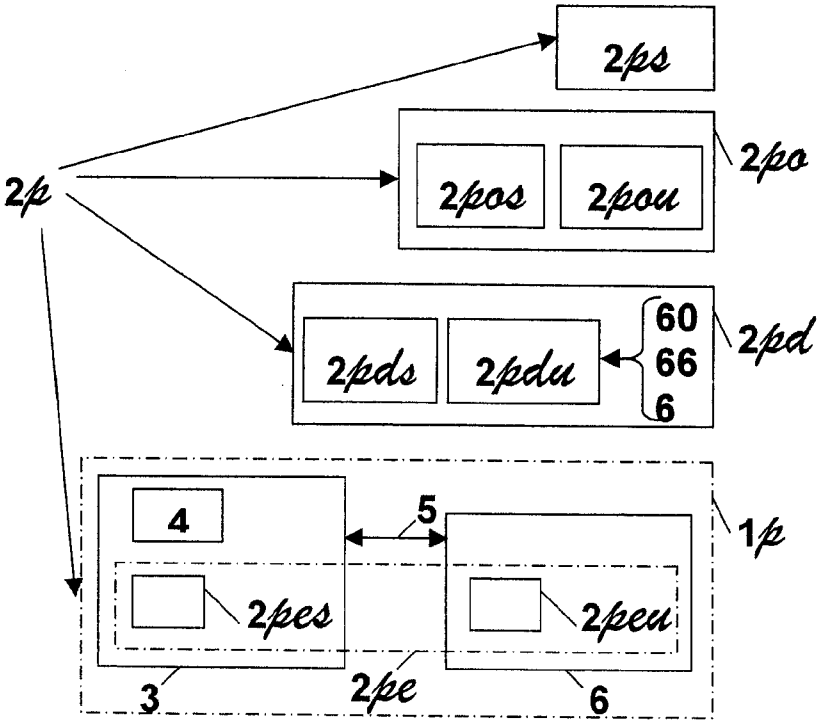

2ps
2p
2pos
2pou
2po
2pds
2pdu
60
66
6
2pd
4
5
1p
2pes
2peu
3
2pe
6

FIG. 20

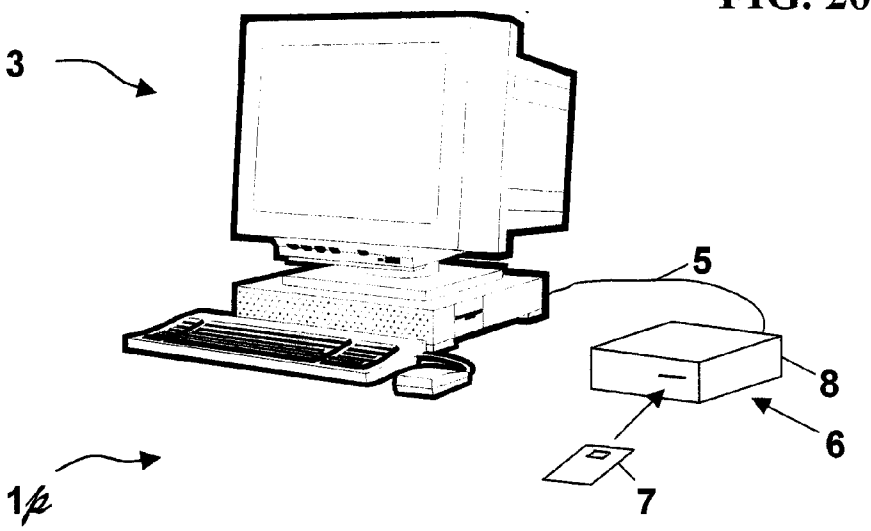


FIG. 21

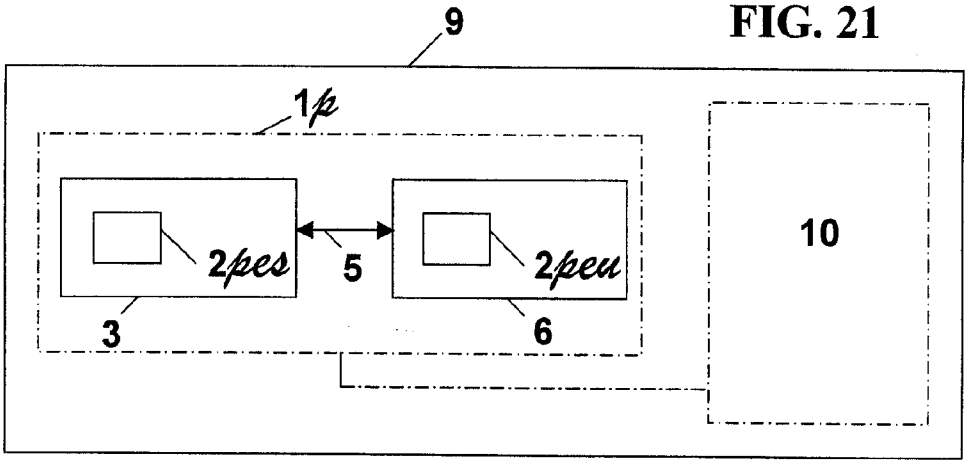


FIG. 22

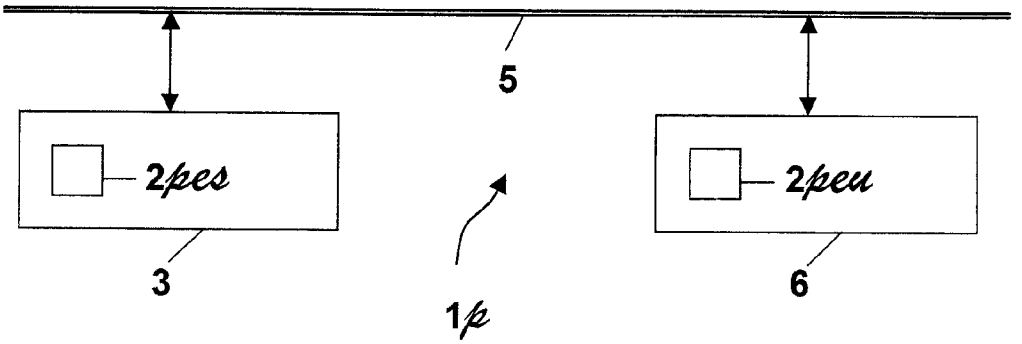


FIG. 30

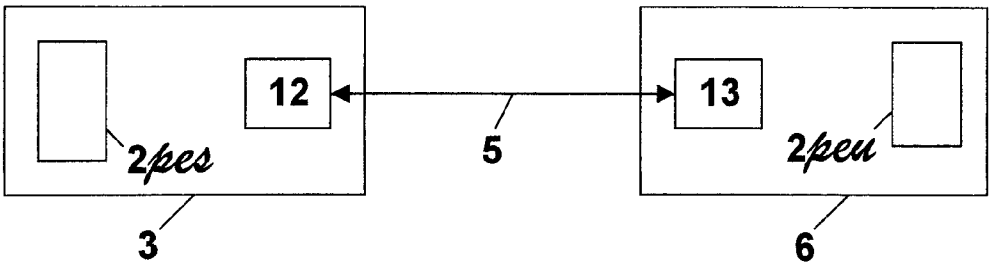


FIG. 31

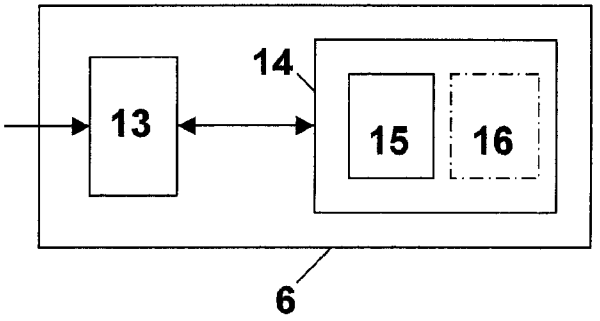


FIG. 40

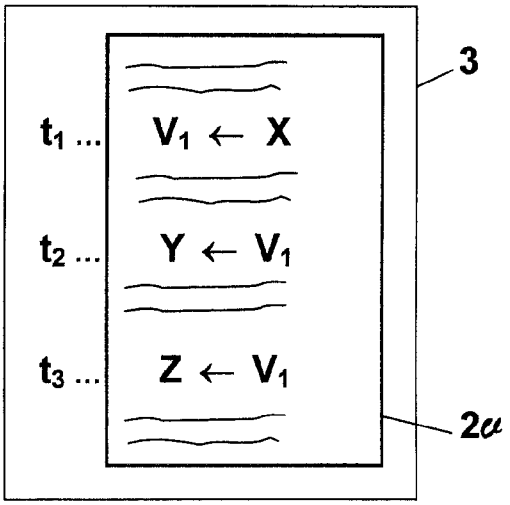


FIG. 41

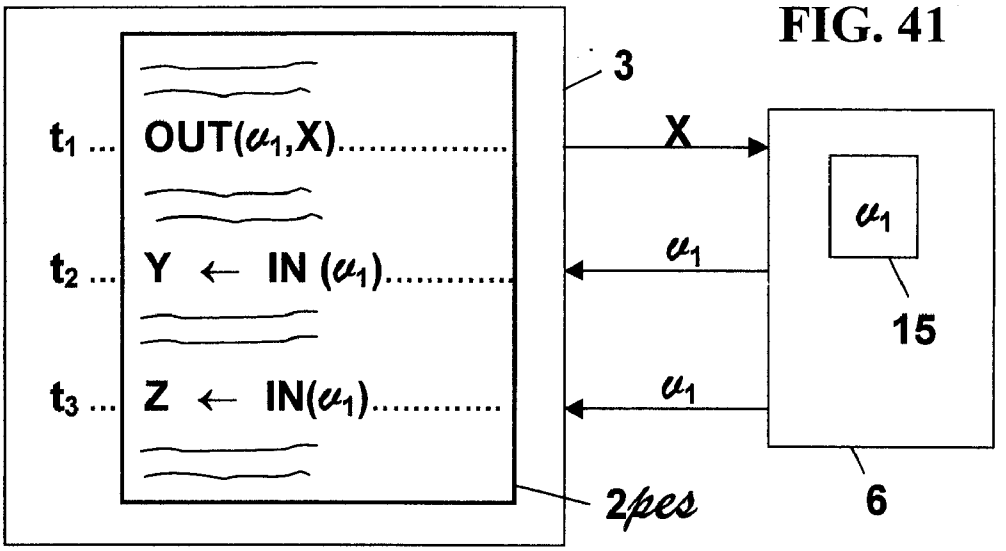


FIG. 42

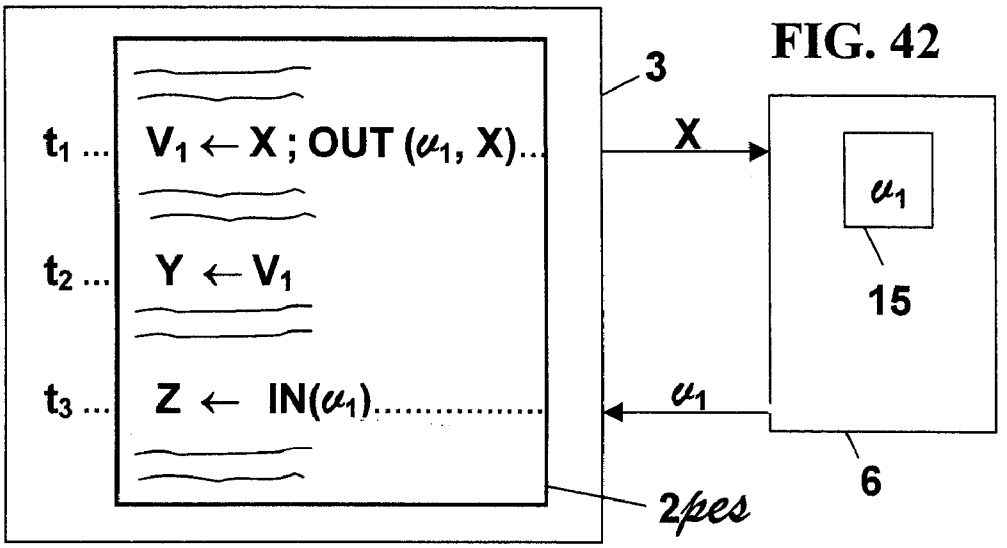
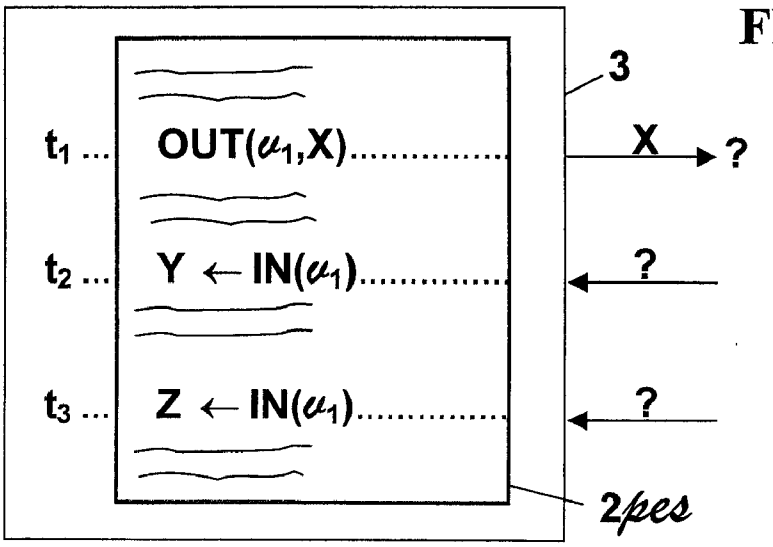


FIG. 43



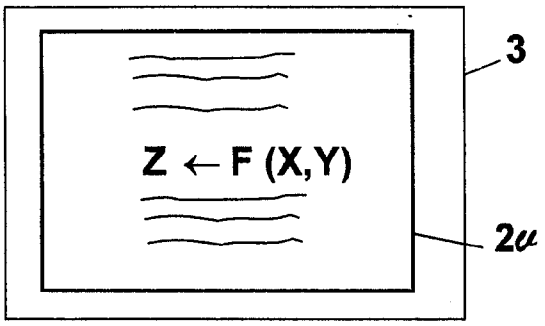


FIG. 50

FIG. 51

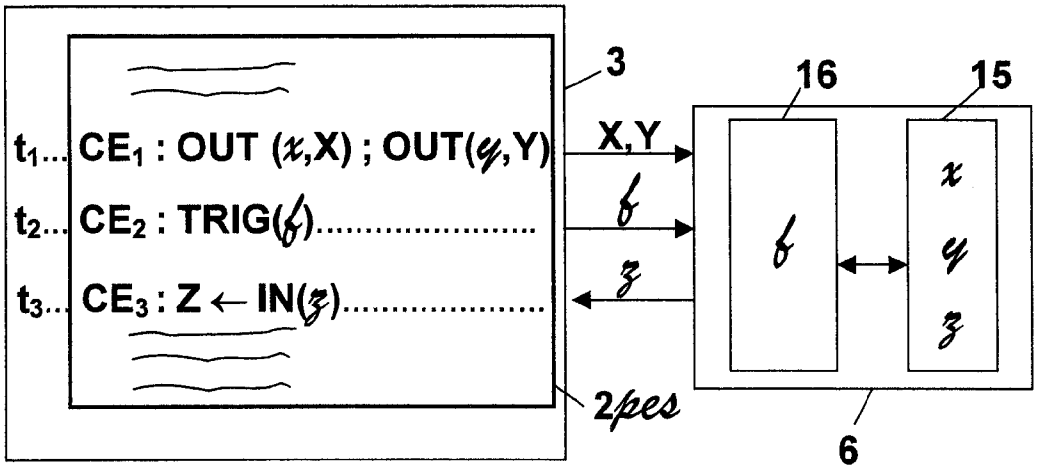


FIG. 52

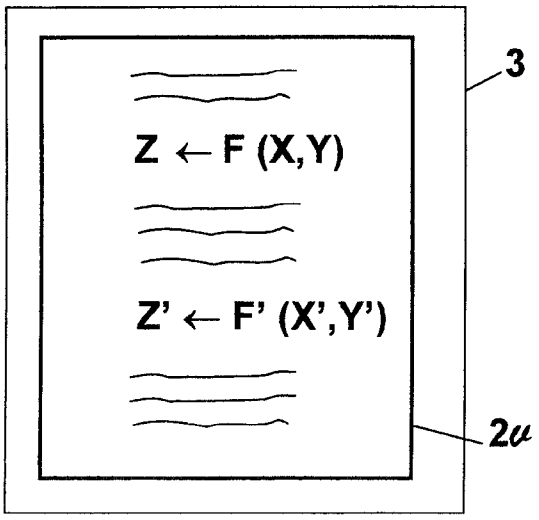


FIG. 53

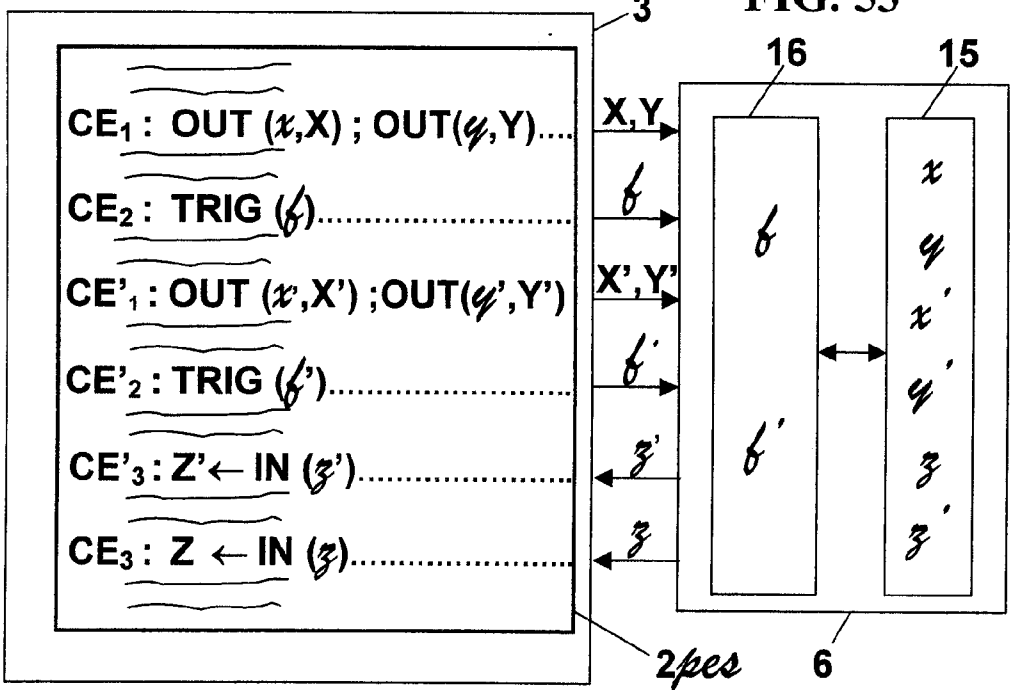


FIG. 54

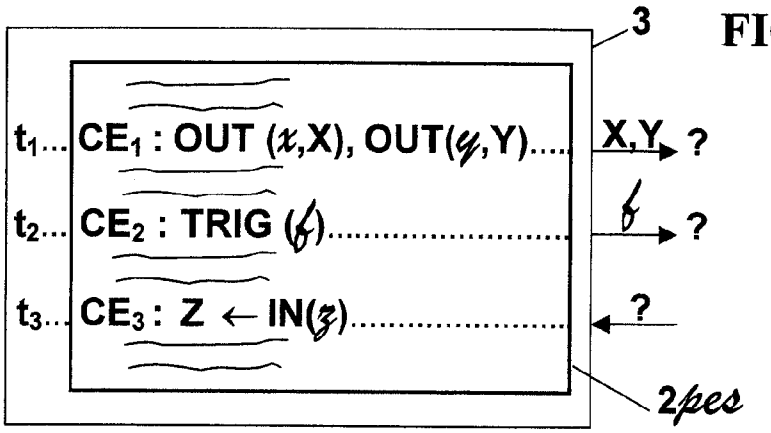


FIG. 60

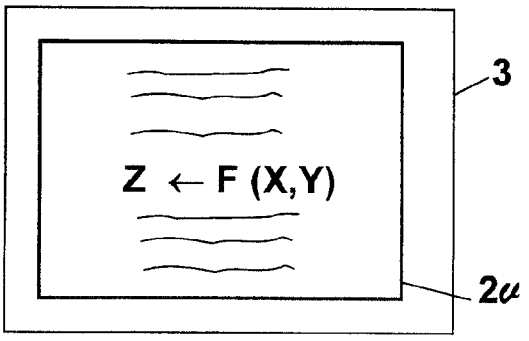


FIG. 61

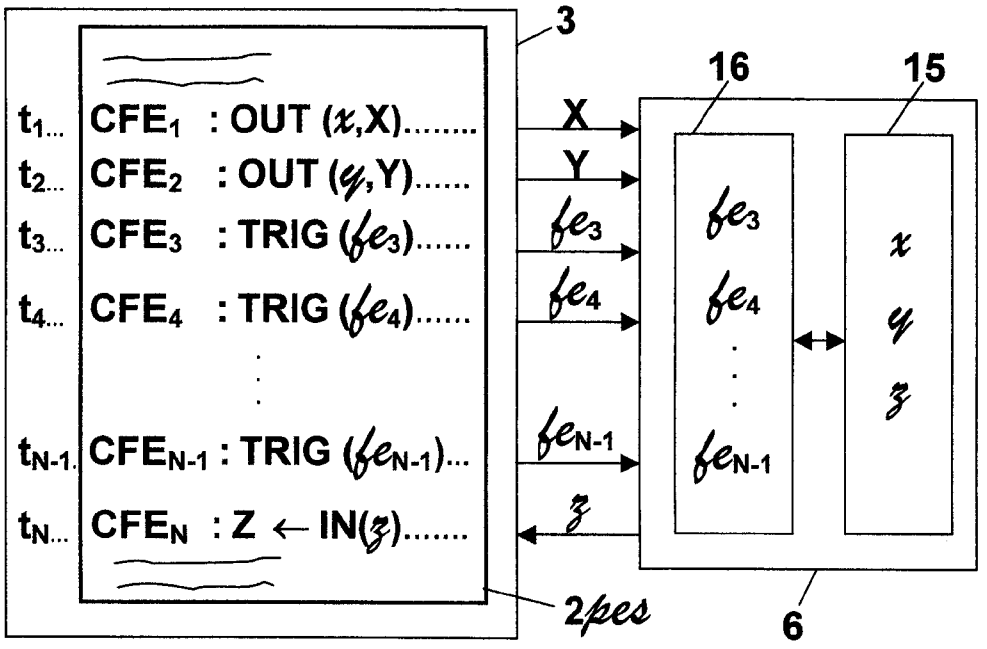

3
16
15
t1...
CFE1 : OUT (x,X).....
t2...
CFE2 : OUT (y,Y).....
t3...
CFE3 : TRIG (fe3).....
t4...
CFE4 : TRIG (fe4).....
tN-1.
CFEN-1 : TRIG (feN-1)...
tN...
CFEN : Z ← IN(z).....
X
Y
fe3
fe4
feN-1
z
fe3
fe4
feN-1
x
y
z
2pes
6

FIG. 62

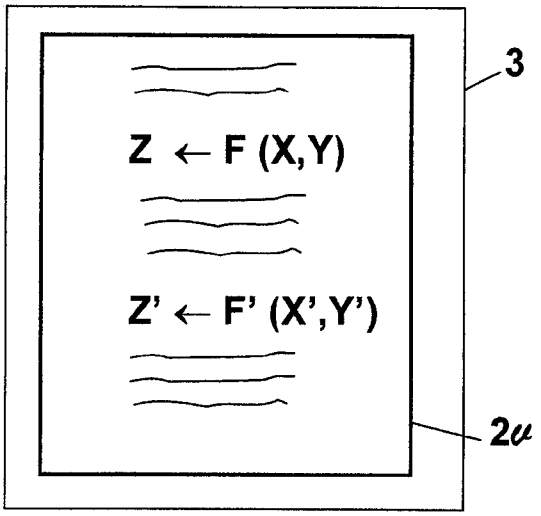

3
Z ← F (X,Y)
Z' ← F' (X',Y')
2v

FIG. 63

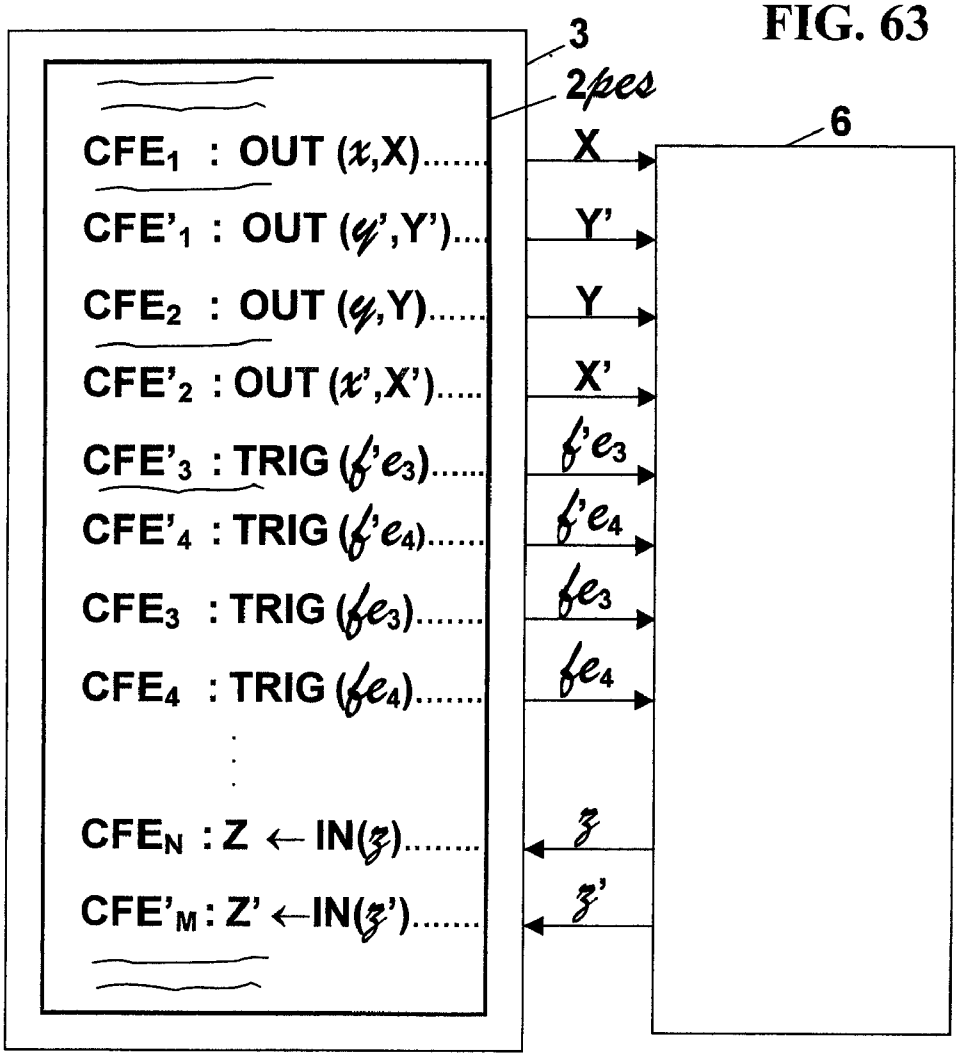

3
2pes
6
CFE1 : OUT (x,X).....
CFE'1 : OUT (y',Y')....
CFE2 : OUT (y,Y).....
CFE'2 : OUT (x',X').....
CFE'3 : TRIG (f'e3).....
CFE'4 : TRIG (f'e4).....
CFE3 : TRIG (fe3).....
CFE4 : TRIG (fe4).....
CFEN : Z ← IN(z).....
CFE'M : Z' ←IN(z').....
X
Y'
Y
X'
f'e3
f'e4
fe3
fe4
z
z'

FIG. 64

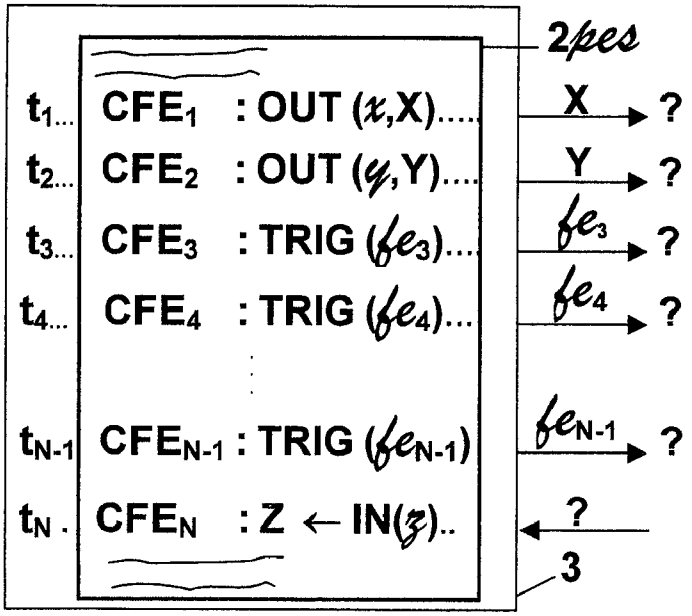

2pes
t1... CFE1 : OUT (x,X)....
t2... CFE2 : OUT (y,Y)....
t3... CFE3 : TRIG (fe3)....
t4... CFE4 : TRIG (fe4)...
tN-1 CFEN-1 : TRIG (feN-1)
tN . CFEN : Z ← IN(z)..
X
Y
fe3
fe4
feN-1
?
3

FIG. 70

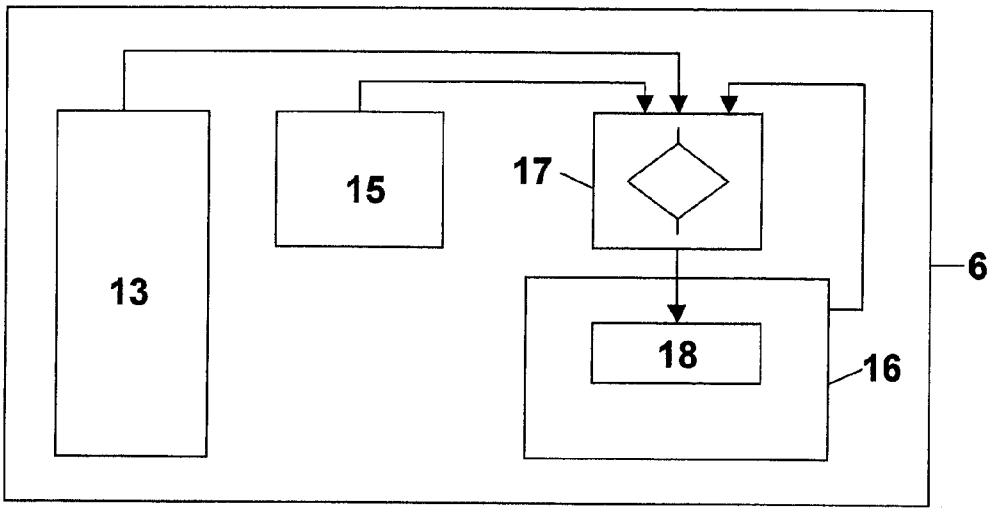

13
15
17
18
16
6

FIG. 71

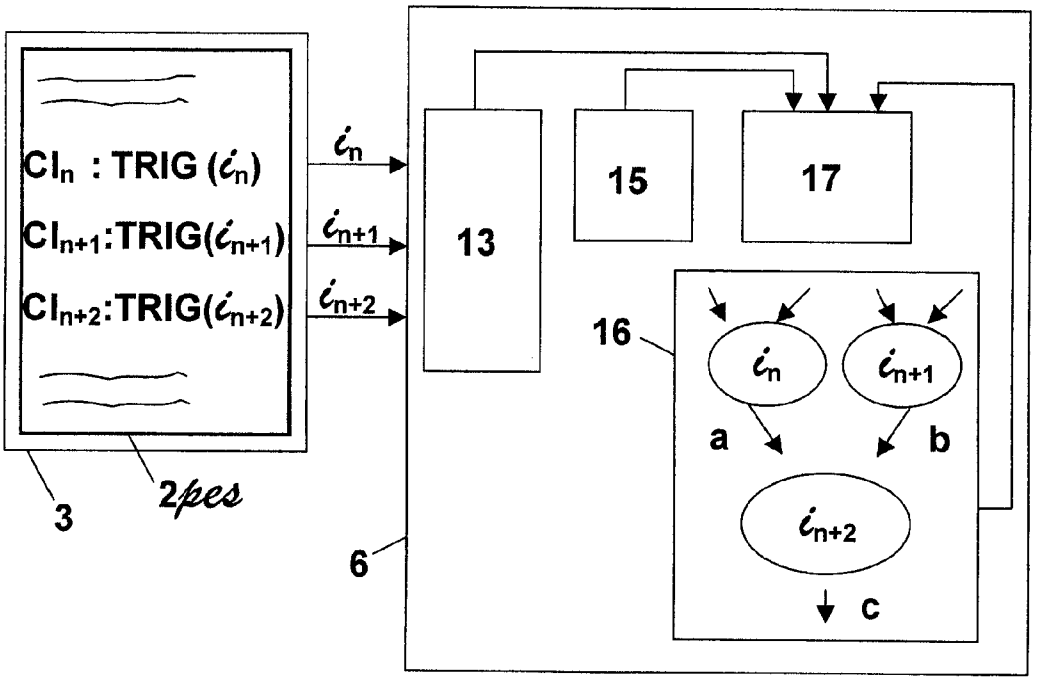

CIn : TRIG (in)
CIn+1:TRIG(in+1)
CIn+2:TRIG(in+2)
in
in+1
in+2
3
2pes
13
15
17
16
in
in+1
a
b
in+2
c
6

FIG. 72

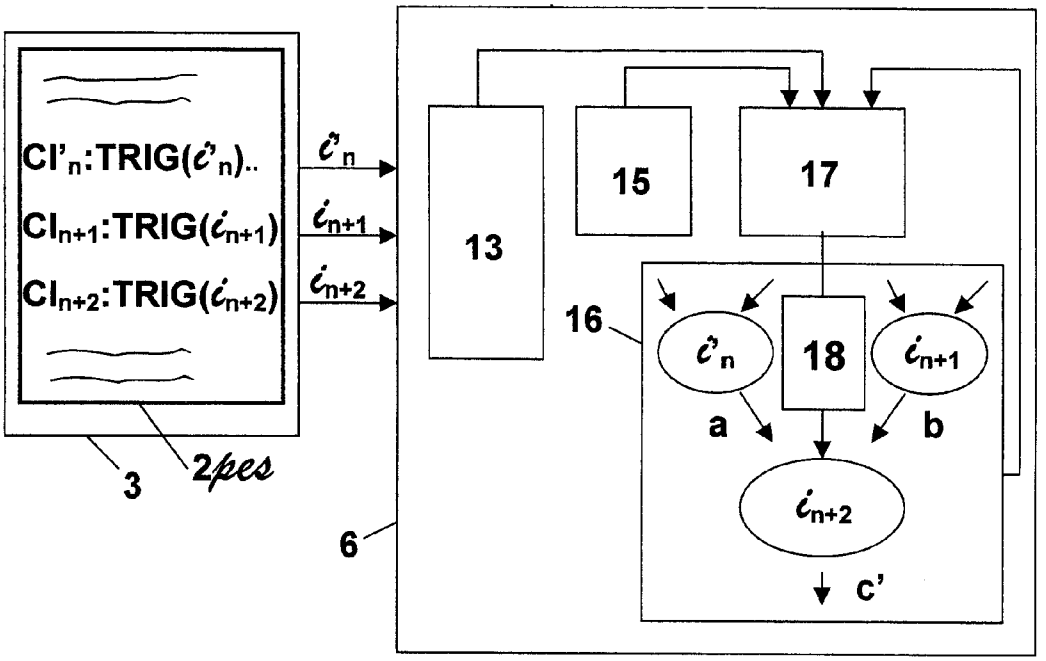


FIG. 73

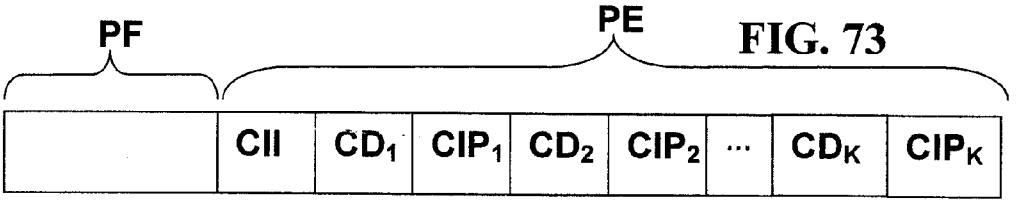


FIG. 74

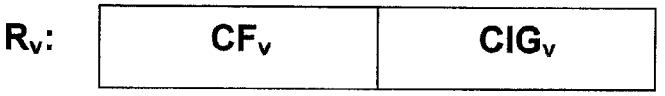


FIG. 80

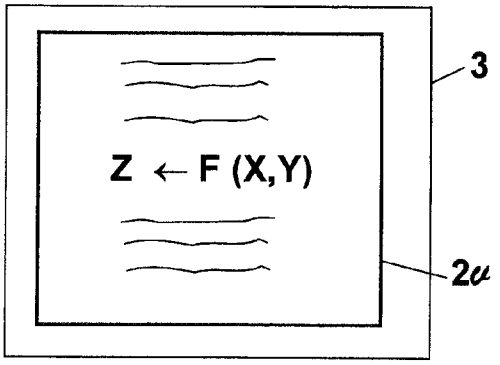


FIG. 81

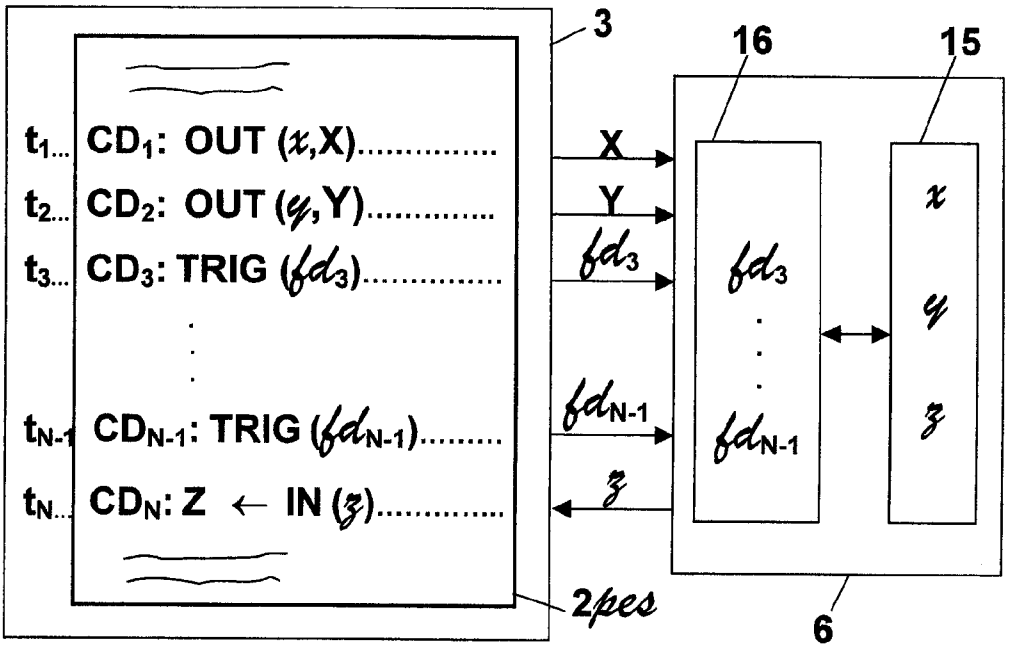
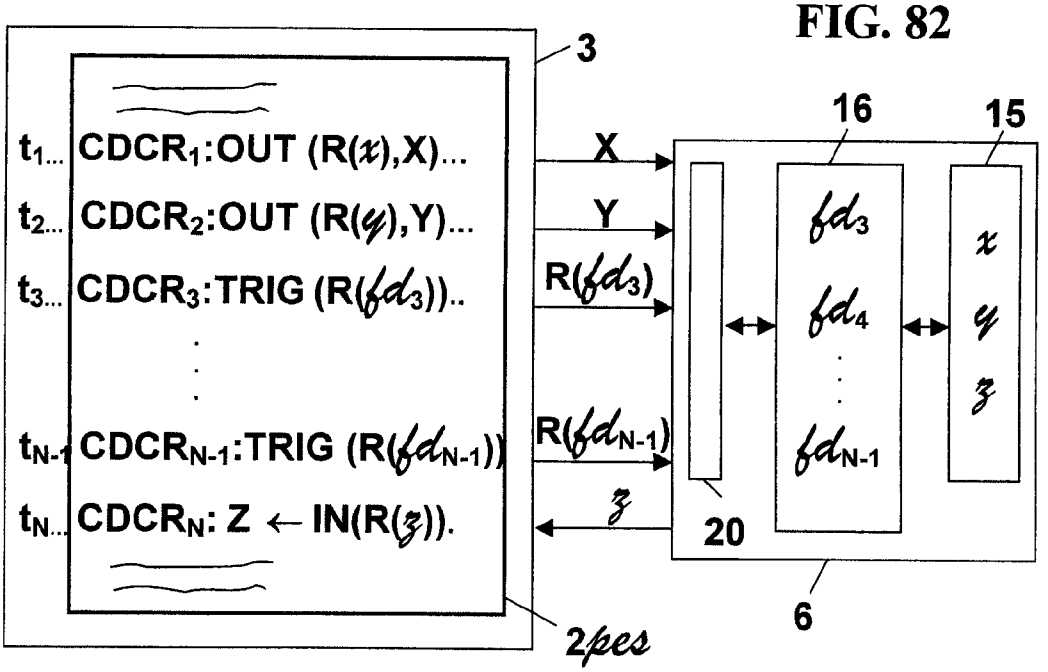

3
16
15
t1... CD1: OUT (x,X).....
t2... CD2: OUT (y,Y).....
t3... CD3: TRIG (fd3).....
tN-1 CDN-1: TRIG (fdN-1).....
tN... CDN: Z ← IN (z).....
X
Y
fd3
fdN-1
z
fd3
fdN-1
x
y
z
2pes
6

FIG. 82


3
16
15
t1... CDCR1:OUT (R(x),X)...
t2... CDCR2:OUT (R(y),Y)...
t3... CDCR3:TRIG (R(fd3))..
tN-1 CDCRN-1:TRIG (R(fdN-1))
tN... CDCRN: Z ← IN(R(z)).
X
Y
R(fd3)
R(fdN-1)
z
fd3
fd4
fdN-1
x
y
z
20
2pes
6

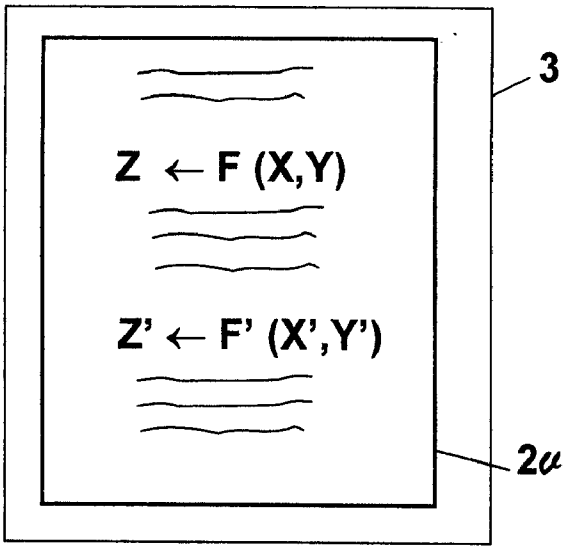

Z ← F (X,Y)
Z' ← F' (X',Y')
3
2u

FIG. 83

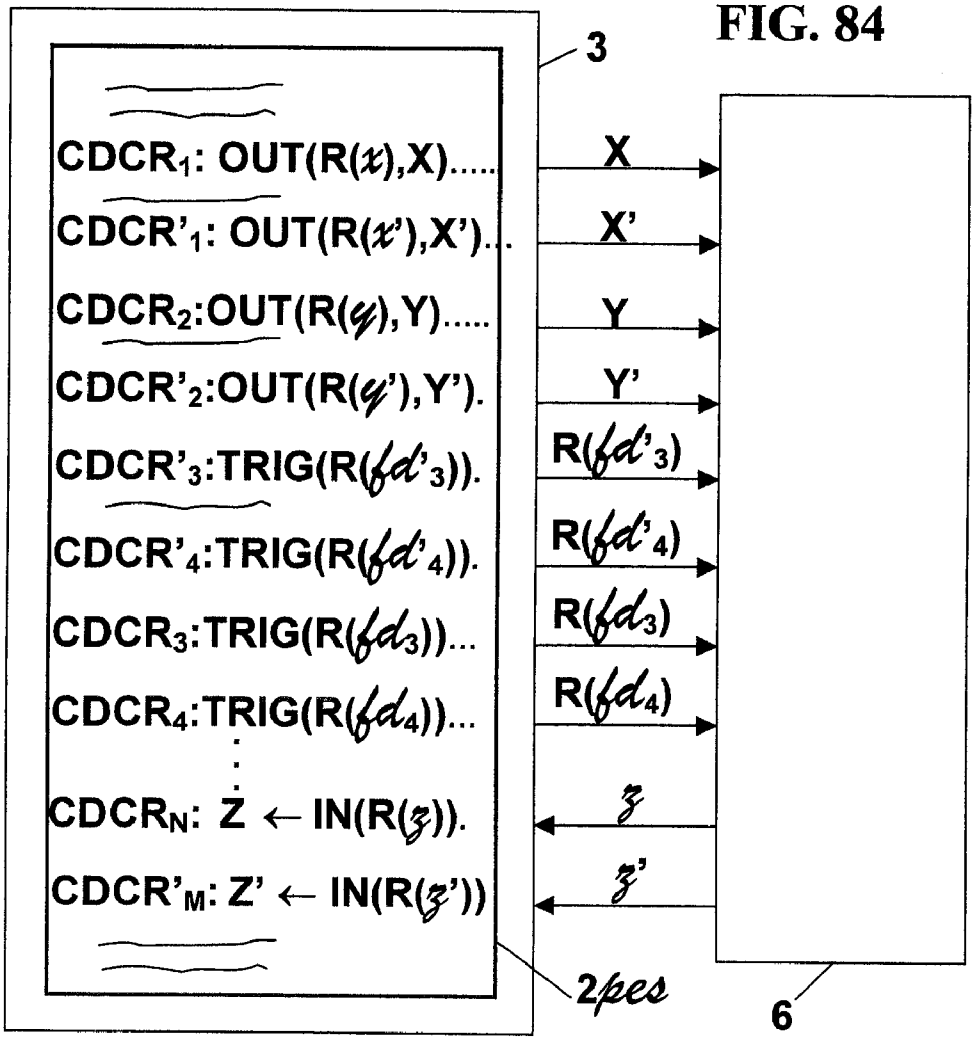

CDCR1: OUT(R(x),X).....
CDCR'1: OUT(R(x'),X')...
CDCR2:OUT(R(y),Y).....
CDCR'2:OUT(R(y'),Y').
CDCR'3:TRIG(R(fd'3)).
CDCR'4:TRIG(R(fd'4)).
CDCR3:TRIG(R(fd3))...
CDCR4:TRIG(R(fd4))...
CDCRN: Z ← IN(R(z)).
CDCR'M: Z' ← IN(R(z'))
3
X
X'
Y
Y'
R(fd'3)
R(fd'4)
R(fd3)
R(fd4)
z
z'
2pes
6

FIG. 84

FIG. 85

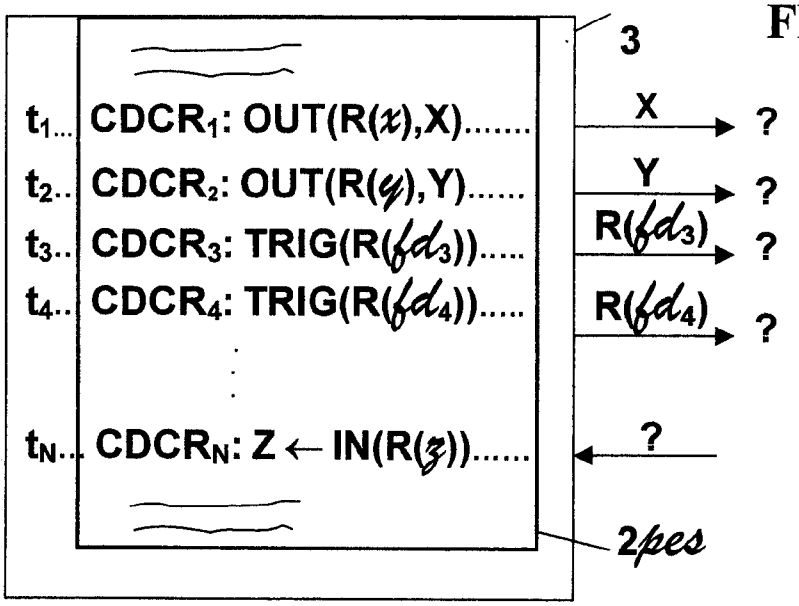


FIG. 90

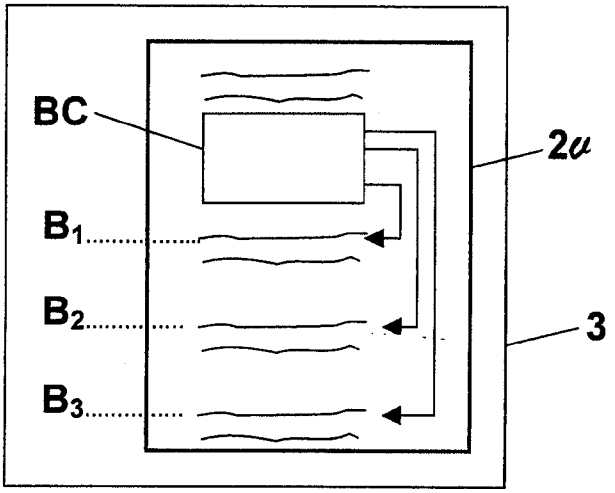


FIG. 91

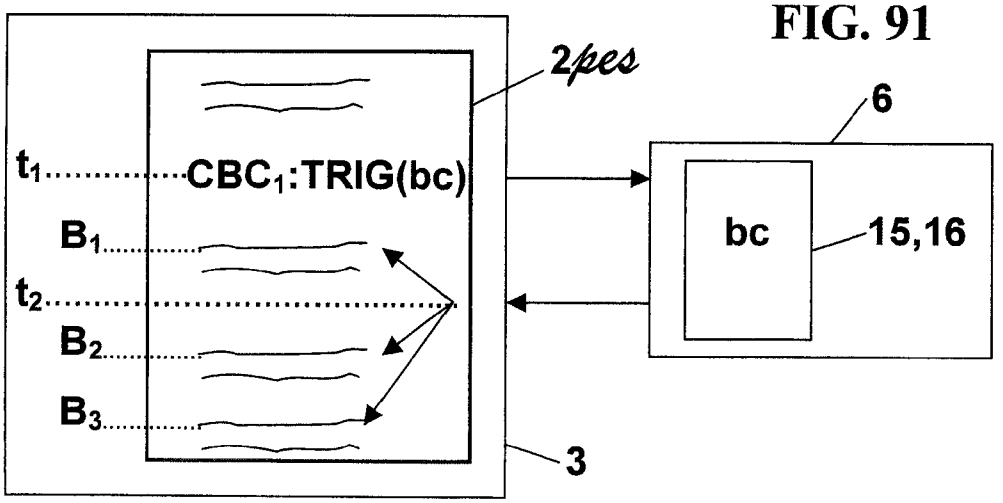


FIG. 92

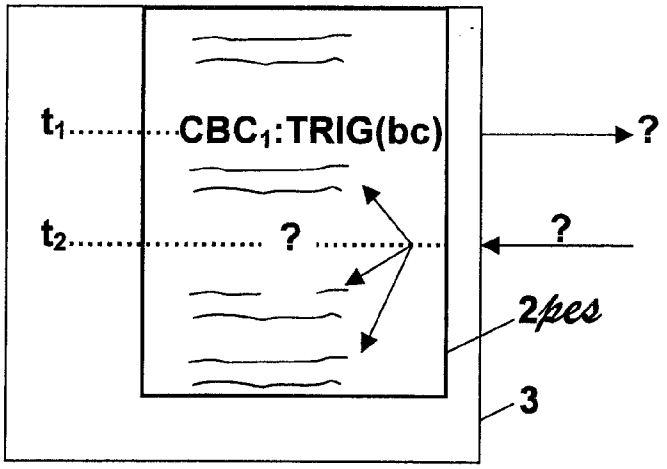


FIG. 100

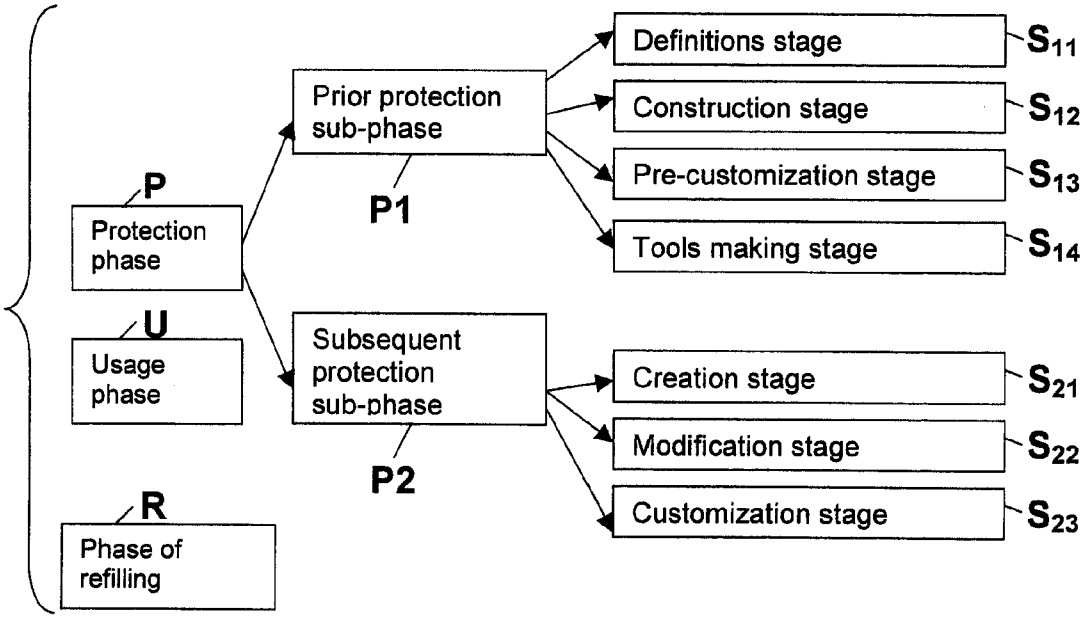
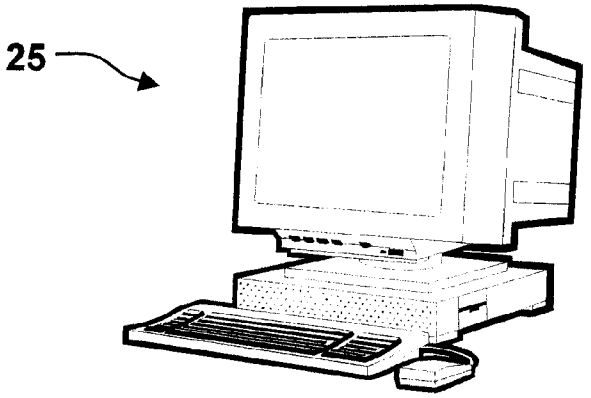


FIG. 110



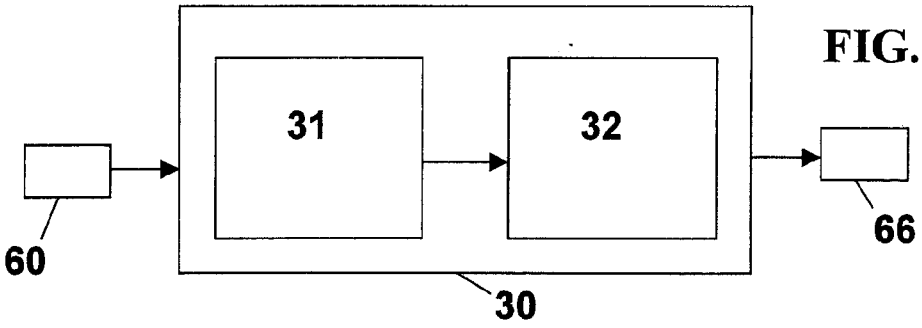


FIG. 120

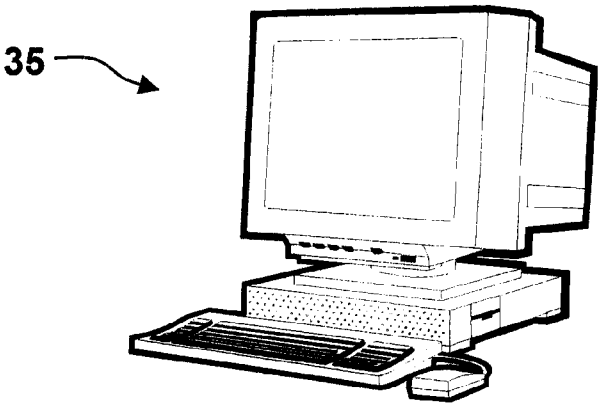


FIG. 130

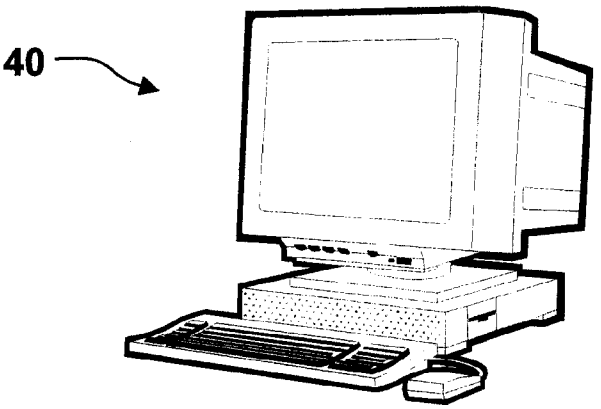


FIG. 140

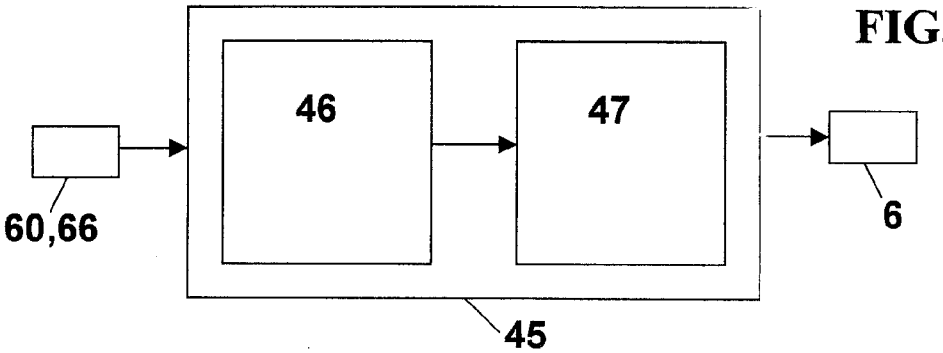


FIG. 150

METHOD TO PROTECT SOFTWARE AGAINST UNWANTED USE WITH A VARIABLE PRINCIPLE

BACKGROUND OF THE INVENTION

[0001] This invention concerns the technical domain of data processing systems in the general sense, and is more precisely aimed at the means of protecting software running on said data processing systems against unauthorized usage.

[0002] The subject of the invention aims in particular at the means of protecting software against unauthorized usage, using a memorizing unit or processing and memorizing unit, such a unit being commonly materialized by a chip card or a material key on USB port.

[0003] In the technical domain above, the main problem concerns the unauthorized usage of software by users who have not paid the license rights. This illicit use of software causes an obvious loss for software editors, software distributors and/or any person integrating such software in products. To avoid such illicit copies, various solutions, in the state of technology, have been proposed to protect software.

[0004] Thus, a protection solution is known, which makes use of a hardware protection system, such as a physical component named protection key or "dongle". Such a protection key should guarantee that the software executes only in presence of the key. Yet, it must be acknowledged that this solution is ineffective because it presents the inconvenience of being easy to bypass. An ill-intentioned person or a hacker can, with the aid of specialized tools such as disassemblers, delete the control instructions of the protection key. It becomes then possible to make illicit copies corresponding to modified versions of the software able to run without the protection. Moreover, this solution cannot be generalized to all software, inasmuch as it is difficult to connect more than two protection keys to the same system.

BRIEF SUMMARY OF THE INVENTION

[0005] The subject of the invention aims precisely at finding a solution to the aforementioned problems by proposing a process to protect a software against unauthorized usage, using an ad hoc memorizing unit or processing and memorizing unit, inasmuch as the presence of such a unit is necessary for the software to be completely functional.

[0006] So as to reach such a goal, the subject of the invention concerns a process to protect, using at least one blank unit including at least memorization means, a vulnerable software against its unauthorized usage, said vulnerable software being produced from a source and working on a data processing system. The process according to the invention comprises:

[0007] during a protection phase:

[0008] creating a protected software:

[0009] by choosing in the source of the vulnerable software:

[0010] at least one variable which, during the execution of the vulnerable software, partially defines the state of the latter,

[0011] and at least one portion containing at least one chosen variable,

[0012] by producing a source of the protected software from the source of the vulnerable software, by modifying at least one chosen portion of the source of the vulnerable software, this modification being such that during the execution of the protected software, at least one chosen variable or at least one copy of chosen variable resides in the blank unit which is thus transformed into a unit,

[0013] and by producing a first object part of the protected software from the source of the protected software, said first object part being such that during the execution of the protected software, appears a first execution part which is executed in the data processing system and whose at least a portion takes into account that at least a variable or at least a copy of variable resides in the unit,

[0014] and during a usage phase during which the protected software is executed:

[0015] in the presence of the unit, each time a portion of the first execution part imposes it, using a variable or a copy of variable residing in the unit, so that said portion is executed correctly and that, consequently, the protected software is completely functional,

[0016] and in the absence of the unit, in spite of the request by a portion of the first execution part to use a variable or a copy of variable residing in the unit, not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently the protected software is not completely functional.

[0017] According to a preferred embodiment, the process according to the invention comprises:

[0018] during the protection phase:

[0019] modifying the protected software:

[0020] by choosing in the source of the protected software:

[0021] at least one algorithmic processing which during the execution of the protected software, uses at least one chosen variable, and enables to obtain at least one result variable,

[0022] and at least one portion containing at least one chosen algorithmic processing,

[0023] by modifying at least one chosen portion of the source of the protected software, this modification being such that:

[0024] during the execution of the protected software the first execution part is executed in the data processing system and a second execution part is executed in the unit which also includes processing means,

[0025] at least the functionality of at least one chosen algorithmic processing is executed by means of the second execution part,

[0026] at least one chosen algorithmic processing is split so that during the execution of the pro-

tected software, appear, by means of the second execution part, several distinct steps, namely:

[0027] the placing of at least one variable at the unit's disposal,

[0028] the carrying out in the unit, of the functionality of the algorithmic processing on at least said variable,

[0029] and possibly, the placing of at least one result variable at the data processing system's disposal by the unit,

[0030] for at least one chosen algorithmic processing, steps commands are defined so that during the execution of the protected software, each step command is executed by the first execution part and triggers in the unit, the execution by means of the second execution part, of a step,

[0031] and a sequence of the steps commands is chosen among the set of sequences allowing the execution of the protected software,

[0032] and by producing:

[0033] the first object part of the protected software, said first object part being such that during the execution of the protected software, the steps commands are executed according to the chosen sequence,

[0034] and a second object part of the protected software, said second object part being such that, after upload to the blank unit and during the execution of the protected software, appears the second execution part by means of which the steps triggered by the first execution part are executed,

[0035] and uploading the second object part to the blank unit, with the intention of obtaining the unit,

[0036] and during the usage phase:

[0037] in the presence of the unit and each time a step command contained in a portion of the first execution part imposes it, executing the corresponding step in the unit, so that said portion is executed correctly and that, consequently, the protected software is completely functional,

[0038] and in the absence of the unit, in spite of the request by a portion of the first execution part to trigger the execution of a step in the unit, not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently, the protected software is not completely functional.

[0039] According to another preferred embodiment, the process according to the invention comprises:

[0040] during the protection phase:

[0041] defining:

[0042] a set of elementary functions whose elementary functions are liable to be executed in the unit which also includes processing means,

[0043] and a set of elementary commands for said set of elementary functions, said elementary commands being liable to be executed in the data processing system and to trigger the execution in the unit, of the elementary functions,

[0044] constructing exploitation means enabling to transform the blank unit into the unit able to execute the elementary functions of said set, the execution of said elementary functions being triggered by the execution in the data processing system, of elementary commands,

[0045] modifying the protected software:

[0046] by choosing in the source of the protected software:

[0047] at least one algorithmic processing which during the execution of the protected software, uses at least one chosen variable, and enables to obtain at least one result variable,

[0048] and at least one portion containing at least one chosen algorithmic processing,

[0049] by modifying at least one chosen portion of the source of the protected software, this modification being such that:

[0050] during the execution of the protected software the first execution part is executed in the data processing system and a second execution part is executed in the unit,

[0051] at least the functionality of at least one chosen algorithmic processing is executed by means of the second execution part,

[0052] at least one chosen algorithmic processing is split so that during the execution of the protected software, said algorithmic processing is executed by means of the second execution part, using elementary functions,

[0053] for at least one chosen algorithmic processing, elementary commands are integrated to the source of the protected software, so that during the execution of the protected software, each elementary command is executed by the first execution part and triggers in the unit, the execution by means of the second execution part, of an elementary function,

[0054] and a sequence of the elementary commands is chosen among the set of sequences allowing the execution of the protected software,

[0055] and by producing:

[0056] the first object part of the protected software, said first object part being such that during the execution of the protected software, the elementary commands are executed according to the chosen sequence,

[0057] and a second object part of the protected software containing the exploitation means, said second object part being such that, after upload to the blank unit and during the execution of the protected software, appears the second execution part by means of which the

elementary functions triggered by the first execution part are executed,

[0058] and uploading the second object part to the blank unit, with the intention of obtaining the unit,

[0059] and during the usage phase:

[0060] in the presence of the unit and each time an elementary command contained in a portion of the first execution part imposes it, executing the corresponding elementary function in the unit, so that said portion is executed correctly and that, consequently, the protected software is completely functional,

[0061] and in the absence of the unit, in spite of the request by a portion of the first execution part, to trigger the execution of an elementary function in the unit, not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently, the protected software is not completely functional.

[0062] According to another preferred embodiment, the process according to the invention comprises:

[0063] during the protection phase:

[0064] defining:

[0065] a set of elementary functions whose elementary functions are liable to be executed in the unit,

[0066] and a set of elementary commands for said set of elementary functions, said elementary commands being liable to be executed in the data processing system and to trigger the execution in the unit, of the elementary functions,

[0067] constructing exploitation means enabling the unit, to execute the elementary functions of said set, the execution of said elementary functions being triggered by the execution in the data processing system, of elementary commands,

[0068] and modifying the protected software:

[0069] by choosing in the source of the protected software, at least one step which during the execution of the protected software, carries out the functionality of an algorithmic processing,

[0070] by modifying at least one chosen portion of the source of the protected software, this modification being such that:

[0071] at least one chosen step is split so that during the execution of the protected software, said step is executed by means of the second execution part, using elementary functions,

[0072] for at least one chosen step, elementary commands are integrated to the source of the protected software, so that during the execution of the protected software, each elementary command is executed by the first execution part and triggers in the unit, the execution by means of the second execution part, of an elementary function,

[0073] and a sequence of the elementary commands is chosen among the set of sequences allowing the execution of the protected software,

[0074] and by producing:

[0075] the first object part of the protected software, said first object part being such that during the execution of the protected software, the elementary commands are executed according to the chosen sequence,

[0076] and the second object part of the protected software also containing the exploitation means, said second object part being such that, after upload to the unit and during the execution of the protected software, appears the second execution part by means of which the elementary functions triggered by the first execution part are executed,

[0077] and during the usage phase:

[0078] in the presence of the unit and each time an elementary command contained in a portion of the first execution part imposes it, executing the corresponding elementary function in the unit, so that said portion is executed correctly and that, consequently, the protected software is completely functional,

[0079] and in the absence of the unit, in spite of the request by a portion of the first execution part, to trigger the execution of an elementary function in the unit, not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently, the protected software is not completely functional.

[0080] According to another preferred embodiment, the process according to the invention comprises:

[0081] a during the protection phase:

[0082] defining:

[0083] at least one software execution characteristic, liable to be monitored at least in part in the unit,

[0084] at least one criterion to abide by for at least one software execution characteristic,

[0085] detection means to implement in the unit and enabling to detect that at least one software execution characteristic does not abide by at least one associated criterion,

[0086] and coercion means to implement in the unit and enabling to inform the data processing system and/or modify the execution of a software, when at least one criterion is not abided by,

[0087] constructing the exploitation means enabling the unit, to also implement the detection means and the coercion means,

[0088] and modifying the protected software:

[0089] by choosing at least one software execution characteristic to monitor, among the software execution characteristics liable to be monitored,

[0090] by choosing at least one criterion to abide by for at least one chosen software execution characteristic,

[0091] by choosing in the source of the protected software, elementary functions for which at least one chosen software execution characteristic is to be monitored,

[0092] by modifying at least one chosen portion of the source of the protected software, this modification being such that during the execution of the protected software, at least one chosen execution characteristic is monitored by means of the second execution part, and the fact that a criterion is not abided by leads to the data processing system being informed and/or to a modification of the execution of the protected software,

[0093] and by producing the second object part of the protected software containing the exploitation means also implementing the detection means and the coercion means, said second object part being such that, after upload to the unit and during the execution of the protected software, at least one software execution characteristic is monitored and the fact that a criterion is not abided by leads to the data processing system being informed and/or to a modification of the execution of the protected software,

[0094] and during the usage phase:

[0095] in the presence of the unit:

[0096] as long as all the criteria corresponding to all the monitored execution characteristics of all the modified portions of the protected software are abided by, enabling said portions of the protected software to work nominally and consequently enabling the protected software to work nominally,

[0097] and if at least one of the criteria corresponding to a monitored execution characteristic of a portion of the protected software is not abided by, informing the data processing system of it and/or modifying the functioning of the portion of the protected software, so that the functioning of the protected software is modified.

[0098] According to a variant embodiment, the process according to the invention comprises:

[0099] during the protection phase:

[0100] defining:

[0101] as software execution characteristic liable to be monitored, a variable of measurement of the usage of a functionality of a software,

[0102] as criterion to abide by, at least one threshold associated to each variable of measurement,

[0103] and actualization means enabling to update at least one variable of measurement,

[0104] constructing the exploitation means enabling the unit to also implement the actualization means,

[0105] and modifying the protected software:

[0106] by choosing as software execution characteristic to monitor, at least one variable of measurement of the usage of at least one functionality of a software,

[0107] by choosing:

[0108] at least one functionality of the protected software whose usage is liable to be monitored using a variable of measurement,

[0109] at least one variable of measurement used to quantify the usage of said functionality,

[0110] at least one threshold associated to a chosen variable of measurement corresponding to a limit of usage of said functionality,

[0111] and at least one method of update of a chosen variable of measurement depending on the usage of said functionality,

[0112] and by modifying at least one chosen portion of the source of the protected software, this modification being such that, during the execution of the protected software, the variable of measurement is actualized by means of the second execution part depending on the usage of said functionality, and at least one threshold crossing is taken into account,

[0113] and during the usage phase, in the presence of the unit, and in the case where at least one threshold crossing corresponding to at least one limit of usage is detected, informing the data processing system of it and/or modifying the functioning of the portion of the protected software, so that the functioning of the protected software is modified.

[0114] According to a variant embodiment, the process according to the invention comprises:

[0115] during the protection phase:

[0116] defining:

[0117] for at least one variable of measurement, several associated thresholds,

[0118] and different coercion means corresponding to each of said thresholds,

[0119] and modifying the protected software:

[0120] by choosing in the source of the protected software, at least one chosen variable of measurement to which must be associated several thresholds corresponding to different limits of usage of the functionality,

[0121] by choosing at least two thresholds associated to the chosen variable of measurement,

[0122] and by modifying at least one chosen portion of the source of the protected software, this modification being such that, during the execution of the protected software, the crossings of the various thresholds are taken into account differently, by means of the second execution part,

[0123] and during the usage phase:

[0124] in the presence of the unit:

[0125] in the case where the crossing of a first threshold is detected, enjoining the protected software not to use the corresponding functionality anymore,

[0126] and in the case where the crossing of a second threshold is detected, making ineffective the corresponding functionality and/or at least one portion of the protected software.

[0127] According to a variant embodiment, the process according to the invention comprises:

[0128] during the protection phase:

[0129] defining refilling means enabling to credit at least one software functionality monitored by a variable of measurement with at least one additional usage,

[0130] constructing the exploitation means also allowing the unit to implement the refilling means,

[0131] and modifying the protected software:

[0132] by choosing in the source of the protected software, at least one chosen variable of measurement enabling to limit the usage of a functionality and which must be able to be credited with at least one additional usage,

[0133] and by modifying at least one chosen portion, this modification being such that during a phase called of refilling, at least one additional usage of at least one functionality corresponding to a chosen variable of measurement can be credited,

[0134] and during the phase of refilling:

[0135] reactualizing at least one chosen variable of measurement and/or at least one associated threshold, so as to allow at least one additional usage of the functionality.

[0136] According to a variant embodiment, the process according to the invention comprises:

[0137] during the protection phase:

[0138] defining:

[0139] as software execution characteristic liable to be monitored, a profile of software usage,

[0140] and as criterion to abide by, at least one feature of software execution,

[0141] and modifying the protected software:

[0142] by choosing as software execution characteristic to monitor at least one profile of software usage,

[0143] by choosing at least one feature of execution by which at least one chosen profile of usage must abide,

[0144] and by modifying at least one chosen portion of the source of the protected software, this modification being such that, during the execution of the protected software, the second execution part abides by all the chosen features of execution,

[0145] and during the usage phase in the presence of the unit, and in the case where it is detected that at least one feature of execution is not abided by, informing the data processing system of it and/or modifying the functioning of the portion of the protected software, so that the functioning of the protected software is modified.

[0146] According to a variant embodiment, the process according to the invention comprises:

[0147] during the protection phase:

[0148] defining:

[0149] an instructions set whose instructions are liable to be executed in the unit,

[0150] a set of instructions commands for said instructions set, said instructions commands being liable to be executed in the data processing system and to trigger in the unit the execution of the instructions,

[0151] as profile of usage, the chaining of the instructions,

[0152] as feature of execution, an expected chaining for the execution of the instructions,

[0153] as detection means, means enabling to detect that the chaining of the instructions does not correspond to the expected one,

[0154] and as coercion means, means enabling to inform the data processing system and/or to modify the functioning of the portion of protected software when the chaining of the instructions does not correspond to the expected one,

[0155] constructing the exploitation means also enabling the unit to execute the instructions of the instructions set, the execution of said instructions being triggered by the execution in the data processing system, of the instructions commands,

[0156] and modifying the protected software:

[0157] by modifying at least one chosen portion of the source of the protected software:

[0158] by transforming the elementary functions into instructions,

[0159] by specifying the chaining by which must abide at least some of the instructions during their execution in the unit,

[0160] and by transforming the elementary commands into instructions commands corresponding to the instructions used,

[0161] and during the usage phase, in the presence of the unit, in the case where it is detected that the chaining of the instructions executed in the unit does not correspond to the expected one, informing the data processing system of it and/or modifying the functioning of the portion of the protected software, so that the functioning of the protected software is modified.

[0162] According to a variant embodiment, the process according to the invention comprises:

[0163] during the protection phase:

[0164] defining:

[0165] as instructions set, an instructions set whose at least some instructions work with registers and use at least one operand with the intention of returning a result,

[0166] for at least some of the instructions working with registers:

[0167] a part defining the functionality of the instruction,

[0168] and a part defining the expected chaining for the execution of the instructions and including bits fields corresponding to:

[0169] an identification field of the instruction,

[0170] and for each operand of the instruction:

[0171] a flag field,

[0172] and an expected identification field of the operand,

[0173] for each register belonging to the exploitation means and used by the instructions set, a generated identification field in which is automatically memorized the identification of the last instruction which has returned its result in said register,

[0174] as detection means, means enabling, during the execution of an instruction, for each operand, when the flag field imposes it, to check the equality of the generated identification field corresponding to the register used by said operand, and the expected identification field of the origin of said operand,

[0175] and as coercion means, means enabling to modify the result of the instructions, if at least one of the checked equalities is false.

[0176] According to another preferred embodiment, the process according to the invention comprises:

[0177] during the protection phase:

[0178] defining:

[0179] as a triggering command, an elementary command or an instruction command,

[0180] as a dependent function, an elementary function or an instruction,

[0181] as an order, at least one argument for a triggering command, corresponding at least in part to the information transmitted by the data processing system to the unit, so as to trigger the execution of the corresponding dependent function,

[0182] a method of renaming of the orders enabling to rename the orders so as to obtain triggering commands with renamed orders,

[0183] and restoring means designed to be used in the unit during the usage phase, and enabling to restore the dependent function to execute, from the renamed order,

[0184] constructing exploitation means enabling the unit to also implement the restoring means,

[0185] and modifying the protected software:

[0186] by choosing in the source of the protected software, triggering commands,

[0187] by modifying at least one chosen portion of the source of the protected software by renaming the orders of the chosen triggering commands, so as to conceal the identity of the corresponding dependent functions,

[0188] and by producing:

[0189] the first object part of the protected software, said first object part being such that during the execution of the protected software, the triggering commands with renamed orders are executed,

[0190] and the second object part of the protected software containing the exploitation means also implementing the restoring means, said second object part being such that, after upload to the unit and during the execution of the protected software, the identity of the dependent functions whose execution is triggered by the first execution part is restored by means of the second execution part, and the dependent functions are executed by means of the second execution part,

[0191] and during the usage phase:

[0192] in the presence of the unit and each time a triggering command with renamed order, contained in a portion of the first execution part imposes it, restoring in the unit, the identity of the corresponding dependent function and executing it, so that said portion is executed correctly and that, consequently, the protected software is completely functional,

[0193] and in the absence of the unit, in spite of the request by a portion of the first execution part, to trigger the execution of a dependent function in the unit, not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently, the protected software is not completely functional.

[0194] According to a variant embodiment, the process according to the invention comprises:

[0195] during the protection phase:

[0196] defining for at least one dependent function, a family of dependent functions algorithmically equivalent, but triggered by triggering commands whose renamed orders are different,

[0197] and modifying the protected software:

[0198] by choosing, in the source of the protected software at least one triggering command with renamed order,

[0199] and by modifying at least one chosen portion of the source of the protected software by replacing at least the renamed order of one chosen triggering command with renamed order, with

another renamed order, triggering a dependent function of the same family.

[0200] According to a variant embodiment, the process according to the invention comprises:

[0201] during the protection phase, defining, for at least one dependent function, a family of algorithmically equivalent dependent functions:

[0202] by concatenating a field of noise to the information defining the functional part of the dependent function to execute in the unit,

[0203] or by using the identification field of the instruction and the expected identification fields of the operands.

[0204] According to a variant embodiment, the process according to the invention comprises:

[0205] during the protection phase:

[0206] defining:

[0207] as method of renaming of the orders, a ciphering method to cipher the orders,

[0208] and as restoring means, means implementing a deciphering method to decipher the renamed orders and thus restore the identity of the dependent functions to execute in the unit.

[0209] According to another preferred embodiment, the process according to the invention comprises:

[0210] during the protection phase:

[0211] modifying the protected software:

[0212] by choosing, in the source of the protected software, at least one conditional branch carried out in at least one chosen algorithmic processing,

[0213] by modifying at least one chosen portion of the source of the protected software, this modification being such that during the execution of the protected software, the functionality of at least one chosen conditional branch is executed, by means of the second execution part, in the unit,

[0214] and by producing:

[0215] the first object part of the protected software, said first object part being such that during the execution of the protected software, the functionality of at least one chosen conditional branch is executed in the unit,

[0216] and the second object part of the protected software, said second object part being such that, after upload to the unit and during the execution of the protected software, appears the second execution part by means of which the functionality of at least one chosen conditional branch is executed,

[0217] and during the usage phase:

[0218] in the presence of the unit and each time a portion of the first execution part imposes it, executing the functionality of at least one conditional branch in the unit, so that said portion is executed correctly and that, consequently, the protected software is completely functional,

[0219] and in the absence of the unit and in spite of the request by a portion of the first execution part to execute the functionality of a conditional branch in the unit, not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that consequently, the protected software is not completely functional.

[0220] According to a variant embodiment, the process according to the invention comprises, during the protection phase, modifying the protected software:

[0221] by choosing, in the source of the protected software, at least one series of chosen conditional branches,

[0222] by modifying at least one chosen portion of the source of the protected software, this modification being such that during the execution of the protected software, the overall functionality of at least one chosen series of conditional branches is executed, by means of the second execution part, in the unit,

[0223] and by producing:

[0224] the first object part of the protected software, said first object part being such that during the execution of the protected software, the functionality of at least one chosen series of conditional branches is executed in the unit,

[0225] and the second object part of the protected software, said second object part being such that, after upload to the unit and during the execution of the protected software, appears the second execution part by means of which the overall functionality of at least one chosen series of conditional branches is executed.

[0226] The process according to the invention thus enables to protect usage of a software by using a memorizing unit which presents the characteristic of containing a part of the software being executed. It follows that any derived version of the software attempting to work without the memorizing unit imposes to recreate the part of the software contained in the memorizing unit during the execution, or else said derived version of the software will not be completely functional.

BRIEF DESCRIPTION OF THE DRAWINGS

[0227] Various other characteristics emerge from the description made below in reference to the appended diagrams which show, as non-limiting examples, embodiments and implementations of the subject of the invention.

[0228] FIGS. **10** and **11** are functional blocks diagrams illustrating the various representations of a software respectively not protected and protected by the process in accordance with the invention.

[0229] FIGS. **20** to **22** illustrate as examples, various embodiments of an apparatus implementing the process in accordance with the invention.

[0230] FIGS. **30** and **31** are functional blocks diagrams making explicit the general principle of the process in accordance with the invention.

[0231] FIGS. **40** to **43** are diagrams illustrating the protection process according to the invention implementing the principle of protection by variable.

[0232] FIGS. **50** to **54** are diagrams illustrating the protection process according to the invention implementing the principle of protection by temporal dissociation.

[0233] FIGS. **60** to **64** are diagrams illustrating the protection process according to the invention implementing the principle of protection by elementary functions.

[0234] FIGS. **70** to **74** are diagrams illustrating the protection process according to the invention implementing the principle of protection by detection and coercion.

[0235] FIGS. **80** to **85** are diagrams illustrating the protection process according to the invention implementing the principle of protection by renaming.

[0236] FIGS. **90** to **92** are diagrams illustrating the protection process according to the invention implementing the principle of protection by conditional branch.

[0237] FIG. **100** is a diagram illustrating the different phases of implementation of the subject of the invention.

[0238] FIG. **110** illustrates an embodiment of a system allowing the implementation of the construction stage of the protection phase in accordance with the invention.

[0239] FIG. **120** illustrates an embodiment of a pre-customization unit used in the protection process in accordance with the invention.

[0240] FIG. **130** illustrates an embodiment of a system allowing the implementation of the tools making stage of the protection phase in accordance with the invention.

[0241] FIG. **140** illustrates an embodiment of a system allowing the implementation of the protection process according to the invention.

[0242] FIG. **150** illustrates an embodiment of a customization unit used in the protection process in accordance with the invention.

DETAILED DESCRIPTION OF THE INVENTION

[0243] In the rest of the description, the following definitions will be used:

[0244] A data processing system **3** is a system able to execute a program.

[0245] A memorizing unit is a unit able to accept data provided by a data processing system **3**, to store the data and to restore it upon request of the data processing system **3**.

[0246] A processing and memorizing unit is a unit able:

[0247] to accept data provided by a data processing system **3**,

[0248] to return data to the data processing system **3**,

[0249] to store data at least partly in secret and to retain at least a part of said data even if the unit is switched off,

[0250] and to carry out algorithmic processing on data, part or all of the result being secret.

[0251] A unit **6** is a memorizing unit or a processing and memorizing unit implementing the process according to the invention.

[0252] A blank unit **60** is a unit which does not implement the process according to the invention, but which can receive data transforming it into a unit **6**.

[0253] A blank unit **60** can possibly become a unit **6** during the execution of a software protected by the process according to the invention and become again after the execution, a blank unit **60**.

[0254] A pre-customized unit **66** is a blank unit **60** which has received part of data enabling it, after reception of supplementary data, to be transformed into a unit **6**.

[0255] The upload of information to a blank unit **60** or a pre-customized unit **66** corresponds to a transfer of information to the blank unit **60** or the pre-customized unit **66**, and to a storage of said transferred information. The transfer can possibly include a change of the information format.

[0256] A variable, a function or data contained in the data processing system **3** will be indicated by an uppercase letter, while a variable, a function or data contained in the unit **6** will be indicated by a lowercase letter.

[0257] A "protected software", is a software which has been protected by at least one of the principles of protection implemented by the process in accordance with the invention.

[0258] A "vulnerable software", is a software which has not been protected by any principle of protection implemented by the process in accordance with the invention.

[0259] In the case where differentiation between a vulnerable software and a protected software is not important, the term "software" is used.

[0260] A software has various representations depending on the instant considered in its life cycle:

[0261] a source representation,

[0262] an object representation,

[0263] a distribution,

[0264] or a dynamic representation.

[0265] A source representation of a software is understood as a representation which after transformation, results in an object representation. A source representation can offer different levels, from a conceptual abstract level to a level executable directly by a data processing system or a processing and memorizing unit.

[0266] An object representation of a software corresponds to a level of representation which after transfer to a distribution and upload to a data processing system or a processing and memorizing unit, can be executed. It can be, for instance, a binary code, an interpreted code, etc.

[0267] A distribution is a physical or virtual support containing the object representation, said distribution having to be put at the user's disposal to enable them to use the software.

[0268] A dynamic representation corresponds to the execution of the software from its distribution.

[0269] A portion of a software corresponds to some part of the software and can, for instance correspond, to one or several consecutive or not instructions, and/or one or several consecutive or not functional blocks, and/or one or several functions, and/or one or several subprograms, and/or one or several modules. A portion of a software can also correspond to all of said software.

[0270] FIGS. **10** and **11** illustrate the various representations respectively of a vulnerable software **2***v* in the general sense, and of a protected software **2***p* protected according to the process in accordance with the invention.

[0271] FIG. **10** illustrates various representations of a vulnerable software **2***v* appearing during its life cycle. The vulnerable software **2***v* can thus appear under any of the following representations:

[0272] a source representation **2***vs*,

[0273] an object representation **2***vo*,

[0274] a distribution **2***vd*. Said distribution can have commonly the form of a physical distribution medium such as a CDROM or the form of files distributed through a network (GSM, Internet, etc.),

[0275] or a dynamic representation **2***ve* corresponding to the execution of the vulnerable software **2***v* on a data processing system **3** of any known type, which classically includes, at least one processor **4**.

[0276] FIG. **11** illustrates various representations of a protected software **2***p* appearing during its life cycle. The protected software **2***p* can thus appear under any of the following representations:

[0277] a source representation **2***ps* including a first source part intended for the data processing system **3** and possibly, a second source part intended for the unit **6**, part of said source parts can commonly be contained in common files,

[0278] an object representation **2***po* including a first object part **2***pos* intended for the data processing system **3** and possibly, a second object part **2***pou* intended for the unit **6**,

[0279] a distribution **2***pd* including:

[0280] a first distribution part **2***pds* containing the first object part **2***pos*, said first distribution part **2***pds* being intended for the data processing system **3** and which can commonly have the form of a physical distribution medium such as a CDROM or the form of files distributed through a network (GSM, Internet, etc.),

[0281] and a second distribution part **2***pdu* having the form:

[0282] of at least one blank unit **60**,

[0283] or of at least one pre-customized unit **66** to which a part of the second object part **2***pou* has been uploaded and for which the user has to finish the customization by uploading supplementary data so as to obtain a unit **6**, said supplementary data being obtained, for instance, by download through a network,

[0284] or of at least one unit **6** to which the second object part **2***pou* has been uploaded,

[0285] or a dynamic representation **2***pe* corresponding to the execution of the protected software **2***p*. Said dynamic representation **2***pe* includes a first execution part **2***pes* which is executed in the data processing system **3** and an second execution part **2***peu* which is executed in the unit **6**.

[0286] In the case where the differentiation between the different representations of the protected software **2***p* is not important, the expressions first part of the protected software and second part of the protected software shall be used.

[0287] The implementation of the process according to the invention in accordance with the dynamic representation of FIG. **11**, uses an apparatus **1***p* including a data processing system **3** linked up by a link **5** to a unit **6**. The data processing system **3** is of any type and includes, classically, at least one processor **4**. The data processing system **3** can be a computer or be part, for instance, of various machines, devices, fixed or mobile products, or vehicles in the general sense. The link **5** can be realized in any possible way, such as for instance a serial link, a USB bus, a radio link, an optical link, a network link or a direct electric connection to a circuit of data processing system **3**, etc. It should be observed that the unit **6** can possibly be physically located inside the same integrated circuit than the processor **4** of the data processing system **3**. In this case, the unit **6** can be considered as a co-processor in relation to the processor **4** of the data processing system **3** and the link **5** is internal to the integrated circuit.

[0288] FIGS. **20** to **22** show in an illustrative and non-limiting manner, various embodiments of the apparatus **1***p* allowing the implementation of the protection process in accordance with the invention.

[0289] In the embodiment illustrated in FIG. **20**, the protection apparatus **1***p* includes, as a data processing system **3**, a computer and, as a unit **6**, a chip card **7** and its interface **8** commonly called card reader. The computer **3** is linked up to the unit **6** by a link **5**. During the execution of the protected software **2***p*, the first execution part **2***pes* which is executed in the computer **3** and the second execution part **2***peu* which is executed in the chip card **7** and its interface **8**, must both be functional so that the protected software **2***p* is completely functional.

[0290] In the embodiment illustrated in FIG. **21**, the protection apparatus **1***p* equips a product **9** in the general sense, including various components **10** adapted to the function(s) assumed by such a product **9**. The protection apparatus **1***p* includes, on the one hand, a data processing system **3** embedded in the product **9** and, on the other hand, a unit **6** associated with the product **9**. So that the product **9** is completely functional, the protected software **2***p*, must be completely functional. Thus, during the execution of the protected software **2***p*, the first execution part **2***pes* which is

executed in the data processing system **3** and the second execution part **2***peu* which is executed in the unit **6**, must both be functional. Said protected software **2***p* enables therefore indirectly, to protect against unauthorized usage, the product **9** or one of its functionalities. For instance, the product **9** can be an installation, a system, a machine, a toy, a piece of domestic appliances, a phone, etc.

[**0291**] In the embodiment illustrated in FIG. **22**, the protection apparatus **1***p* includes several computers, as well as part of a communication network. The data processing system **3** is a first computer linked up by a link **5** of network type, to a unit **6** constituted by a second computer. For the implementation of the invention, the second computer **6** is used as a license server for a protected software **2***p*. During the execution of the protected software **2***p*, the first execution part **2***pes* which is executed in the first computer **3** and the second execution part **2***peu* which is executed in the second computer **6**, must both be functional so that the protected software **2***p* is completely functional.

[**0292**] FIG. **30** enables to make explicit more precisely, the protection process in accordance with the invention. It should be observed that a vulnerable software **2***v*, is considered as being executed totally in a data processing system **3**. On the other hand, in the case of the implementation of a protected software **2***p*, the data processing system **3** includes transfer means **12** linked up by the link **5**, to transfer means **13** being part of the unit **6** enabling to establish communication between the first execution part **2***pes* and the second execution part **2***peu* of the protected software **2***p*.

[**0293**] It must be considered that the transfer means **12**, **13** are of software and/or hardware nature and are capable of providing and, possibly, optimizing the data communication between the data processing system **3** and the unit **6**. Said transfer means **12**, **13** are adapted to enable to have at one's disposal a protected software **2***p* which is, preferably, independent from the type of link **5** used. Said transfer means **12**, **13** are not part of the subject of the invention and are not described more precisely as they are well known by the Man of art. The first part of the protected software **2***p* includes commands. During the execution of the protected software **2***p*, the execution of said commands by the first execution part **2***pes* enables the communication between the first execution part **2***pes* and the second execution part **2***peu*. In the rest of the description, said commands are represented by IN, OUT or TRIG.

[**0294**] As illustrated in FIG. **31**, to allow the implementation of the second execution part **2***peu* of the protected software **2***p*, the unit **6** includes protection means **14**. In the case where the unit **6** is a memorizing unit, the protection means **14** include memorization means **15**. In the case where the unit **6** is a processing and memorizing, the protection means **14** include memorization means **15** and processing means **16**.

[**0295**] For the sake of simplification in the rest of the description, it is chosen to consider, during the execution of the protected software **2***p*, the presence of the unit **6** or the absence of the unit **6**. In actual fact, a unit **6** providing protection means **14** not adapted to the execution of the second execution part **2***peu* of the protected software **2***p* is also considered as missing, each time the execution of the protected software **2***p* is not correct. In other words:

[**0296**] a unit **6** physically present and including protection means **14** adapted to the execution of the second execution part **2***peu* of the protected software **2***p*, is always considered as present,

[**0297**] a unit **6** physically present but including protection means **14** not adapted, i.e. not allowing the correct implementation of the second execution part **2***peu* of the protected software **2***p* is considered as present, when it works correctly, and as missing when it does not work correctly,

[**0298**] and a unit **6** physically missing is always considered as missing.

[**0299**] In the case where the unit **6** is constituted by a chip card **7** and its interface **8**, the transfer means **13** are split into two parts, one being on the interface **8** and the other one being on the chip card **7**. In this embodiment, the absence of the chip card **7** is considered as equivalent to the absence of the unit **6**. In other words, in the absence of the chip card **7** and/or its interface **8**, the protection means **14** are not accessible and do not enable the execution of the second execution part **2***peu* of the protected software **2***p*, so much so that the protected software **2***p* is not completely functional.

[**0300**] In accordance with the invention, the protection process aims at implementing a principle of protection called by <<variable>> a description of which is carried out in relation to FIGS. **40** to **43**.

[**0301**] For the implementation of the principle of protection by variable, is chosen in the source of the vulnerable software **2***vs* at least one variable which, during the execution of the vulnerable software **2***v*, partially defines its state. By state of a software, must be understood the set of pieces of information, at a given moment, necessary to the complete execution of said software, so much so that the absence of such a chosen variable prejudices the complete execution of said software. Is also chosen at least one portion of the source of the vulnerable software **2***vs* containing at least one chosen variable.

[**0302**] At least one chosen portion of the source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*. This modification is such that during the execution of the protected software **2***p*, at least one portion of the first execution part **2***pes* which is executed in the data processing system **3**, takes into account that at least one chosen variable or at least one copy of chosen variable resides in the unit **6**. For the implementation of the principle of protection by variable, the unit **6** includes at least memorization means **15**.

[**0303**] FIG. **40** illustrates an example of execution of a vulnerable software **2***v*. In this example, during the execution of the vulnerable software **2***v* in the data processing system **3**, appear:

[**0304**] at time instant t_1, the assignment of the data X to the variable V_1, represented by $V_1 \leftrightarrows X$,

[**0305**] at time instant t_2, the assignment of the value of the variable V_1 to the variable Y, represented by $Y \leftrightarrows V_1$,

[**0306**] and at time instant t_3, the assignment of the value of the variable V_1 to the variable Z, represented by $Z \leftrightarrows V_1$.

[**0307**] FIG. **41** illustrates an example of a first form of implementation of the invention for which the variable resides in the unit **6**. In this example, during the execution

in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p*, and in presence of the unit **6**, appear:

[**0308**] at time instant t_1, the execution of a transfer command triggering the transfer of the data X from the data processing system **3** to the variable v_1 located in the memorization means **15** of the unit **6**, said transfer command being represented by OUT(v_1, X) and corresponding in the end to the assignment of the data X to the variable v_1,

[**0309**] at time instant t_2, the execution of a transfer command triggering the transfer of the value of the variable v_1 residing in the unit **6** to the data processing system **3** so as to assign it to the variable Y, said transfer command being represented by IN(v_1) and corresponding in the end to the assignment of the value of the variable v_1 to the variable Y,

[**0310**] and at time instant t_3, the execution of a transfer command triggering the transfer of the value of the variable v_1 residing in the unit **6** to the data processing system **3** so as to assign it to the variable Z, said transfer command being represented by IN(v_1) and corresponding in the end to the assignment of the value of the variable v_1 to the variable Z.

[**0311**] It should be observed that during the execution of the protected software **2***p*, at least one variable resides in the unit **6**. Thus, when a portion of the first execution part **2***pes* of the protected software **2***p* imposes it, and in the presence of the unit **6**, the value of said variable residing in the unit **6** is transferred to the data processing system **3** to be used by the first execution part **2***pes* of the protected software **2***p*, so much so that said portion is **110** executed correctly and that, consequently, the protected software **2***p* is completely functional.

[**0312**] FIG. **42** illustrates an example of a second form of implementation of the invention for which a copy of the variable resides in the unit **6**. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p*, and in the presence of the unit **6**, appear:

[**0313**] at time instant t_1, the assignment of the data X to the variable V_1 located in the data processing system **3**, as well as the execution of a transfer command triggering the transfer of the data X from the data processing system **3** to the variable v_1 located in the memorization means **15** of the unit **6**, said transfer command being represented by OUT(v_1, X),

[**0314**] at time instant t_2, the assignment of the value of the variable V_1 to the variable Y,

[**0315**] and at time instant t_3, the execution of a transfer command triggering the transfer of the value of the variable v_1 residing in the unit **6** to the data processing system **3** so as to affect it to the variable Z, said transfer command being represented by IN(v_1).

[**0316**] It should be observed that during the execution of the protected software **2***p*, at least one copy of a variable resides in the unit **6**. Thus, when a portion of the first execution part **2***pes* of the protected software **2***p*, imposes it, and in the presence of the unit **6**, the value of said copy of variable residing in the unit **6** is transferred to the data processing system **3** to be used by the first execution part **2***pes* of the protected software **2***p*, so much so that said portion is executed correctly and that, consequently, the protected software **2***p* is completely functional.

[**0317**] FIG. **43** illustrates an example of attempt of execution of the protected software **2***p*, when the unit **6** is missing. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p:*

[**0318**] at time instant t_1, the execution of the transfer command OUT(v_1, X) cannot trigger the transfer of the data X to the variable v_1, taking into account the absence of the unit **6**,

[**0319**] at time instant t_2, the execution of the transfer command IN(v_1) cannot trigger the transfer of the value of the variable v_1 to the data processing system **3**, taking into account the absence of the unit **6**,

[**0320**] and at time instant t_3, the execution of the transfer command IN(v_i) cannot trigger the transfer of the value of the variable v_1 to the data processing system **3**, taking into account the absence of the unit **6**.

[**0321**] It therefore appears that in the absence of the unit **6**, at least one request by a portion of the first execution part **2***pes* to use a variable or a copy of variable residing in the unit **6**, cannot be fulfilled correctly, so that at least said portion is not executed correctly and that, consequently, the protected software **2***p* is not completely functional.

[**0322**] It should be observed that the data transfers between the data processing system **3** and the unit **6** illustrated in the previous examples use only simple assignments but that the Man of art will know how to combine them with other operations to obtain complex operations such as for instance OUT(v**1**, 2*X+3) or Z⇆(5*v**1**+v**2**).

[**0323**] According to another advantageous characteristic of the invention, the protection process aims at implementing a principle of protection, called by "temporal dissociation", a description of which is carried out in relation to FIGS. **50** to **54**.

[**0324**] For the implementation of the principle of protection by temporal dissociation, is chosen, in the source of the vulnerable software **2***vs*, at least one algorithmic processing using at least one operand and returning at least one result. Is also chosen at least one portion of the source of the vulnerable software **2***vs* containing at least one chosen algorithmic processing.

[**0325**] At least one chosen portion of the source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*. This modification is such that, among others:

[**0326**] during the execution of the protected software **2***p*, at least one portion of the first execution part **2***pes*, which is executed in the data processing system **3**, takes into account that the functionality of at least one chosen algorithmic processing is executed in the unit **6**,

[**0327**] during the execution of the protected **2***p*, the second execution part **2***peu*, which is executed in the unit **6**, executes at least the functionality of at least one chosen algorithmic processing,

[0328] during the execution of the protected software **2***p*, each chosen algorithmic processing is split into several distinct steps, namely:

[0329] step 1: the placing of the operand(s) at the unit **6**'s disposal,

[0330] step 2: the carrying out in the unit **6**, of the functionality of the chosen algorithmic processing using said operand(s),

[0331] and step 3: possibly, the placing of the result of the chosen algorithmic processing at the data processing system **3**'s disposal by the unit **6**,

[0332] steps commands are defined to trigger the execution of the steps,

[0333] and a sequence of the steps commands is chosen among the set of sequences allowing the execution of the protected software **2***p*.

[0334] The first execution part **2***pes* of the protected software **2***p*, which is executed in the data processing system **3**, executes the steps commands, triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of each of the previously defined steps. For the implementation of the principle of protection by temporal dissociation, the unit **6** includes memorization means **15** and processing means **16**.

[0335] FIG. **50** illustrates an example of execution of a vulnerable software **2***v*. In this example, appears, during the execution of the vulnerable software **2***v*, in the data processing system **3**, at a certain time instant, the calculation of Z⇆F(X, Y) corresponding to the assignment to a variable Z, of the result of an algorithmic processing represented by a function F and using operands X and Y.

[0336] FIG. **51** illustrates an example of implementation of the invention for which the algorithmic processing chosen in FIG. **50** is remoted in the unit **6**. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p* and in the presence of the unit **6**, appear:

[0337] at time instant t_1, the step 1, i.e. the execution of a step command CE_1 triggering the transfer of data X and Y from the data processing system **3** to the memorization zones respectively x and y located in the memorization means **15** of the unit **6**, said step command CE_1 being represented by OUT(x, X), OUT(y, Y),

[0338] at time instant t_2, the step 2, i.e. the execution of a step command CE_2, triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the function f, said function f being algorithmically equivalent to the function F and said step command CE_2 being represented by TRIG(f). More precisely, the execution of the step command CE_2 leads to the execution of the function f which uses the contents of the memorization zones x and y and returns its result to a memorization zone z of the unit **6**,

[0339] and at time instant t_3, the step 3, i.e. the execution of a step command CE_3 triggering the transfer of the result of the function f, contained in the memorization zone z of the unit **6** to the data processing system **3** so as to assign it to the variable Z, said step command CE_3 being represented by IN(z).

[0340] In the illustrated example, the steps 1 to 3 are executed successively. It should be observed that two improvements can be effected:

[0341] The first improvement concerns the case where several algorithmic processings are remoted in the unit **6** and at least the result of one algorithmic processing is used by another algorithmic processing. In this case, certain transfer steps can possibly be removed.

[0342] The second improvement aims at opting for a pertinent sequence of the steps commands among the set of sequences allowing the execution of the protected software **2***p*. In this respect, it is preferable to chose a sequence of the steps commands which temporally dissociates the execution of the steps, by intercalating between them, portions of code executed in the data processing system **3** and including or not steps commands used to determine other data.

[0343] FIGS. **52** and **53** illustrate the principle of such an embodiment.

[0344] FIG. **52** shows an example of execution of a vulnerable software **2***v*. In this example, appears, during the execution of the vulnerable software **2***v*, in the data processing system **3**, the execution of two algorithmic processings leading to the determination of Z and Z', such that Z⇆F (X, Y) and Z'⇆F'(X', Y').

[0345] FIG. **53** illustrates an example of implementation of the process according to the invention for which the two algorithmic processings chosen in FIG. **52** are remoted in the unit **6**. According to such an example, during the execution in the data processing system **3**, of the first execution part **2***pes* of the protected software **2***p*, and in the presence of the unit **6**, appears, as explained above, the execution of steps commands CE_1, CE_2, CE_3 corresponding to the determination of Z and of steps commands CE'_1, CE'_2, CE'_3 corresponding to the determination of Z'. As illustrated, the steps commands CE_1 to CE_3 are not executed consecutively inasmuch as steps commands CE'_1 to CE'_3, as well as other code portions are intercalated. In the example, the following sequence is thus carried out: CE_1, portion of intercalated code, CE_2, portion of intercalated code, CE'_1, portion of intercalated code, CE'_2, portion of intercalated code, CE'_3, portion of intercalated code, CE_3.

[0346] It should be observed that, during the execution of the protected software **2***p*, in the presence of the unit **6**, each time a step command contained in a portion of the first execution part **2***pes* of the protected software **2***p* imposes it, the corresponding step is executed in the unit **6**. Thus, it appears, that in the presence of the unit **6**, said portion is executed correctly and that, consequently, the protected software **2***p* is completely functional.

[0347] FIG. **54** illustrates an example of an attempt of execution of the protected software **2***p*, when the unit **6** is missing. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p*:

[0348] at time instant t_1, the execution of the step command OUT(x, X), OUT(y, Y) cannot trigger the

transfer of data X and Y to the respective memorization zones x and y taking into account the absence of the unit **6**,

[**0349**] at time instant t_2, the execution of the step command TRIG(f) cannot trigger the execution of the function f, taking into account the absence of the unit **6**,

[**0350**] and at time instant t_3, the execution of the step command IN(z) cannot trigger the transfer of the result of the function f, taking into account the absence of the unit **6**.

[**0351**] It therefore appears that in the absence of the unit **6**, at least one request by a portion of the first execution part **2***pes* to trigger the execution of a step in the unit **6**, cannot be fulfilled correctly, so that at least said portion is not executed correctly and that, consequently, the protected software **2***p* is not completely functional.

[**0352**] According to another advantageous characteristic of the invention, the protection process aims at implementing a principle of protection called by <<elementary function>> a description of which is carried out in relation to FIGS. **60** to **64**.

[**0353**] For the implementation of the principle of protection by elementary functions, are defined:

[**0354**] a set of elementary functions whose elementary functions are liable to be executed, by means of the second execution part **2***peu*, in the unit **6**, and possibly to transfer data between the data processing system **3** and the unit **6**,

[**0355**] and a set of elementary commands for said set of elementary functions, said elementary commands being liable to be executed in the data processing system **3** and to trigger the execution in the unit **6**, of the corresponding elementary functions.

[**0356**] For the implementation of the principle of protection by elementary functions, are also constructed exploitation means enabling to transform a blank unit **60** containing memorization means **15** and processing means **16** into a unit **6** able to execute elementary functions, the execution of said elementary functions being triggered by the execution in the data processing system **3**, of elementary commands.

[**0357**] For the implementation of the principle of protection by elementary functions, is also chosen, in the source of the vulnerable software **2***vs*, at least one algorithmic processing using at least one operand and returning at least one result. Is also chosen at least one portion of the source of the vulnerable software **2***vs* containing at least one chosen algorithmic processing.

[**0358**] At least one chosen portion of the source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*. This modification is such that, among others:

[**0359**] during the execution of the protected software **2***p*, at least one portion of the first execution part **2***pes*, which is executed in the data processing system **3**, takes into account that the functionality of at least one chosen algorithmic processing is executed in the unit **6**,

[**0360**] during the execution of the protected software **2***p*, the second execution part **2***peu*, which is executed in the unit **6**, executes at least the functionality of at least one chosen algorithmic processing,

[**0361**] each chosen algorithmic processing is split so that during the execution of the protected software **2***p*, each chosen algorithmic processing is executed, by means of the second execution part **2***peu*, using elementary functions. Preferably, each chosen algorithmic processing is split into elementary functions fe_n (with n varying from 1 to N), namely:

[**0362**] possibly one or several elementary functions enabling the placing of one or several operands at the unit **6**'s disposal,

[**0363**] elementary functions, some of which use the operand(s) and in combination, execute the functionality of the chosen algorithmic processing, using said operand(s),

[**0364**] and possibly one or several elementary functions enabling the placing of the result of the chosen algorithmic processing at the data processing system **3**'s disposal by the unit **6**,

[**0365**] and a sequence of the elementary commands is chosen among the set of sequences allowing the execution of the protected software **2***p*.

[**0366**] The first execution part **2***pes* of the protected software **2***p*, which is executed in the data processing system **3**, executes elementary commands CFE_n (with n varying from 1 to N), triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of each of the previously defined elementary functions fe_n.

[**0367**] FIG. **60** illustrates an example of execution of a vulnerable software **2***v*. In this example, appears, during the execution of the vulnerable software **2***v* in the data processing system **3**, at a certain time instant, the calculation of $Z \leftrightarrows F(X, Y)$ corresponding to the assignment to a variable Z of the result of an algorithmic processing represented by a function F and using operands X and Y.

[**0368**] FIG. **61** illustrates an example of implementation of the invention for which the algorithmic processing chosen in FIG. **60** is remoted in the unit **6**. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p* and in the presence of the unit **6**, appear:

[**0369**] at time instants t_1, t_2, the execution of the elementary commands CFE_1, CFE_2 triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the corresponding elementary functions fe_1, fe_2 which provide the transfer of data X, Y from the data processing system **3** to memorization zones respectively x, y located in the memorization means **15** of the unit **6**, said elementary commands CFE_1, CFE_2 being represented respectively by OUT(x, X), OUT(y, Y),

[**0370**] at time instants t_3 to t_{N-1}, the execution of the elementary commands CFE_3 to CFE_{N-1}, triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the corresponding elementary functions fe_3 to fe_{N-1}, said elementary commands CFE_3

to CFE_{N-1} being represented, respectively, by $TRIG(fe_3)$ to $TRIG(fe_{N-1})$. The series of elementary functions fe_3 to fe_{N-1} executed in combination is algorithmically equivalent to the function F. More precisely, the execution of said elementary commands leads to the execution in the unit **6**, of the elementary functions fe_3 to fe_{N-1} which use the contents of the memorization zones x, y and return the result to a memorization zone z of the unit **6**,

[0371] and at time instant t_N, the execution of the elementary command CFE_N triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the elementary function fe_N providing the transfer of the result of the algorithmic processing, contained in the memorization zone z of the unit **6** to the data processing system **3**, so as to assign it to the variable Z, said elementary command CFE_N being represented by IN(z).

[0372] In the illustrated example, the elementary commands 1 to N are executed successively. It should be observed that two improvements can be effected:

[0373] The first improvement concerns the case where several algorithmic processings are remoted in the unit **6** and at least the result of one algorithmic processing is used by another algorithmic processing. In this case, some elementary commands used for the transfer, can possibly be removed.

[0374] The second improvement aims at opting for a pertinent sequence of the elementary commands among the set of sequences allowing the execution of the protected software **2***p*. In this respect, it is preferable to choose a sequence of the elementary commands which temporally dissociates the execution of the elementary functions, by intercalating between them, portions of code executed in the data processing system **3** and including or not elementary commands used for the determination of other data. FIGS. **62** and **63** illustrate the principle of such an embodiment.

[0375] FIG. **62** shows an example of execution of a vulnerable software **2***v*. In this example, appears during the execution of the vulnerable software **2***v*, in the data processing system **3**, the execution of two algorithmic processings leading to the determination of Z and Z', such that $Z \leftrightarrows F(X, Y)$ and $Z' \leftrightarrows F'(X', Y')$.

[0376] FIG. **63** illustrates an example of implementation of the process according to the invention for which the two algorithmic processing chosen in FIG. **62** are remoted in the unit **6**. According to such an example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p* and in the presence of the unit **6**, appear, as explained above, the execution of the elementary commands CFE_1 to CFE_N corresponding to the determination of Z and the execution of the elementary commands CFE'_1 to CFE'_M corresponding to the determination of Z'. As illustrated, the elementary commands CFE_1 to CFE_N are not executed consecutively, inasmuch as the elementary commands CFE'_1 to CFE'_M, as well as other portions of code are intercalated. In the example, the following sequence is thus carried out: CFE_1, portion of intercalated code, CFE'_1, CFE_2, portion of intercalated code, CFE'_2, CFE'_3, portion of intercalated code, CFE'_4, CFE_3, CFE_4, . . . , CFE_N, CFE'_M.

[0377] It should be observed that, during the execution of the protected software **2***p*, in the presence of the unit **6**, each time an elementary command contained in a portion of the first execution part **2***pes* of the protected software **2***p* imposes it, the corresponding elementary function is executed in the unit **6**. Thus, it appears, that in the presence of the unit **6**, said portion is executed correctly and that, consequently, the protected software **2***p* is completely functional.

[0378] FIG. **64** illustrates an example of an attempt of execution of the protected software **2***p*, when the unit **6** is missing. In this example, during the execution in the data processing system **3**, of the first execution part **2***pes* of the protected software **2***p*, at every time instant, the execution of an elementary command cannot trigger the execution of the corresponding elementary function, because of the absence of the unit **6**. The value to assign to the variable Z cannot therefore be determined correctly. It therefore appears, that in the absence of the unit **6**, at least one request by a portion of the first execution part **2***pes* of the protected software **2***p*, to trigger the execution of an elementary function in the unit **6** cannot be fulfilled correctly, so that at least said portion is not executed correctly and that, consequently, the protected software **2***p* is not completely functional.

[0379] According to another advantageous characteristic of the invention, the protection process aims at implementing a principle of protection, called by <<detection and coercion>>, a description of which is carried out in relation to FIGS. **70** to **74**.

[0380] For the implementation of the principle of protection by detection and coercion, are defined:

[0381] at least one software execution characteristic liable to be monitored at least in part in the unit **6**,

[0382] at least one criterion to abide by for at least one software execution characteristic,

[0383] detection means **17** to implement in the unit **6** and enabling to detect that at least one software execution characteristic does not abide by at least one associated criterion,

[0384] and coercion means **18** to implement in the unit **6** and enabling to inform the data processing system **3** and/or modify the execution of a software, when at least one criterion is not abided by.

[0385] For the implementation of the principle of protection by detection and coercion, are also constructed exploitation means enabling to transform a blank unit **60** into a unit **6** implementing at least the detection means **17** and the coercion means **18**.

[0386] FIG. **70** illustrates the means necessary to the implementation of this principle of protection by detection and coercion. The unit **6** includes the detection means **17** and the coercion means **18** belonging to the processing means **16**. The coercion means **18** are informed by the detection means **17** that a criterion has not been abided by.

[0387] More precisely, the detection means **17** use information coming from the transfer means **13** and/or from the memorization means **15** and/or from the processing means **16**, so as to monitor one or several software execution

characteristics. For each software execution characteristic is set at least one criterion to abide by.

[0388] In the case where it is detected that at least one software execution characteristic does not abide by at least one criterion, the detection means **17** inform the coercion means **18** of it. Said coercion means **18** are adapted to modify, in the appropriate way, the state of the unit **6**.

[0389] For the implementation of the principle of protection by detection and coercion, are also chosen:

[0390] at least one software execution characteristic to monitor, among the software execution characteristics liable to be monitored,

[0391] at least one criterion to abide by for at least one chosen software execution characteristic,

[0392] in the source of the vulnerable software **2***vs*, at least one algorithmic processing for which at least one software execution characteristic is to be monitored,

[0393] and in the source of the vulnerable software **2***vs*, at least one portion containing at least one chosen algorithmic processing.

[0394] At least one chosen portion of the source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*. This modification is such that, during the execution of the protected software **2***p*, among others:

[0395] at least one portion of the first execution part **2***pes*, which is executed in the data processing system **3**, takes into account that at least one chosen software execution characteristic is to be monitored, at least in part in the unit **6**,

[0396] and the second execution part **2***peu*, which is executed in the unit **6**, monitors at least in part, a chosen software execution characteristic.

[0397] During the execution of the protected software **2***p*, protected by this principle of protection by detection and coercion, in the presence of the unit **6**:

[0398] as long as all the criteria corresponding to all the monitored execution characteristics of all the modified portions of the protected software **2***p* are abided by, said modified portions of the protected software **2***p* work nominally, so that said protected software **2***p* works nominally,

[0399] and if at least one of the criteria corresponding to a monitored execution characteristic of a portion of the protected software **2***p* is not abided by, the data processing system **3** is informed of it and/or the functioning of the portion of the protected software **2***p* is modified, so that the functioning of the protected software **2***p* is modified.

[0400] Naturally, in the absence of the unit **6**, at least one request by a portion of the first execution part **2***pes* of the protected software **2***p* to use the unit **6** cannot be fulfilled correctly so that at least said portion is not executed correctly and that consequently the protected software **2***p* is not completely functional.

[0401] For the implementation of the principle of protection by detection and coercion, two types of software execution characteristics are used preferentially.

[0402] The first type of software execution characteristic corresponds to a variable of measurement of the execution of a software and the second type corresponds to a profile of usage of a software. Said two types of characteristics can be used independently or in combination.

[0403] For the implementation of the principle of protection by detection and coercion using, as execution characteristic, a variable of measurement of software execution, are defined:

[0404] in the memorization means **15**, the possibility to memorize at least one variable of measurement used to quantify the usage of at least one functionality of a software,

[0405] in the detection means **17**, the possibility to monitor at least one threshold associated to each variable of measurement,

[0406] and actualization means enabling to update each variable of measurement depending on the usage of the functionality to which it is associated.

[0407] Are also constructed exploitation means implementing, in addition to the detection means **17** and the coercion means **18**, the actualization means.

[0408] Are also chosen, in the source of the vulnerable software **2***vs:*

[0409] at least one functionality of the vulnerable software **2***v* whose usage is liable to be monitored using a variable of measurement,

[0410] at least one variable of measurement used to quantify the usage of said functionality,

[0411] at least one threshold associated to the variable of measurement corresponding to a limit of usage of said functionality,

[0412] and at least one method of update of the variable of measurement depending on the usage of said functionality.

[0413] The source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*, this modification being such that, during the execution of the protected software **2***p*, the second execution **2***peu:*

[0414] actualizes the variable of measurement depending on the usage of said functionality,

[0415] and takes into account at least one threshold crossing.

[0416] In other words, during the execution of the protected software **2***p*, the variable of measurement is updated depending on the usage of said functionality, and when the threshold is crossed, the detection means **17** inform of it the coercion means **18** which make an adapted decision to inform the data processing system **3** and/or to modify the processings carried out by the processing means **16** enabling to modify the functioning of the portion of the protected software **2***p*, so that the functioning of the protected software **2***p* is modified.

[0417] For the implementation of a first preferred variant embodiment of the principle of protection by detection and coercion using, as characteristic, a variable of measurement, are defined:

[0418] for at least one variable of measurement, several associated thresholds,

[0419] and different coercion means corresponding to each of said thresholds.

[0420] Are also chosen, in the source of the vulnerable software **2***vs:*

[0421] at least one variable of measurement used to quantify the usage of at least one functionality of the software and to which must be associated several thresholds corresponding to different limits of usage of said functionalities,

[0422] and at least two thresholds associated to the variable of measurement.

[0423] The source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*, this modification being such that, during the execution of the protected software **2***p*, the second execution part **2***peu:*

[0424] actualizes the variable of measurement depending on the usage of said functionality,

[0425] and takes into account, differently, the crossing of the various thresholds.

[0426] In other words, classically, during the execution of the protected software **2***p*, when the first threshold is crossed, the unit **6** informs the data processing system **3** enjoining the protected software **2***p* not to use said functionality anymore. If the protected software **2***p* carries on using said functionality, the second threshold will potentially be crossed. In the case where the second threshold is crossed, the coercion means **18** can make the chosen functionality ineffective and/or make the protected software **2***p* ineffective.

[0427] For the implementation of a second preferred variant embodiment of the principle of protection by detection and coercion using, as characteristic, a variable of measurement, are defined refilling means enabling to credit at least one software functionality monitored by a variable of measurement with at least one additional usage.

[0428] Are also constructed exploitation means implementing, in addition to the detection means **17**, the coercion means **18** and the actualization means, the refilling means.

[0429] Is also chosen, in the source of the vulnerable software **2***vs*, at least one variable of measurement used to limit the usage of at least one functionality of the software and which must be able to be credited with at least one additional usage.

[0430] The source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*, this modification being such that, during a phase called of refilling, at least one additional usage of at least one functionality corresponding to a chosen variable of measurement can be credited.

[0431] Is carried out, during the phase of refilling, the reactualization of at least one chosen variable of measurement and/or of at least one associated threshold, so as to allow at least one additional usage of the corresponding functionality. In other words, it is possible, during the phase of refilling, to credit additional usages of at least one functionality of the protected software **2***p*.

[0432] For the implementation of the principle of protection by detection and coercion using, as characteristic, a profile of software usage, is defined as criterion to abide by for said profile of usage, at least one feature of software execution.

[0433] Are also chosen, in the source of the vulnerable software **2***vs:*

[0434] at least one profile of usage to monitor,

[0435] and at least one feature of execution by which at least one chosen profile of usage must abide.

[0436] The source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*, this modification being such that, during the execution of the protected software **2***p*, the second execution part **2***peu* abides by all the chosen features of execution. In other words, the unit **6** itself monitors the way the second execution part **2***peu* is executed and can inform the data processing system **3** and/or modify the functioning of the protected software **2***p*, in the case where at least one feature of execution is not abided by.

[0437] During the execution of the protected software **2***p*, protected by this principle, in the presence of the unit **6**:

[0438] as long as all the features of execution of all the modified portions of the protected software **2***p* are abided by, said modified portions of the protected software **2***p* work nominally, so that said protected software **2***p* works nominally,

[0439] and if at least one feature of execution of a portion of protected software **2***p* is not abided by, the data processing system **3** is informed of it and/or the functioning of the portion of the protected software **2***p* is modified, so that the functioning of the protected software **2***p* is modified.

[0440] The monitoring of different features of execution can be considered, like for instance the monitoring of the presence of instructions including a marker or the monitoring of the execution chaining for at least one part of the instructions.

[0441] For the implementation of the principle of protection by detection and coercion using as feature of execution to abide by, the monitoring of the execution chaining for at least one part of the instructions, are defined:

[0442] an instructions set, whose instructions are liable to be executed in the unit **6**,

[0443] a set of instructions commands for said instructions set, said instructions commands are liable to be executed in the data processing system **3**. The execution of each of said instructions commands in the data processing system **3** triggers in the unit **6**, the execution of the corresponding instruction,

[0444] detection means **17** enabling to detect that the chaining of the instructions does not correspond to the expected one,

[0445] and coercion means **18** enabling to inform the data processing system **3** and/or to modify the execution of a software when the chaining of the instructions does not correspond to the expected one.

[0446] Are also constructed exploitation means enabling the unit **6** to also execute the instructions of the instructions set, the execution of said instructions being triggered by the execution in the data processing system **3** of the instructions commands.

[0447] Is also chosen, in the source of the vulnerable software **2***vs*, at least one algorithmic processing which must be remoted in the unit **6** and for which the chaining of at least one part of the instructions is to be monitored.

[0448] The source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the vulnerable software **2***ps*, this modification being such that, during the execution of the protected software **2***p:*

[0449] the second execution part **2***peu* executes at least the functionality of the chosen algorithmic processing,

[0450] the chosen algorithmic processing is split into instructions,

[0451] the chaining by which at least some of the instructions must abide during their execution in the unit **6** is specified,

[0452] and the first execution part **2***pes* of the protected software **2***p* executes instructions commands which trigger the execution of the instructions in the unit **6**.

[0453] During the execution of the protected software **2***p*, protected by this principle, in the presence of the unit **6**:

[0454] as long as the chaining of the instructions of all the modified portions of the protected software **2***p*, executed in the unit **6** corresponds to the expected one, said modified portions of the protected software **2***p* work nominally, so that said protected software **2***p* works nominally,

[0455] and if the chaining of the instructions of a portion of the protected software **2***p* executed in the unit **6** does not correspond to the expected one, the data processing system **3** is informed of it and/or the functioning of the portion of protected software **2***p* is modified, so that the functioning of the protected software **2***p* is modified.

[0456] FIG. **71** illustrates an example of implementation of the principle of protection by detection and coercion using, as feature of execution to abide by the monitoring of the execution chaining of a at least one part of the instructions, in the case where the expected chaining is abided by.

[0457] The first execution part **2***pes* of the protected software **2***p*, executed in the data processing system **3**, executes instructions commands CI_i triggering, in the unit **6** the execution of the instructions i_i belonging to the instructions set. In said instructions set, at least some of the instructions each include a part defining the functionality of the instruction and a part enabling to verify the expected chaining for the execution of the instructions. In this example, the instructions commands CI_i are represented by $TRIG(i_i)$ and the expected chaining for the execution of the instructions is i_n, i_{n+1}, and i_{n+2}. The execution in the unit **6**, of the instruction i_n gives the result a and the execution of the instruction i_{n+1} gives the result b. The instruction i_{n+2} uses as operand, the results a and b of the instructions i_n and i_{n+1} and its execution gives the result c.

[0458] Taking into account that said chaining of the instructions executed in the unit **6** corresponds to the expected one, it results in a normal or nominal functioning of the protected software **2***p*.

[0459] FIG. **72** illustrates an example of implementation of the principle of protection by detection and coercion using, as feature of execution to abide by, the monitoring of the execution chaining of at least one part of the instructions, in the case where the expected chaining is not abided by.

[0460] According to this example, the expected chaining for the execution of the instructions is still i_n, i_{n+1} and i_{n+2}. However, the execution chaining is modified by the replacement of the instruction i_n with the instruction i'_n, so that the chaining actually executed is i'_n, i_{n+1} and i_{n+2}. The execution of the instruction i'_n gives the result a, i.e. the same result that the execution of the instruction i_n. However, at the latest during the execution of the instruction i_{n+2}, the detection means **17** detect that the instruction i'_n does not correspond to the expected instruction to generate the result a used as operand of the instruction i_{n+2}. The detection means **17** inform of it the coercion means **18** which modify accordingly, the functioning of the instruction i_{n+2}, so that the execution of the instruction i_{n+2} gives the result c' which can be different than c. Naturally, if the execution of the instruction i'_n gives a result a' different from the result a of the instruction i_n, it is clear that the result of the instruction i_{n+2} can also be different from c.

[0461] Inasmuch as the execution chaining of the instructions executed in the unit **6** does not correspond to the expected one, a modification of the functioning of the protected software **2***p* can therefore be obtained.

[0462] FIGS. **73** and **74** illustrates a preferred variant embodiment of the principle of protection by detection and coercion using, as feature of execution to abide by, the monitoring of the execution chaining of at least one part of the instructions. According to this preferred variant, is defined an instructions set whose at least some instructions work with registers and use at least one operand with the intention of returning a result.

[0463] As illustrated in FIG. **73**, are defined for at least some of the instructions working with registers, a part PF defining the functionality of the instruction and a part PE defining the expected chaining for the execution of the instructions. The part PF corresponds to the operation code known by the Man of art. The part PE defining the expected chaining, includes bits fields corresponding to:

[0464] an identification field of the instruction CII,

[0465] and for each operand k of the instruction, with k varying from 1 to K, and K number of operands of the instruction:

[0466] a flag field CD_k, indicating whether or not it is appropriate to verify the origin of the operand k,

[0467] and an expected identification field CIP_k of the operand, indicating the expected identity of the instruction which has generated the contents of the operand k.

[0468] As illustrated in FIG. **74**, the instructions set includes V registers belonging to the processing means **16**,

each register being named R_v, with v varying from 1 to V. For each register R_v, are defined two fields, namely:

[0469] a functional field CF_v, known by the Man of art and enabling to store the result of the execution of the instructions,

[0470] and a generated identification field CIG_v enabling to memorize the identity of the instruction which has generated the contents of the functional field CF_v. Said generated identification field CIG_v is automatically updated with the contents of the identification field of the instruction CII which has generated the functional field CF_v. Said generated identification field CIG_v is neither accessible, nor modifiable by any of the instructions and is solely used for the detection means **17**.

[0471] During the execution of an instruction, the detection means **17** carry out for each operand k the following operations:

[0472] the flag field CD_k is read,

[0473] if the flag field CD_k imposes it, the expected identification field CIP_k and the generated identification field CIG_v corresponding to the register used by the operand k are both read,

[0474] the equality of the two fields CIP_k and CIG_v is checked,

[0475] and if the equality is false, the detection means **17** consider that the execution chaining of the instructions is not abided by.

[0476] The coercion means **18** enable to modify the result of the instructions when the detection means **17** has informed them of an instructions chaining not abided by. A preferred embodiment is carried out by modifying the functional part PF of the instruction currently executed or the functional part PF of subsequent instructions.

[0477] According to another advantageous characteristic of the invention, the protection process aims at implementing a principle of protection, called by <<renaming>> a description of which is carried out in relation to FIGS. **80** to **85**.

[0478] For the implementation of the principle of protection by renaming, are defined:

[0479] a set of dependent functions, whose dependent functions are liable to be executed, by means of the second execution part **2***peu*, in the unit **6**, and possibly to transfer data between the data processing system **3** and the unit **6**, said set of dependent functions can be finite or infinite,

[0480] a set of triggering commands for said dependent functions, said triggering commands being liable to be executed in the data processing system **3** and to trigger in the unit **6**, the execution of corresponding dependent functions,

[0481] for each triggering command, an order corresponding at least in part to the information transmitted by the first execution part **2***pes*, to the second execution part **2***peu*, so as to trigger the execution of the corresponding dependent function, said order having the form of at least one argument of the triggering command,

[0482] a method of renaming of the orders designed to be used during the modification of the vulnerable software **2***v*, such a method enabling to rename the orders so as to obtain triggering commands with renamed orders enabling to conceal the identity of the corresponding dependent functions,

[0483] and restoring means **20** designed to be used in the unit **6** during the usage phase and enabling to restore the initial order, from the renamed order, so as to restore the dependent function to execute.

[0484] For the implementation of the principle of protection by renaming, are also constructed exploitation means enabling to transform a blank unit **60** containing memorization means **15** and processing means **16** into a unit **6** implementing at least the restoring means **20**.

[0485] For the implementation of the principle of protection by renaming, are also chosen, in the source of the vulnerable software **2***vs:*

[0486] at least one algorithmic processing using at least one operand and returning at least one result,

[0487] and at least one portion of the source of the vulnerable software **2***vs*, containing at least one chosen algorithmic processing.

[0488] The source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*. This modification is such that, among others:

[0489] during the execution of the protected software **2***p*, at least one portion of the first execution part **2***pes*, which is executed in the data processing system **3**, takes into account that the functionality of at least one chosen algorithmic processing is executed in the unit **6**,

[0490] during the execution of the protected software **2***p*, the second execution part **2***peu*, which is executed in the unit **6**, executes at least the functionality of at least one chosen algorithmic processing,

[0491] each chosen algorithmic processing is split so that during the execution of the protected software **2***p*, each chosen algorithmic processing is executed, by means of the second execution part **2***peu*, using dependent functions. Preferably, each chosen algorithmic processing is split into dependent functions fd_n (with n varying from 1 to N), namely:

[0492] possibly one or several dependent functions enabling the placing of one or several operands at the unit **6**'s disposal,

[0493] dependent functions, some of which use the operand(s) and execute in combination the functionality of the chosen algorithmic processing, using said operand(s),

[0494] and possibly, one or several dependent functions enabling the placing by the unit **6**, at the data processing system **3**'s disposal of the result of the chosen algorithmic processing,

[0495] during the execution of the protected software **2***p*, the second execution part **2***peu* executes the dependent functions fd_n,

[0496] during the execution of the protected software **2***p*, the dependent functions are triggered by triggering commands with renamed orders,

[0497] and a sequence of the triggering commands is chosen among the set of sequences allowing the execution of the protected software **2***p*.

[0498] The first execution part **2***pes* of the protected software **2***p*, executed in the data processing system **3**, executes triggering commands with renamed orders transferring renamed orders to the unit **6**, and triggering in the unit **6** the restoring by means of the restoring means **20**, of the orders, and then the execution by means of the second execution part **2***peu*, of each of the previously defined dependent functions fd_n.

[0499] In other words, the principle of protection by renaming is carried out by renaming the orders of the triggering commands, so as to obtain triggering commands with renamed orders whose execution in the data processing system **3**, triggers in the unit **6**, the execution of the dependent functions which would have been triggered by the triggering commands with not-renamed orders, without however the examination of the protected software **2***p* enabling to determine the identity of the executed dependent functions.

[0500] FIG. **80** illustrates an example of execution of a vulnerable software **2***v*. In this example, appears during the execution of the vulnerable software **2***v* in the data processing system **3**, at a certain time instant, the calculation of $Z \leftrightarrows F(X, Y)$ corresponding to the assignment to a variable Z of the result of an algorithmic processing represented by a function F and using the operands X and Y.

[0501] FIGS. **81** and **82** illustrate an example of implementation of the invention.

[0502] FIG. **81** illustrates the partial implementation of the invention. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p* and in the presence of the unit **6**, appear:

[0503] at time instants t_1, t_2, the execution of the triggering commands CD_1, CD_2 triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the corresponding dependent functions fd_1, fd_2 which provide the transfer of data X, Y from the data processing system **3** to the memorization zones respectively x, y located in the memorization means **15** of the unit **6**, said triggering commands CD_1, CD_2 being represented respectively by OUT(x, X), OUT(y, Y),

[0504] at time instants t_3 to t_{N-1}, the execution of the triggering commands CD_3 to CD_{N-1}, triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the corresponding dependent functions fd_3 to fd_{N-1}, said triggering commands CD_3 to CD_{N-1} being represented respectively, by $TRIG(fd_3)$ to $TRIG(fd_{N-1})$. The series of dependent functions fd_3 to fd_{N-1} executed in combination is algorithmically equivalent to the function F. More precisely, the execution of said triggering commands leads to the execution in the unit **6**, of the dependent functions fd_3 to fd_{N-1} which use the contents of the memorization zones x, y and return the result in a memorization zone z of the unit **6**,

[0505] and at time instant t_N, the execution of a triggering command CD_N triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the dependent function fd_N providing the transfer of the result of the algorithmic processing contained in the memorization zone z of the unit **6** to the data processing system **3**, so as to assign it to the variable Z, said command being represented by IN(z).

[0506] In this example, to completely implement the invention, are chosen as orders, the first argument of the triggering commands OUT and the argument of the triggering commands TRIG and IN. The orders chosen in this way are renamed using the method of renaming of the orders. In this manner, the orders of the triggering commands CD_1 to CD_N i.e. x, y, fd_3, fd_{N-1}, z are renamed so as to obtain respectively R(x), R(y), $R(fd_3)$ . . . , $R(fd_{N-1})$, R(z).

[0507] FIG. **82** illustrates the complete implementation of the invention. In this example, during the execution in the data processing system **3**, of the first execution part **2***pes* of the protected software **2***p*, and in the presence of the unit **6**, appear:

[0508] at time instants t_1, t_2, the execution of the triggering commands with renamed orders $CDCR_1$, $CDCR_2$, transferring to the unit **6**, the renamed orders R(x), R(y) as well as the data X, Y triggering in the unit **6** the restoring by means of the restoring means **20**, of the renamed orders to restore the orders i.e. the identity of the memorization zones x, y, and then the execution by means of the second execution part **2***peu*, of the corresponding dependent functions fd_1, fd_2 which provide the transfer of the data X, Y from the data processing system **3** to the memorization zones respectively x, y located in the memorization means **15** of the unit **6**, said triggering commands with renamed orders $CDCR_1$, $CDCR_2$ being represented respectively by OUT (R(x), X), OUT (R(y), Y),

[0509] at time instants t_3 to t_{N-1}, the execution of the triggering commands with renamed orders $CDCR_3$ to $CDCR_{N-1}$, transferring to the unit **6**, the renamed orders $R(fd_3)$ to $R(fd_{N-1})$, triggering in the unit **6** the restoring by means of the restoring means **20**, of the orders, i.e. fd_3 to fd_{N-1}, and then the execution by means of the second execution part **2***peu*, of the dependent functions fd_3 to fd_{N-1}, said triggering commands with renamed orders $CDCR_3$ to $CDCR_{N-1}$ being represented respectively by TRIG ($R(fd_3)$) to TRIG ($R(fd_{N-1})$),

[0510] and at time instant t_N, the execution of the triggering command with renamed order $CDCR_N$ transferring to the unit **6**, the renamed order R(z) triggering in the unit **6** the restoring by means of restoring means **20**, of the order i.e. the identity of the memorization zone z, and then the execution by means of the second execution part **2***peu*, of the dependent function fd_N providing the transfer of the result of the algorithmic processing contained in the memorization zone z of the unit **6** to the data processing system **3**, so as to assign it to the variable Z, said triggering command with renamed order $CDCR_N$ being represented by IN (R(z)).

[0511] In the illustrated example, the triggering commands with renamed orders 1 to N are executed successively. It should be observed that two improvements can be effected:

[0512] The first improvement concerns the case where several algorithmic processings are remoted to the unit **6** and at least the result of one algorithmic processing is used by another algorithmic processing. In this case, some triggering commands with renamed orders used for the transfer, can possibly be removed.

[0513] The second improvement aims at opting for a pertinent sequence of the triggering commands with renamed orders among the set of sequences allowing the execution of the protected software **2***p*. In this respect, it is preferable to choose a sequence of the triggering commands with renamed orders which dissociate temporally the execution of the dependent functions, by intercalating, between them portions of code executed in the data processing system **3** and including or not triggering commands with renamed orders used of the determination of other data. FIGS. **83** and **84** illustrate the principle of such an embodiment.

[0514] FIG. **83** shows an example of execution of a vulnerable software **2***v*. In this example, appears, during the execution of the vulnerable software **2***v*, in the data processing system **3**, the execution of two algorithmic processings leading to the determination of Z and Z', such as $Z \leftrightarrows F(X, Y)$ and $Z' \leftrightarrows F'(X', Y')$.

[0515] FIG. **84** illustrates an example of implementation of the process according to the invention for which the two algorithmic proccesings chosen in FIG. **83** are remoted to the unit **6**. According to such an example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p* and in the presence of the unit **6**, appear, as explained above, the execution of the triggering commands with renamed orders $CDCR_1$ to $CDCR_N$ corresponding to the determination of Z and the execution of the triggering commands with renamed orders $CDCR'_1$ to $CDCR'_M$ corresponding to the determination of Z'. As illustrated, the triggering commands with renamed orders $CDCR_1$ to $CDCR_N$ are not executed consecutively, inasmuch as the triggering commands with renamed orders $CDCR'_1$ to $CDCR'_M$ as well as other portions of code are intercalated. In the example, the following sequence is thus carried out: $CDCR_1$, portion of intercalated code, $CDCR'_1$, $CDCR_2$, portion of intercalated code, $CDCR'_2$, $CDCR'_3$, portion of intercalated code, $CDCR'_4$, $CDCR_3$, $CDCR_4$, . . . , $CDCR_N$, $CDCR'_M$.

[0516] It should be observed that, during the execution of a portion of the first execution part **2***pes* of the protected software **2***p*, the triggering commands with renamed orders executed in the data processing system **3**, trigger in the unit **6** the restoring of the identity of the corresponding dependent functions and then their execution. Thus, it appears that in the presence of the unit **6**, said portion is executed correctly and that, consequently, the protected software **2***p* is completely functional.

[0517] FIG. **85** illustrates an example of an attempt of execution of the protected software **2***p*, when the unit **6** is missing. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p*, at every time instant, the execution of a triggering command with renamed order can trigger neither the restoring of the order nor the execution of the corresponding dependent function, because of the absence of the unit **6**. The value to assign to the variable Z cannot therefore be determined correctly.

[0518] It therefore appears, that in the absence of the unit **6**, at least one request by a portion of the first execution part **2***pes* of the protected software **2***p*, to trigger the restoring of an order and the execution of a dependent function in the unit **6** cannot be fulfilled correctly, so that at least said portion is not executed correctly and that, consequently, the protected software **2***p* is not completely functional.

[0519] Thanks to this principle of protection by renaming, the examination in the protected software **2***p* of the triggering commands with renamed orders does not enable to determine the identity of the dependent functions which have to be executed in the unit **6**. It should be observed that the renaming of the orders is carried out during the modification of the vulnerable **2***v* to a protected software **2***p*.

[0520] According to a variant of the principle of protection by renaming, is defined for at least one dependent function, a family of dependent functions algorithmically equivalent but triggered by different triggering commands with renamed orders. According to this variant, for at least one algorithmic processing using dependent functions, said algorithmic processing is split into dependent functions which for at least one of them is replaced with a dependent function of the same family instead of keeping several occurrences of the same dependent function. To this end, triggering commands with renamed orders are modified to take into account the replacement of dependent functions with dependent functions of the same family. In other words, two dependent functions of the same family have different orders and consequently different triggering commands with renamed orders and, it is not possible, by examining the protected software **2***p*, to discover that the dependent functions called are algorithmically equivalent.

[0521] According to a first preferred embodiment of the variant of the principle of protection by renaming, is defined for at least one dependent function, a family of algorithmically equivalent dependent functions, by concatenating a noise field to the information defining the functional part of the dependent function to execute in the unit **6**.

[0522] According to a second preferred embodiment of the variant of the principle of protection by renaming, is defined for at least one dependent function, a family of algorithmically equivalent dependent functions by using identification fields.

[0523] According to a preferred variant embodiment of the principle of protection by renaming, is defined as method of renaming of the orders a ciphering method enabling to cipher the orders to transform them into renamed orders. Remember that the renaming of the orders is carried out during the phase of protection P. For this preferred variant, the restoring means **20** are means implementing a deciphering method enabling to decipher the renamed orders and thus to restore the identity of the dependent functions to execute in the unit **6**. Said restoring means are implemented in the unit **6** and can be of software or hardware nature. Said restoring means **20** are appealed to during the usage phase U each time a triggering command with renamed order is

executed in the data processing system **3** with the intention of triggering in the unit **6**, the execution of a dependent function.

[**0524**] According to another advantageous characteristic of the invention, the protection process aims at implementing a principle of protection called by <<conditional branch>> a description of which is carried out in relation to FIGS. **90** to **92**.

[**0525**] For the implementation of the principle of protection by conditional branch, is chosen in the source of the vulnerable software **2***vs*, at least one conditional branch BC. Is also chosen at least one portion of the source of the vulnerable software **2***vs* containing at least one chosen conditional branch BC.

[**0526**] At least one chosen portion of the source of the vulnerable software **2***vs* is then modified, so as to obtain the source of the protected software **2***ps*. This modification is such that, during the execution of the protected software **2***p*, among others:

[**0527**] at least one portion of the first execution part **2***pes*, which is executed in the data processing system **3**, takes into account that the functionality of at least one chosen conditional branch BC is executed in the unit **6**,

[**0528**] and the second execution part **2***peu*, which is executed in the unit **6**, executes at least the functionality of at least one chosen conditional branch BC and puts at the data processing system **3**'s disposal, a piece of information enabling the first execution part **2***pes*, to carry on its execution at the chosen spot.

[**0529**] The first execution part **2***pes* of the protected software **2***p*, executed in the data processing system **3**, executes conditional branches commands, triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of remoted conditional branches bc whose functionality is equivalent to the functionality of the chosen conditional branches BC. For the implementation of the principle of protection by conditional branch, the unit **6** includes memorization means **15** and processing means **16**.

[**0530**] FIG. **90** illustrates an example of execution of a vulnerable software **2***v*. In this example, appears, during the execution of the vulnerable software **2***v* in the data processing system **3** at a certain time instant, a conditional branch BC indicating to the vulnerable software **2***v* the spot where to carry on its execution, i.e. one of the three possible spots B_1, B_2 or B_3. It must be understood that the conditional branch BC takes the decision to carry on the execution of the software at spot B_1, B_2 or B_3.

[**0531**] FIG. **91** illustrates an example of implementation of the invention for which the conditional branch chosen to be remoted to the unit **6**, corresponds to the conditional branch BC. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p* and in the presence of the unit **6**, appear:

[**0532**] at time instant t_1, the execution of the conditional branch command CBC_1 triggering in the unit **6**, the execution by means of the second execution part **2***peu*, of the remoted conditional branch bc algorithmically equivalent to the conditional branch BC, said conditional branch command CBC_1 being represented by TRIG(bc),

[**0533**] and at time instant t_2, the transfer from the unit **6** to the data processing system **3**, of the information enabling the first execution part **2***pes*, to carry on its execution at the chosen spot, i.e. the spot B_1, B_2 or B_3.

[**0534**] It should be observed that during the execution of a portion of the first execution part **2***pes* of the protected software **2***p*, the conditional branches commands executed in the data processing system **3** trigger the execution of the corresponding remoted conditional branches in the unit **6**. Thus, it appears, that in the presence of the unit **6**, said portion is executed correctly and that, consequently, the protected software **2***p* is completely functional.

[**0535**] FIG. **92** illustrates an example of an attempt of execution of the protected software **2***p*, when the unit **6** is missing. In this example, during the execution in the data processing system **3** of the first execution part **2***pes* of the protected software **2***p:*

[**0536**] at time instant t_1, the execution of the conditional branch command CBC_1, cannot trigger the execution of the remoted conditional branch bc, taking into account the absence of the unit **6**,

[**0537**] and at time instant t_2, the transfer of the piece of information enabling the first execution part **2***pes* to carry on at the chosen spot fails taking into account the absence of the unit **6**.

[**0538**] It therefore appears that in the absence of the unit **6**, at least one request by a portion of the first execution part **2***pes* to trigger the execution of a remoted conditional branch in the unit **6**, cannot be fulfilled correctly, so that at least said portion is not executed correctly and that, consequently, the protected software **2***p* is not completely functional.

[**0539**] In the previous description in relation to FIGS. **90** to **92**, the subject of the invention aims at remoting in the unit **6**, a conditional branch. Naturally, a preferred embodiment of the invention can be carried out by remoting in the unit **6**, a series of conditional branches whose overall functionality is equivalent to all the functionalities of the conditional branches which have been remoted. The execution of the overall functionality of said series of remoted conditional branches leads to the placing at the data processing system **3**'s disposal of a piece of information enabling the first execution part **2***pes* of the protected software **2***p* to carry on its execution at the chosen spot.

[**0540**] In the previous description in relation to FIGS. **40** to **92**, six different principles of software protection have been made explicit generally speaking independently of one another. The protection process in accordance with the invention, is implemented by using the principle of protection by variable, possibly combined with one or several other principles of protection. In the case where the principle of protection by variable is complemented by the implementation of at least another principle of protection, the principle of protection by variable is advantageously complemented by the principle of protection by temporal dissociation and/or the principle of protection by elementary functions.

[0541] And when the principle of protection by temporal dissociation is also implemented, it can be complemented in its turn by the principle of protection by elementary functions and/or the principle of protection by conditional branch.

[0542] And when the principle of protection by elementary functions is also implemented, it can be complemented in its turn by the principle of protection by detection and coercion and/or the principle of protection by renaming and/or the principle of protection by conditional branch.

[0543] And when the principle of protection by detection and coercion is also implemented, it can be complemented in its turn by the principle of protection by renaming and/or the principle of protection by conditional branch.

[0544] And when the principle of protection by renaming is also implemented, it can be complemented in its turn by the principle of protection by conditional branch.

[0545] According to the preferred variant embodiment, the principle of protection by variable is complemented by the principle of protection by temporal dissociation, complemented by the principle of protection by elementary functions, complemented by the principle of protection by detection and coercion, complemented by the principle of protection by renaming, complemented by the principle of protection by conditional branch.

[0546] In the case where a principle of protection is applied, in complement to the principle of protection by variable, its previously carried out description must include, to take into account its combined implementation, the following modifications:

[0547] the notion of vulnerable software must be understood as software vulnerable towards the principle of protection being described. Thus, in the case where a principle of protection has already been applied to the vulnerable software, the expression "vulnerable software" must be interpreted by the reader as the expression "software protected by the principle(s) of protection already applied";

[0548] the notion of protected software must be understood as software protected towards the principle of protection being described. Thus, in the case where a principle of protection has already been applied, the expression "protected software" must be interpreted by the reader as the expression "new version of the protected software";

[0549] and the choice(s) made for the implementation of the principle of protection being described must take into account the choice(s) made for the implementation of the principle(s) of protection already applied.

[0550] The rest of the description enables to have a better understanding of the implementation of the protection process in accordance with the invention. This protection process according to the invention is composed, as shown more precisely in FIG. **100**:

[0551] first, of a protection phase P during which a vulnerable software **2***v* is modified to become a protected software **2***p*,

[0552] then, of a usage phase U during which the protected software **2***p* is used. During this usage phase U:

[0553] in the presence of the unit **6** and each time a portion of the first execution part **2***pes* executed in the data processing system **3** imposes it, an imposed functionality is executed in the unit **6**, so that said portion is executed correctly and that, consequently, the protected software **2***p* is completely functional,

[0554] in the absence of the unit **6** and in spite of the request by a portion of the first execution part **2***pes* to execute a functionality in the unit **6**, said request cannot be fulfilled correctly, so that at least said portion is not executed correctly and that consequently, the protected software **2***p* is not completely functional,

[0555] and possibly of a phase of refilling R during which is credited at least one additional usage of a functionality protected by the implementation of the second preferred variant embodiment of the principle of protection by detection and coercion using as characteristic, a variable of measurement.

[0556] The protection phase P can be split into two protection sub-phases P_1 and P_2. The first one, called prior protection sub-phase P_1, takes place independently of the vulnerable software **2***v* to protect. The second one, called subsequent protection sub-phase P_2 is dependent of the vulnerable software **2***v* to protect. It should be observed that the prior protection sub-phase P_1 and the subsequent protection sub-phase P_2 can be carried out advantageously by two different persons or two different teams. For instance, the prior protection sub-phase P_1 can be carried out by a person or a company providing the development of software protection systems, while the subsequent protection sub-phase P_2 can be carried out by a person or a company providing the development of software requiring to be protected. Naturally, it is clear that the prior protection sub-phase P_1 and the subsequent protection sub-phase P_2 can also be carried out by the same person or team.

[0557] The prior protection sub-phase P_1 is composed of several stages $S_{11}, \ldots, S_{1i}$ for each of which various tasks or jobs are to be carried out.

[0558] The first stage of this prior protection sub-phase P_1 is called "definitions stage S_{11}". During this definitions stage S_{11}:

[0559] are chosen:

[0560] the type of the unit **6**, namely in particular a memorizing unit or a processing and memorizing unit. As an illustrative example, can be chosen as unit **6**, a chip card reader **8** and the chip card **7** associated to the reader,

[0561] and the transfer means **12**, **13** designed to be implemented respectively in the data processing system **3** and in the unit **6**, during the usage phase U and capable of providing the transfer of data between the data processing system **3** and the unit **6**,

[0562] and in the case where the protection process according to the invention implements the principle of protection by elementary function, are also defined:

[0563] a set of elementary functions whose elementary functions are liable to be executed in the unit **6**,

[0564] and a set of elementary commands for said set of elementary functions, said elementary commands being liable to be executed in the data processing system **3** and to trigger the execution in the unit **6**, of the elementary functions,

[0565] and in the case where the protection process according to the invention implements the principle of protection by detection and coercion, are also defined:

[0566] at least one software execution characteristic, liable to be monitored at least in part in the unit **6**,

[0567] at least one criterion to abide by for at least one software execution characteristic,

[0568] detection means **17** to implement in the unit **6** and enabling to detect that at least one software execution characteristic does not abide by at least one associated criterion,

[0569] and coercion means **18** to implement in the unit **6** and enabling to inform the data processing system **3** and/or modify the execution of a software, when at least one criterion is not abided by,

[0570] and in the case where the protection process according to the invention implements the principle of protection by detection and coercion using as characteristic a variable of measurement of the software execution, are also defined:

[0571] as software execution characteristic liable to be monitored, a variable of measurement of the usage of a functionality of a software,

[0572] as criterion to abide by, at least one threshold associated to each variable of measurement,

[0573] and actualization means enabling to update at least one variable of measurement,

[0574] and in the case where the protection process according to the invention also implements a first preferred variant embodiment of the principle of protection by detection and coercion using as characteristic a variable of measurement of the software execution, are also defined:

[0575] for at least one variable of measurement, several associated thresholds,

[0576] and different coercion means corresponding to each of said thresholds,

[0577] and in the case where the protection process according to the invention implements a second preferred variant embodiment of the principle of protection by detection and coercion using as characteristic a variable of measurement of the software execution, are also defined refilling means enabling to add at least one additional usage to at least one software functionality monitored by a variable of measurement,

[0578] and in the case where the protection process according to the invention implements the principle of protection by detection and coercion using as characteristic a profile of software usage, are also defined:

[0579] as software execution characteristic liable to be monitored, a profile of software usage,

[0580] and as criterion to abide by, at least one feature of software execution,

[0581] and in the case where the protection process according to the invention implements the principle of protection by detection and coercion using as feature of execution to abide by, the monitoring of the execution chaining, are also defined:

[0582] an instructions set whose instructions are liable to be executed in the unit **6**,

[0583] a set of instructions commands for said instructions set, said instructions commands being liable to be executed in the data processing system **3** and to trigger in the unit **6** the execution of the instructions,

[0584] as profile of usage, the chaining of the instructions,

[0585] as feature of execution, an expected chaining for the execution of the instructions,

[0586] as detection means **17**, means enabling to detect that the chaining of the instructions does not correspond to the expected one,

[0587] and as coercion means **18**, means enabling to inform the data processing system **3** and/or to modify the functioning of the portion of protected software **2***p* when the chaining of the instructions does not correspond to the expected one,

[0588] and in the case where the protection process according to the invention implements a preferred variant embodiment of the principle of protection by detection and coercion using as feature of execution to abide by, the monitoring of the execution chaining, are also defined:

[0589] as instructions set, an instructions set whose at least some instructions work with registers and use at least one operand with the intention of returning a result,

[0590] for at least some of the instructions working with registers:

[0591] a part PF defining the functionality of the instruction,

[0592] and a part defining the expected chaining for the execution of the instructions and including bits fields corresponding to:

[0593] an identification field of the instruction CII,

[0594] and for each operand of the instruction:

[0595] a flag field CD_k,

[0596] and an expected identification field CIP_k of the operand,

[0597] for each register belonging to the exploitation means and used by the instructions set, a generated identification field CIG_v in which is automatically memorized the identification of the last instruction which has returned its result in said register,

[0598] as detection means **17**, means enabling, during the execution of an instruction, for each operand, when the flag field CD_k imposes it, to check the equality of the generated identification field CIG_v corresponding to

the register used by said operand, and the expected identification field CIP_k of the origin of said operand,

[0599] and as coercion means **18**, means enabling to modify the result of the instructions, if at least one of the checked equalities is false.

[0600] and in the case where the protection process according to the invention implements the principle of protection by renaming, are also defined:

[0601] as a triggering command, an elementary command or an instruction command,

[0602] as a dependent function, an elementary function or an instruction,

[0603] as an order, at least one argument for a triggering command, corresponding at least in part to the information transmitted by the data processing system **3** to the unit **6**, so as to trigger the execution of the corresponding dependent function,

[0604] a method of renaming of the orders enabling to rename the orders so as to obtain triggering commands with renamed orders,

[0605] and restoring means **20** designed to be used in the unit **6** during the usage phase U, and enabling to restore the dependent function to execute, from the renamed order,

[0606] and in the case where the protection process according to the invention implements a variant of the principle of protection by renaming, is also defined for at least one dependent function, a family of dependent functions algorithmically equivalent, but triggered by triggering commands whose renamed orders are different,

[0607] and in the case where the protection process according to the invention implements one of the preferred embodiments of the variant of the principle of protection by renaming, are also defined for at least one dependent function, a family of algorithmically equivalent dependent functions:

[0608] by concatenating a field of noise to the information defining the functional part of the dependent function to execute in the unit **6**,

[0609] or by using the identification field of the instruction CII and the expected identification fields CIP_k of the operands.

[0610] and in the case where the protection process according to the invention implements a preferred variant of the principle of protection by renaming, are also defined:

[0611] as method of renaming of the orders, a ciphering method to cipher the orders,

[0612] and as restoring means **20**, means implementing a deciphering method to decipher the renamed orders and thus restore the identity of the dependent functions to execute in the unit **6**.

[0613] During the prior protection sub-phase P_1, the definitions stage S_{11} is followed by a stage called "construction stage S_{12}". During such a stage S_{12}, are constructed the transfer means **12**, **13** and the exploitation means corresponding to the definitions of the definitions stage S_{11}.

[0614] During this construction stage S_{12}, are therefore carried out:

[0615] the construction of the transfer means **12**, **13** enabling, during the usage phase U, the transfer of data between the data processing system **3** and the unit **6**,

[0616] and when the principle of protection by elementary functions is also implemented, the construction of the exploitation means also enabling the unit **6**, during the usage phase U to execute the elementary functions of the set of elementary functions,

[0617] and when the principle of protection by detection and coercion is also implemented, the construction:

[0618] of the exploitation means enabling the unit **6**, during the usage phase U to also implement the detection means **17** and the coercion means **18**,

[0619] and possibly of the exploitation means enabling the unit **6**, during the usage phase U to also implement the actualization means,

[0620] and possibly of the exploitation means enabling the unit **6**, during the usage phase U to also implement the refilling means,

[0621] and possibly of the exploitation means also enabling the unit **6**, during the usage phase U to execute the instructions of the instructions set,

[0622] and when the principle of protection by renaming is also implemented, the construction of the exploitation means enabling the unit **6**, during the usage phase U to also implement the restoring means.

[0623] The construction of the exploitation means is carried out classically, through a program development unit and taking into account the definitions intervened in the definitions stages S_{11}. Such a unit is described in the rest of the description in FIG. **110**.

[0624] During the prior protection sub-phase P_1, the construction stage S_{12} can be followed by a stage called "pre-customization stage S_{13}". During this pre-customization stage S_{13}, at least a part of the transfer means **13** and/or the exploitation means are uploaded to at least one blank unit **60**, with the intention of obtaining at least one pre-customized unit **66**. It should be observed that part of the exploitation means, once transferred to a pre-customized unit **66**, is no longer directly accessible outside said pre-customized unit **66**. The transfer of the exploitation means to a blank unit **60** can be carried out through an adapted pre-customization unit, which is described in the rest of the description in FIG. **120**. In the case of a pre-customized unit **66**, constituted by a chip card **7** and its reader **8**, the pre-customization concerns only the chip card **7**.

[0625] During the prior protection sub-phase P_1, after the definitions stage S_{11} and, possibly after the construction stage S_{12}, a stage called "tools making stage S_{14}" can take place. During this tools making stage S_{14} are made tools enabling to help generate protected software or automate the protection of software. Such tools enable:

[0626] to help choose or to choose automatically in the vulnerable software **2***v* to protect:

[0627] the variable(s) liable to be remoted in the unit **6**,

[0628] the portion(s) liable to be modified,

[0629] and when the principle of protection by temporal dissociation is also implemented, the algorithmic processing(s) liable to be split into steps remotable in the unit **6**,

[0630] and when the principle of protection by elementary functions is also implemented, the algorithmic processing(s) liable to be split into elementary functions remotable in the unit **6**,

[0631] and when the principle of protection by detection and coercion is also implemented, the execution characteristic(s) to monitor and, possibly, the algorithmic processing(s) liable to be split into instructions remotable in the unit **6**,

[0632] and when the principle of protection by renaming is also implemented, the algorithmic processing(s) liable to be split into dependent functions remotable in the unit **6** and for which the orders of the triggering commands can be renamed,

[0633] and when the principle of protection by conditional branch is also implemented, the conditional branch(es) whose functionality is liable to be remoted in the unit **6**,

[0634] and, possibly, to help generate protected software or to automate the protection of software.

[0635] These different tools can be carried out independently or in combination and each tool can have various forms, such as for instance pre-processor, assembler, compiler, etc.

[0636] The prior protection sub-phase P_1 is followed by a subsequent protection sub-phase P_2 which depends on the vulnerable software **2***v* to protect. This subsequent protection sub-phase P_2 is composed of several stages as well. The first stage corresponding to the implementation of the principle of protection by variable is called "creation stage S_{21}". During this creation stage S_{21}, the choices made during the definition stage S_{11} are used. With the aid of said choices and possibly of tools constructed during the tools making stage S_{14}, the protected software **2***p* is created:

[0637] by choosing in the source of the vulnerable software **2***vs:*

[0638] at least one variable which, during the execution of the vulnerable software **2***v*, partially defines the state of the latter,

[0639] and at least one portion containing at least one chosen variable,

[0640] by producing a source of the protected software **2***ps* from the source of the vulnerable software **2***vs*, by modifying at least one chosen portion of the source of the vulnerable software **2***vs*, this modification being such that during the execution of the protected software **2***p*, at least one chosen variable or at least one copy of chosen variable resides in the blank unit **60** which is thus transformed into a unit **6**,

[0641] and by producing a first object part **2***pos* of the protected software **2***p* from the source of the protected software **2***ps*, said first object part **2***pos* being such that during the execution of the protected software **2***p*, appears a first execution part **2***pes* which is executed in the data processing system **3** and whose at least a portion takes into account that at least a variable or at least a copy of variable resides in the unit **6**.

[0642] Naturally, the principle of protection by variable according to the invention can be applied directly during the development of a new software without requiring the prior realization of a vulnerable software **2***v*. In this way, a protected software **2***p* is obtained directly.

[0643] During the subsequent protection sub-phase P_2, and when at least another principle of protection is applied in addition to the principle of protection by variable, a "modification stage S_{22}" takes place. During this modification stage S_{22}, the definitions intervened during the definitions stage S_{11} are used. With the aid of said definitions and possibly of tools constructed during the tools making stage S_{14}, the protected software **2***p* is modified to allow the implementation of the principles of protection according to one of the arrangements herebefore defined.

[0644] When the principle of protection by temporal dissociation is implemented, the protected software **2***p* is modified:

[0645] by choosing in the source of the protected software **2***ps:*

[0646] at least one algorithmic processing which during the execution of the protected software **2***p*, uses at least one chosen variable, and enables to obtain at least one result variable,

[0647] and at least one portion containing at least one chosen algorithmic processing,

[0648] by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that:

[0649] during the execution of the protected software **2***p* the first execution part **2***pes* is executed in the data processing system **3** and a second execution part **2***peu* is executed in the unit **6** which also includes processing means **16**,

[0650] at least the functionality of at least one chosen algorithmic processing is executed by means of the second execution part **2***peu,*

[0651] at least one chosen algorithmic processing is split so that during the execution of the protected software **2***p*, appear, by means of the second execution part **2***peu*, several distinct steps, namely:

[0652] the placing of at least one variable at the unit **6**'s disposal,

[0653] the carrying out in the unit **6**, of the functionality of the algorithmic processing on at least said variable,

[0654] and possibly, the placing of at least one result variable at the data processing system **3**'s disposal by the unit **6**,

[0655] for at least one chosen algorithmic processing, steps commands are defined so that during the execution of the protected software **2***p*, each step command is executed by the first execution part **2***pes* and triggers in the unit **6**, the execution by means of the second execution part **2***peu*, of a step,

[0656] and a sequence of the steps commands is chosen among the set of sequences allowing the execution of the protected software **2***p*,

[0657] and by producing:

[0658] the first object part **2***pos* of the protected software **2***p*, said first object part **2***pos* being such that during the execution of the protected software **2***p*, the steps commands are executed according to the chosen sequence,

[0659] and a second object part **2***pou* of the protected software **2***p*, said second object part **2***pou* being such that, after upload to the blank unit **60** and during the execution of the protected software **2***p*, appears the second execution part **2***peu* by means of which the steps triggered by the first execution part **2***pes* are executed.

[0660] When the principle of protection by elementary functions is implemented whereas the principle of protection by temporal dissociation is not implemented, the protected software **2***p* is modified:

[0661] by choosing in the source of the protected software **2***ps*:

[0662] at least one algorithmic processing which during the execution of the protected software **2***p*, uses at least one chosen variable, and enables to obtain at least one result variable,

[0663] and at least one portion containing at least one chosen algorithmic processing,

[0664] by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that:

[0665] during the execution of the protected software **2***p* the first execution part **2***pes* is executed in the data processing system **3** and a second execution part **2***peu* is executed in the unit **6**,

[0666] at least the functionality of at least one chosen algorithmic processing is executed by means of the second execution part **2***peu*,

[0667] at least one chosen algorithmic processing is split so that during the execution of the protected software **2***p*, said algorithmic processing is executed by means of the second execution part **2***peu*, using elementary functions,

[0668] for at least one chosen algorithmic processing, elementary commands are integrated to the source of the protected software **2***ps*, so that during the execution of the protected software **2***p*, each elementary command is executed by the first execution part **2***pes* and triggers in the unit **6**, the execution by means of the second execution part **2***peu*, of an elementary function,

[0669] and a sequence of the elementary commands is chosen among the set of sequences allowing the execution of the protected software **2***p*,

[0670] and by producing:

[0671] the first object part **2***pos* of the protected software **2***p*, said first object part **2***pos* being such that during the execution of the protected software **2***p*, the elementary commands are executed according to the chosen sequence,

[0672] and a second object part **2***pou* of the protected software **2***p* containing the exploitation means, said second object part **2***pou* being such that, after upload to the blank unit **60** and during the execution of the protected software **2***p*, appears the second execution part **2***peu* by means of which the elementary functions triggered by the first execution part **2***pes* are executed.

[0673] When the principles of protection by temporal dissociation and by elementary functions are both implemented, the protected software **2***p* is modified:

[0674] by choosing in the source of the protected software **2***ps*, at least one step which during the execution of the protected software **2***p*, carries out the functionality of an algorithmic processing,

[0675] by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that:

[0676] at least one chosen step is split so that during the execution of the protected software **2***p*, said step is executed by means of the second execution part **2***peu*, using elementary functions,

[0677] for at least one chosen step, elementary commands are integrated to the source of the protected software **2***ps*, so that during the execution of the protected software **2***p*, each elementary command is executed by the first execution part **2***pes* and triggers in the unit **6**, the execution by means of the second execution part **2***peu*, of an elementary function,

[0678] and a sequence of the elementary commands is chosen among the set of sequences allowing the execution of the protected software **2***p*,

[0679] and by producing:

[0680] the first object part **2***pos* of the protected software **2***p*, said first object part **2***pos* being such that during the execution of the protected software **2***p*, the elementary commands are executed according to the chosen sequence,

[0681] and the second object part **2***pou* of the protected software **2***p* also containing the exploitation means, said second object part **2***pou* being such that, after upload to the unit **6** and during the execution of the protected software **2***p*, appears the second execution part **2***peu* by means of which the elementary functions triggered by the first execution part **2***pes* are executed.

[0682] When the principle of protection by detection and coercion is implemented, the protected software **2***p* is modified:

[0683] by choosing at least one software execution characteristic to monitor, among the software execution characteristics liable to be monitored,

[0684] by choosing at least one criterion to abide by for at least one chosen software execution characteristic,

[0685] by choosing in the source of the protected software **2***ps*, elementary functions for which at least one chosen software execution characteristic is to be monitored,

[0686] by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that during the execution of the protected software **2***p*, at least one chosen execution characteristic is monitored by means of the second execution part **2***peu*, and the fact that a criterion is not abided by leads to the data processing system **3** being informed and/or to a modification of the execution of the protected software **2***p*,

[0687] and by producing the second object part **2***pou* of the protected software **2***p* containing the exploitation means also implementing the detection means **17** and the coercion means **18**, said second object part **2***pou* being such that, after upload to the unit **6** and during the execution of the protected software **2***p*, at least one software execution characteristic is monitored and the fact that a criterion is not abided by leads to the data processing system **3** being informed and/or to a modification of the execution of the protected software **2***p*.

[0688] For the implementation of the principle of protection by detection and coercion using as characteristic a variable of measurement of the software execution, the protected software **2***p* is modified:

[0689] by choosing as software execution characteristic to monitor, at least one variable of measurement of the usage of at least one functionality of a software,

[0690] by choosing:

[0691] at least one functionality of the protected software **2***p* whose usage is liable to be monitored using a variable of measurement,

[0692] at least one variable of measurement used to quantify the usage of said functionality,

[0693] at least one threshold associated to a chosen variable of measurement corresponding to a limit of usage of said functionality,

[0694] and at least one method of update of a chosen variable of measurement depending on the usage of said functionality, and by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that, during the execution of the protected software **2***p*, the variable of measurement is actualized by means of the second execution part **2***peu* depending on the usage of said functionality, and at least one threshold crossing is taken into account.

[0695] For the implementation of a first preferred variant embodiment of the principle of protection by detection and coercion using, as characteristic, a variable of measurement, the protected software **2***p* is modified:

[0696] by choosing in the source of the protected software **2***ps*, at least one chosen variable of measurement to which must be associated several thresholds corresponding to different limits of usage of the functionality,

[0697] by choosing at least two thresholds associated to the chosen variable of measurement,

[0698] and by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that, during the execution of the protected software **2***p*, the crossings of the various thresholds are taken into account differently, by means of the second execution part **2***peu*.

[0699] For the implementation of a second preferred variant embodiment of the principle of protection by detection and coercion using as characteristic, a variable of measurement, the protected software **2***p* is modified:

[0700] by choosing in the source of the protected software **2***ps*, at least one chosen variable of measurement enabling to limit the usage of a functionality and which must be able to be credited with at least one additional usage,

[0701] and by modifying at least one chosen portion, this modification being such that during a phase called of refilling, at least one additional usage of at least one functionality corresponding to a chosen variable of measurement can be credited.

[0702] For the implementation of the principle of protection by detection and coercion using as characteristic, a profile of software usage, the protected software **2***p* is modified:

[0703] by choosing as software execution characteristic to monitor at least one profile of software usage,

[0704] by choosing at least one feature of execution by which at least one chosen profile of usage must abide,

[0705] and by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that, during the execution of the protected software **2***p*, the second execution part **2***peu* abides by all the chosen features of execution.

[0706] For the implementation of the principle of protection by detection and coercion using as feature of execution to abide by, the monitoring of the execution chaining, the protected software **2***p* is modified:

[0707] by modifying at least one chosen portion of the source of the protected software **2***ps*:

[0708] by transforming the elementary functions into instructions,

[0709] by specifying the chaining by which must abide at least some of the instructions during their execution in the unit **6**,

[0710] and by transforming the elementary commands into instructions commands corresponding to the instructions used.

[0711] When the principle of protection by renaming is implemented, the protected software **2***p* is modified:

[0712] by choosing in the source of the protected software **2***ps*, triggering commands,

[0713] by modifying at least one chosen portion of the source of the protected software **2***ps* by renaming the orders of the chosen triggering commands, so as to conceal the identity of the corresponding dependent functions,

[0714] and by producing:

[0715] the first object part **2***pos* of the protected software **2***p*, said first object part **2***pos* being such that during the execution of the protected software **2***p*, the triggering commands with renamed orders are executed,

[0716] and the second object part **2***pou* of the protected software **2***p* containing the exploitation means also implementing the restoring means **20**, said second object part **2***pou* being such that, after upload to the unit **6** and during the execution of the protected software **2***p*, the identity of the dependent functions whose execution is triggered by the first execution part **2***pes* is restored by means of the second execution part **2***peu*, and the dependent functions are executed by means of the second execution part **2***peu*.

[0717] For the implementation of a variant of the principle of protection by renaming, the protected software **2***p* is modified:

[0718] by choosing, in the source of the protected software **2***ps* at least one triggering command with renamed order,

[0719] and by modifying at least one chosen portion of the source of the protected software **2***ps* by replacing at least the renamed order of one chosen triggering command with renamed order, with another renamed order, triggering a dependent function of the same family.

[0720] When the principle of protection by conditional branch is implemented, the protected software **2***p* is modified:

[0721] by choosing, in the source of the protected software **2***ps*, at least one conditional branch carried out in at least one chosen algorithmic processing,

[0722] by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that during the execution of the protected software **2***p*, the functionality of at least one chosen conditional branch is executed, by means of the second execution part **2***peu*, in the unit **6**,

[0723] and by producing:

[0724] the first object part **2***pos* of the protected software **2***p*, said first object part **2***pos* being such that during the execution of the protected software **2***p*, the functionality of at least one chosen conditional branch is executed in the unit **6**,

[0725] and the second object part **2***pou* of the protected software **2***p*, said second object part **2***pou* being such that, after upload to the unit **6** and during the execution of the protected software **2***p*, appears the second execution part **2***peu* by means of which the functionality of at least one chosen conditional branch is executed.

[0726] For the implementation of a preferred embodiment of the principle of protection by conditional branch, the protected software **2***p* is modified:

[0727] by choosing, in the source of the protected software **2***ps*, at least one series of chosen conditional branches,

[0728] by modifying at least one chosen portion of the source of the protected software **2***ps*, this modification being such that during the execution of the protected software **2***p*, the overall functionality of at least one chosen series of conditional branches is executed, by means of the second execution part **2***peu*, in the unit **6**,

[0729] and by producing:

[0730] the first object part **2***pos* of the protected software **2***p*, said first object part **2***pos* being such that during the execution of the protected software **2***p*, the functionality of at least one chosen series of conditional branches is executed in the unit **6**,

[0731] and the second object part **2***pou* of the protected software **2***p*, said second object part **2***pou* being such that, after upload to the unit **6** and during the execution of the protected software **2***p*, appears the second execution part **2***peu* by means of which the overall functionality of at least one chosen series of conditional branches is executed.

[0732] Naturally, the principles of protection according to the invention can be applied directly during the development of a new software without requiring the prior carrying out of intermediate protected pieces of software. In this way, the creation stage S_{21} and the modification stage S_{22} can be carried out concomitantly so as to obtain directly the protected software **2***p*.

[0733] During the subsequent protection sub-phase P_2, in the case where at least another principle of protection is used in complement to the principle of protection by variable, after the creation stage S_{21} of the protected software **2***p*, and possibly after the modification stage S_{22}, a stage called "customization stage S_{23}" takes place. During this customization stage S_{23}, the second object part **2***pou* possibly containing the exploitation means is uploaded to at least one blank unit **60**, with the intention of obtaining at least one unit **6**, or a part of the second object part **2***pou* possibly containing the exploitation means is uploaded to at least one pre-customized unit **66**, with the intention of obtaining at least one unit **6**. The uploading of this customization information enables to make operational at least one unit **6**. It should be observed that part of said information, once transferred to a unit **6**, is not directly accessible outside said unit **6**. The transfer of the customization information to a blank unit **60** or a pre-customized unit **66** can be carried out through an adapted customization unit which is described in

the rest of the description in FIG. **150**. In the case of a unit **6**, constituted by a chip card **7** and its reader **8**, the customization concerns only the chip card **7**.

[**0734**] For the implementation of the protection phase P, various technical means are described more precisely in relation to FIGS. **110**, **120**, **130**, **140** and **150**.

[**0735**] FIG. **110** illustrates an embodiment of a system **25** enabling to implement the construction stage S_{12} which takes into account the definitions intervened during the definitions stage S_{11} and during which are constructed the transfer means **12**, **13** and possibly, the exploitation means intended for the unit **6**. Such a system **25** includes a program development unit or workstation which has classically the form of a computer comprising a system unit, a screen, peripherals such as keyboard-mouse, and including, among others, the following programs: file editors, assemblers, pre-processors, compilers, interpreters, debuggers and link editors.

[**0736**] FIG. **120** illustrates an embodiment of a pre-customization unit **30** enabling to upload at least in part the transfer means **13** and/or the exploitations means to at least one blank unit **60** with the intention of obtaining a pre-customized unit **66**. Said pre-customization unit **30** includes reading and writing means **31** enabling to electrically pre-customize, a blank unit **60** so as to obtain a pre-customized unit **66** to which the transfer means **13** and/or the exploitations means have been uploaded. The pre-customization unit **30** can also include physical customization means **32** of the blank unit **60** which can for instance, have the form of a printer. In the case where the unit **6** is constituted by a chip card **7** and its reader **8**, the pre-customization generally concerns only the chip card **7**.

[**0737**] FIG. **130** illustrates an embodiment of a system **35** enabling to carry out the making of the tools enabling to help generate protected software or to automate software protection. Such a system **35** includes a program development unit or workstation which has classically the form of a computer comprising a system unit, a screen, peripherals such as keyboard-mouse, and including, among others, the following programs: file editors, assemblers, pre-processors, compilers, interpreters, debuggers and link editors.

[**0738**] FIG. **140** illustrates an embodiment of a system **40** enabling to create directly a protected software **2***p* or to modify a vulnerable software **2***v* with the intention of obtaining a protected software **2***p*. Such a system **40** includes a program development unit or workstation which has classically the form of a computer comprising a system unit, a screen, peripherals such as keyboard-mouse, and including, among others, the following programs: file editors, assemblers, pre-processors, compilers, interpreters, debuggers and link editors, as well as tools enabling to help generate protected software or to automate software protection.

[**0739**] FIG. **150** illustrates an embodiment of a customization unit **45** enabling to upload the second object part **2***pou* to at least one blank unit **60** with the intention of obtaining at least one unit **6** or to upload a part of the second object part **2***pou* to at least one pre-customized unit **66** with the intention of obtaining at least one unit **6**. Said customization unit **45** includes reading and writing means **46** enabling to electrically customize, at least one blank unit **60** or at least one pre-customized unit **66**, so as to obtain at least one unit **6**. At the close of this customization, a unit **6** includes the information necessary to the execution of the protected software **2***p*. The customization unit **45** can also include physical customization means **47** for at least one unit **6** which can for instance, have the form of a printer. In the case where a unit **6** is constituted by a chip card **7** and its reader **8**, the customization generally concerns only the chip card **7**.

[**0740**] The protection process according to the invention can be implemented with the following improvements:

[**0741**] It can be planned to use jointly several processing and memorizing units between which is divided out the second object part **2***pou* of the protected software **2***p* so that their joint use enables to execute the protected software **2***p*, the absence of at least one of said processing and memorizing units preventing the usage of the protected software **2***p*.

[**0742**] In the same way, after the pre-customization stage S_{13} and during customization stage S_{23}, the part of the second object part **2***pou* necessary to transform the pre-customized unit **66** into a unit **6** can be contained in a processing and memorizing unit used by the customization unit **45** so as to limit the access to said part of the second object part **2***pou*. Naturally, said part of the second object part **2***pou* can be divided out between several processing and memorizing units so that said part of the second object part **2***pou* is accessible only during the joint use of said processing and memorizing units.

What is claimed is:

1. A method to protect, using at least one blank unit (**60**) including memorization means (**15**), a vulnerable software (**2***v*) against its unauthorized usage, said vulnerable software (**2***v*) being produced from a source (**2***vs*) and working on a data processing system (**3**), said protection process comprising:

during a protection phase (P):

creating a protected software (**2***p*):

by choosing in the source of the vulnerable software (**2***vs*):

at least one variable which, during the execution of the vulnerable software (**2***v*), partially defines the state of the latter,

and at least one portion containing at least one chosen variable,

by producing a source of the protected software (**2***ps*) from the source of the vulnerable software (**2***vs*), by modifying at least one chosen portion of the source of the vulnerable software (**2***vs*), this modification being such that during the execution of the protected software (**2***p*), at least one chosen variable or at least one copy of chosen variable resides in the blank unit (**60**) which is thus transformed into a unit (**6**), and

by producing a first object part (**2***pos*) of the protected software (**2***p*) from the source of the protected software (**2***ps*), said first object part (**2***pos*) being such that during the execution of the protected software (**2***p*), appears a first execution part

(**2***pes*) which is executed in the data processing system (**3**) and whose at least a portion takes into account that at least a variable or at least a copy of variable resides in the unit (**6**), and

during a usage phase (U) during which the protected software (**2***p*) is executed:

in the presence of the unit (**6**), each time a portion of the first execution part (**2***pes*) imposes it, using a variable or a copy of variable residing in the unit (**6**), so that said portion is executed correctly and that, consequently, the protected software (**2***p*) is completely functional, and

in the absence of the unit (**6**), in spite of the request by a portion of the first execution part (**2***pes*) to use a variable or a copy of variable residing in the unit (**6**), not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently the protected software (**2***p*) is not completely functional, wherein said at least one blank unit (**60**) includes only the memorization means (**15**).

2. A method to protect software comprising:

storing a first portion of the software on a first unit, wherein the first unit comprises a memory and a processor;

storing a second portion of the software on a second unit, wherein the second unit comprises a secure processor and a secure memory, wherein the second portion of the software is secret, and wherein the first and second portions of the software form a single program; and

executing the single formed program by utilizing the first and second portions of the software,

wherein the secret second portion of the software comprises at least two computing operations and at least one variable, and

wherein portions of the at least two computing operations are interleaved with each other for transmission from the second unit to the first unit and vise versa, and

wherein the first unit requests the at least one variable from the second unit during the execution of the single formed program.

3. The method of claim 2, wherein portions of the second portion of the software are executed by the secure processor and the first portion of the software is executed by the processor of the first unit.

4. The method of claim 3, wherein:

the at least two computing operations stored of the second portion of the software comprise a first computing operation and a second computing operation,

the first computing operation which uses a first chosen variable to obtain a first result variable,

the second computing operation which uses a second chosen variable to obtain a second result, and

during the execution of the program by the secure processor:

performing a first variable movement by moving the first chosen variable from the first unit into the second unit,

performing a second variable movement by moving the second chosen variable from the first unit into the second unit,

performing a first result movement by moving the first result variable from the second unit into the first unit, and

performing a second result movement by moving the second result variable from the second unit into the first unit,

each of said first and second variable movements, said first and second computing operations, and said first and second result movements comprise an operation,

the first variable movement, the first result movement, and the first computing operation comprise a first set of operations and the second variable movement, the second result movement and the second computing operation comprises a second set of operations, and

at least one operation of one of the sets is interleaved with the operations of the other set.

5. The method according to claim 2, wherein the second unit is a chip medium configured to attach and detach to the first unit.

6. The method according to claim 2, wherein the processor of the second unit is a coprocessor of the processor of the first unit.

7. The method according to claim 2, wherein the second unit is a token.

8. The method according to claim 2, wherein, when the second unit is missing, the program cannot be executed correctly and the software is not completely functional.

9. The method according to claim 2, wherein, when the at least one variable is not provided by the second unit upon request, the program is not executed correctly.

10. The method according to claim 2, wherein the at least two computing operations are elementary functions.

11. The method according to claim 2, further comprising:

storing elementary functions that are to be executed in the second unit; and

providing commands from the first unit provides to the second unit to trigger execution of a respective elementary function.

12. The method according to claim 2, further comprising:

defining instructions set in which instructions work with registers and use at least one operand for returning a result,

wherein at least some of the instructions comprise:

a part defining functionality of the instruction,

a part defining expected chaining for execution of the instruction and comprising bits fields corresponding to an identification field of the instruction, wherein each of the at least one operand comprises: a flag field and an expected identification field,

wherein, for each register used by the instructions set, providing a generated identification field in which the

identification of the last instruction which has returned its result in a respective register is automatically memorized,

wherein, during the execution of an instruction, for each operand, when required by the flag field, checking the equality of the generated identification field corresponding to the register used by said operand, and the expected identification field of the origin of said operand, and modifying the result of the instructions, if at least one of the checked equalities is false.

13. The method according to claim 2, further comprising selecting a part of the software to form the second portion during operation of creating the protected program.

14. A system to protect software comprising:

a first unit comprising a memory and a processor and which stories a first portion of the software; and

a second unit comprising a secure processor and a secure memory and which stores a second portion of the software,

wherein the second portion of the software is secret,

wherein the first and second portions of the software form a single program,

wherein the processor executes the single formed program utilizing the second unit,

wherein the secret second portion of the software comprises at least two computing operations and at least one variable, and

wherein portions of the at least two computing operations are interleaved with each other for transmission from the second unit to the first unit and vise versa, and

wherein the first unit requests the at least one variable from the second unit during the execution of the single formed program.

15. A method to protect, using at least one blank unit (**60**) including at least memorization means (**15**), a vulnerable software (**2***v*) against its unauthorized usage, said vulnerable software (**2***v*) being produced from a source (**2***vs*) and working on a data processing system (**3**), said protection process comprising:

during a protection phase (P):

creating a protected software (**2***p*):

by choosing in the source of the vulnerable software (**2***vs*):

at least one variable which, during the execution of the vulnerable software (**2***v*), partially defines the state of the latter, and

at least one portion containing at least one chosen variable,

by producing a source of the protected software (**2***ps*) from the source of the vulnerable software (**2***vs*), by modifying at least one chosen portion of the source of the vulnerable software (**2***vs*), this modification being such that during the execution of the protected software (**2***p*), at least one chosen variable or at least one copy of chosen variable resides in the blank unit (**60**) which is thus transformed into a unit (**6**), and

by producing a first object part (**2***pos*) of the protected software (**2***p*) from the source of the protected software (**2***ps*), said first object part (**2***pos*) being such that during the execution of the protected software (**2***p*), appears a first execution part (**2***pes*) which is executed in the data processing system (**3**) and whose at least a portion takes into account that at least a variable or at least a copy of variable resides in the unit (**6**), and

during a usage phase (U) during which the protected software (**2***p*) is executed:

in the presence of the unit (**6**), each time a portion of the first execution part (**2***pes*) imposes it, using a variable or a copy of variable residing in the unit (**6**), so that said portion is executed correctly and that, consequently, the protected software (**2***p*) is completely functional, and

in the absence of the unit (**6**), in spite of the request by a portion of the first execution part (**2***pes*) to use a variable or a copy of variable residing in the unit (**6**), not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently the protected software (**2***p*) is not completely functional.

wherein during the protection phase (P):

defining:

a set of elementary functions whose elementary functions are liable to be executed in the unit (**6**) which also includes processing means (**16**), and

a set of elementary commands for said set of elementary functions, said elementary commands being liable to be executed in the data processing system (**3**) and to trigger the execution in the unit (**6**), of the elementary functions,

constructing exploitation means enabling to transform the blank unit (**60**) into the unit (**6**) able to execute the elementary functions of said set, the execution of said elementary functions being triggered by the execution in the data processing system (**3**), of elementary commands,

modifying the protected software (**2***p*):

by choosing in the source of the protected software (**2***ps*): at least one algorithmic processing which during the execution of the protected software (**2***p*), uses at least one chosen variable, and enables to obtain at least one result variable, and at least one portion containing at least one chosen algorithmic processing,

by modifying at least one chosen portion of the source of the protected software (**2***ps*), this modification being such that:

during the execution of the protected software (**2***p*) the first execution part (**2***pes*) is executed in the data processing system (**3**) and a second execution part (**2***peu*) is executed in the unit (**6**),

at least the functionality of at least one chosen algorithmic processing is executed by means of the second execution part (**2***peu*),

said at least one chosen algorithmic processing is executed by means of the second execution part (**2***peu*), using elementary functions of the set of elementary functions,

for at least one chosen algorithmic processing, elementary commands are integrated to the source of the protected software (**2***ps*), so that during the execution of the protected software (**2***p*), each elementary command is executed by the first execution part (**2***pes*) and triggers in the unit (**6**), the execution by means of the second execution part (**2***peu*), of a corresponding elementary function of the set of elementary functions, and

a sequence of the elementary commands is chosen among the set of sequences allowing the execution of the protected software (**2***p*), and

by producing:

the first object part (**2***pos*) of the protected software (**2***p*), said first object part (**2***pos*) being such that during the execution of the protected software (**2***p*), the elementary commands are executed according to the chosen sequence, and

a second object part (**2***pou*) independent of the protected software (**2***p*) containing the exploitation means, said second object part (**2***pou*) being such that, after upload to the blank unit (**60**) and during the execution of the protected software (**2***p*), appears the second execution part (**2***peu*) by means of which the elementary functions triggered by the first execution part (**2***pes*) are executed, and

uploading the second object part (**2***pou*) to the blank unit (**60**), with the intention of obtaining the unit (**6**), and

wherein during the usage phase (U):

in the presence of the unit (**6**) and each time an elementary command contained in a portion of the first execution part (**2***pes*) imposes it, executing the corresponding elementary function in the unit (**6**), so that said portion is executed correctly and that, consequently, the protected software (**2***p*) is completely functional, and

in the absence of the unit (**6**), in spite of the request by a portion of the first execution part (**2***pes*), to trigger the execution of an elementary function in the unit (**6**), not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently, the protected software (**2***p*) is not completely functional.

16. The method according to claim 15, further comprising:

during the protection phase (P):

defining:

as a triggering command, an elementary command,

as a dependent function, an elementary function,

as an order, at least one argument for a triggering command, corresponding at least in part to the information transmitted by the data processing system (**3**) to the unit (**6**), so as to trigger the execution of the corresponding dependent function,

a method of renaming of the orders enabling to rename the orders so as to obtain triggering commands with renamed orders, and

restoring means (**20**) designed to be used in the unit (**6**) during the usage phase (U), and enabling to restore the dependent function to execute, from the renamed order,

constructing exploitation means enabling the unit (**6**) to also implement the restoring means, and

modifying the protected software (**2***p*):

by choosing in the source of the protected software (**2***ps*), triggering commands,

by modifying at least one chosen portion of the source of the protected software (**2***ps*) by renaming the orders of the chosen triggering commands, so as to conceal the identity of the corresponding dependent functions, and

by producing:

the first object part (**2***pos*) of the protected software (**2***p*), said first object part (**2***pos*) being such that during the execution of the protected software (**2***p*), the triggering commands with renamed orders are executed, and

the second object part (**2***pou*) of the protected software (**2***p*) containing the exploitation means also implementing the restoring means (**20**), said second object part (**2***pou*) being such that, after upload to the unit (**6**) and during the execution of the protected software (**2***p*), the identity of the dependent functions whose execution is triggered by the first execution part (**2***pes*) is restored by means of the second execution part (**2***peu*), and the dependent functions are executed by means of the second execution part (**2***peu*), and

during the usage phase (U):

in the presence of the unit (**6**) and each time a triggering command with renamed order, contained in a portion of the first execution part (**2***pes*) imposes it, restoring in the unit (**6**), the identity of the corresponding dependent function and executing it, so that said portion is executed correctly and that, consequently, the protected software (**2***p*) is completely functional, and

in the absence of the unit (**6**), in spite of the request by a portion of the first execution part (**2***pes*), to trigger the execution of a dependent function in the unit (**6**), not being able to fulfill said request correctly, so that at least said portion is not executed correctly and that, consequently, the protected software (**2***p*) is not completely functional.

* * * * *