

G06F 21/00 (2013.01)
G06F 21/31 (2013.01)
G06F 21/36 (2013.01)
G06F 3/023 (2006.01)

(19)
ČESKÁ
REPUBLIKA



ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

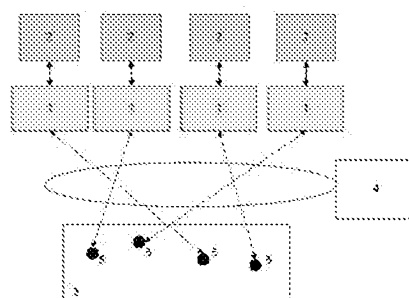
(21) Číslo přihlášky: 2013-558
(22) Přihlášeno: 12.07.2013
(40) Zveřejněno: 21.01.2015
(Věstník č. 3/2015)
(47) Uděleno: 08.07.2022
(24) Oznámení o udělení ve věstníku: 17.08.2022
(Věstník č. 33/2022)

(56) Relevantní dokumenty:
EP 2597590 A2; US 2011090145 A1; US 011246951 A; US 2004030933 A; WO 2009017751 A1; GB 2471142 A; US 2011004769 A; US 2008141362 A1; US 2004030892 A1; WO 02054199 A1; US 2002188872 A1; WO 9618139 A1.

(73) Majitel patentu:
ADUCID s.r.o., Brno, Přízřenice, CZ
(72) Původce:
Ing. Libor Neumann, CSc., Praha 13 - Lužiny, CZ
Ing. Miroslav Řihák, Brno, CZ
(74) Zástupce:
HARBER IP s.r.o., Dukelských hrdinů 567/52,
170 00 Praha 7, Holešovice

(54) Název vynálezu:
**Způsob zadávání tajné informace do
elektronických digitálních zařízení**

(57) Anotace:
Způsob zadávání tajné informace uživatelem do elektronického digitálního zařízení prostřednictvím vstupně/výstupního zařízení, při kterém elektronické digitální zařízení přiřadí každému elementu (2) tajné informace element (1) multimediální informace určené k interakci, přičemž elektronické digitální zařízení zobrazí uživateli při zadávání informace multimediální informaci určenou k interakci obsahující elementy (1) multimediální informace určené k interakci tak, že jejich vzájemný vztah k ovládacím prvkům (5) elektronického digitálního zařízení je mezi jednotlivými zobrazeními proměnný. Uživatel pak vybere elementy (1) multimediální informace určené k interakci přiřazené elementům (2) tajné informace, takže vybráním elementů (1) multimediální informace určené k interakci uživatel vybere k nim přiřazené elementy (2) tajné informace v daném pořadí.



Způsob zadávání tajné informace do elektronických digitálních zařízení

Oblast techniky

5

Vynález se týká způsobu zadávání tajné informace do elektronických digitálních zařízení prostřednictvím běžného vstupně/výstupního zařízení.

10

Dosavadní stav techniky

Znamé způsoby zadávání tajné informace užívají stejné nebo podobné způsoby vstupu tajné informace jako vstupu běžné neutajované informace, který spočívá v přímém propojení ovládacích prvků vstupního zařízení s vkládanou informací.

15

Například pokud je vstupním zařízením klávesnice, je v případě zadávání tajné informace jako je například heslo či PIN běžné, že při zmačknutí příslušné klávesy je zadána informace přímo příslušná této klávese. Podobně fungují také jiné druhy vstupních zařízení jako například virtuální klávesnice zobrazovaná na dotykových displejích, klávesnice zobrazovaná v aplikaci, kde vstupním zařízením je dotyková obrazovka, myš nebo jiný poziční snimač.

20

Analogicky fungují i způsoby zadávání tajné informace využívající přímo informaci o pozici či trajektorii nějakého pozičního vstupního zařízení, např. pozice prstu na dotykové obrazovce.

25

Příkladně je předmětem EP 2597590 A2 autentizační metoda, která identifikační kód (uživatelské jméno) a autentizační kód (uživatelské heslo) společně ukládá do jednoho následně šifrovaného řetězce, který je přenesen na server, na němž je dešifrován a autentizován.

30

Předmětem jiného známého řešení je US 2011090145 A, způsob odemykání mobilního zařízení, který pro přepnutí do odemčeného stavu po uživateli vyžaduje přiřadit k sobě dvě různé informace, které jsou uloženy v paměti mobilního zařízení a patří do stejné skupiny informací. Všechny informace, se kterými se v P2 pracuje, jsou na rozdíl od patentové přihlášky známé uživateli.

35

Předmětem dalšího známého řešení je podle US 011246951 A metoda a elektronický systém pro vícerozměrné vkládání informace, která se používá pro autentizaci. Po spuštění autentizačního procesu je zobrazen vícerozměrný objekt pro zadávání informace, který může být uživatelem otáčen různými způsoby tak, aby byly odkrývány a skrývány jednotlivé strany ("input sides") vícerozměrného objektu, ze kterých následně uživatel vybírá vstupní možnosti ("input options") pro zadání autentizačního kódu do vstupního pole elektronického software. Jednotlivé vstupní možnosti mohou být dále na každé ze stran vícerozměrného objektu zobrazeny v náhodném pořadí. Metoda popsaná v P3 omezuje využití vložené jejím prostřednictvím pouze na autentizaci.

40

45

Podle US 2004030933 A je známá metoda autentizace hesla na mobilním zařízení, která využívá několika různých způsobů uživatelské interakce s mobilním zařízením pro manipulaci objektů klávesnice na displeji z výchozího zobrazení v náhodném pořadí do pořadí dříve určeného pro autentizaci oprávněného uživatele. Mezi způsoby interakce patří například přetažení objektů prstem po dotykovém displeji nebo zatřepání s mobilním zařízením, které je vybaveno senzorem pohybu. Na rozdíl od patentové přihlášky jsou všechny informace, se kterými se pracuje v metodě popsané v P4 známé uživateli.

50

55

Rovněž v 2009017751 A1 je předmětem metoda autentizace uživatele pomocí obrázkového hesla, která zobrazuje uživateli namísto čísel či písmen skupinu náhodně seřazených ikon, ze které uživatel následně po jedné zvolí sekvenci hesla, která je autentizována. Po zadání každého

jednoho vstupu/ikony se může pořadí ikon náhodně změnit. Po zadání každého jednoho vstupu/ikony se mohou i samotné ikony změnit, ale pouze tak, aby oprávněný uživatel stále ikony rozpoznal, např. mohou změnit barvu.

- 5 V GB 2471142 A je zveřejněn systém zadávání hesel a metoda autentizace uživatele tohoto systému. Uživatelské rozhraní systému sestává vždy z alespoň dvou znakových sad, přičemž v primární sadě jsou znaky seřazeny v aritmetické řadě a v ostatních sadách jsou vždy seřazeny náhodně. Zadání jednoho z libovolného množství elementů hesla je provedeno nastavením správné vzájemné pozice tajného páru znaků, ze kterého jeden patří do primární sady a druhý do sekundární sady, a potvrzením této pozice. Od patentové přihlášky se P6 liší tím, že všechny informace se kterými se pracuje v metodě popsané v P6 jsou známy uživateli, přičemž je možné pouze použití symbolů.

- 15 US 2011004769 A řeší systém autentizace "The Pattern Based Password Tool", který autentizuje uživatele na základě číselného jednorázového hesla, které uživatel vypočte pomocí tajného vzorce z náhodně generovaných čísel zobrazených na displeji. Tajný vzorec i výpočet uživatelem jsou klíčovou součástí způsobu podle P7. V patentové přihlášce uživatel neprovádí žádné operace či výpočty a nemusí si pamatovat žádný vzorec, Jedná se opět o autentizační metodu.

- 20 US 2008141362 A1 řeší systém a metoda zadávání hesel pomocí alfanumerické matice, která umožňuje zadávat jednotlivé znaky hesla takovým způsobem, že uživatel zvolí vždy znak v předem určené vzájemné poloze se znakem, který je skutečným znakem uživatele hesla. Metoda dále popisuje možnost náhodně přemístit znaky na alfanumerické matici po zadání každého znaku. Na rozdíl od patentové přihlášky, P8 popisuje volbu skutečného znaku pomocí
25 znaku v předem určené vzájemné poloze se skutečným znakem, přičemž všechny znaky informace jsou známy uživateli.

- Ze spisu US 2004030892 A1 je známé grafické autentizační uživatelské rozhraní pro výpočetní zařízení, které autentizuje uživatele na základě vzájemné polohy dvou elementů. První element,
30 oblast na digitálním obrázku předem definovaná uživatelem, uživatel překryje svým autentizačním elementem vybraným ze sekundární vrstvy pravidelně rozmístěných elementů, která je zobrazena přes digitální obrázek v pozadí. P9 tedy popisuje dvě vrstvy informací, přičemž obě jsou zobrazovány uživateli a s oběma uživatel pracuje při autentizaci, přičemž jsou uživateli známy informace ve obou vrstvách, jedná se tedy i v tomto případě o odlišný způsob od
35 způsobu dle patentové přihlášky.

- Nevýhodami známých způsobů zadávání tajné informace je malá entropie zadávané tajné informace a pevné propojení zadávané tajné informace se vstupním zařízením shodné s propojením užívaným pro zadávání neutajované informace. To ve svých důsledcích vyžaduje,
40 aby si uživatel musel pamatovat dlouhé na zapamatování komplikované tajné sekvence, např. dlouhá hesla a zároveň zvyšuje šance pro útočníka, který může využít, např. kamerového záznamu pohybu prstů při zadávání tajné informace k jejímu odhalení.

45 Podstata vynálezu

- Cílem vynálezu je odstranění uvedených nevýhod a to zadávání tajné informace do elektronických zařízení novým způsobem, spočívajícím v tom, že elementy tajné informace jsou se vstupním zařízením propojeny nepřímou a to zcela odlišným způsobem než při zadávání
50 neutajované informace. Pro zadání tajné informace se použije sada dvojic elementů informace. Propojení dvojic elementů se vstupním zařízením je dynamické a může být odlišné při každém použití, přičemž propojení elementů ve dvojici je konstantní. Dvojice obsahuje vždy element multimediální informace určené k interakci s uživatelem a element tajné informace. Uživatel pomocí výběru správné sekvence elementů multimediální informace určené k interakci pomocí
55 vstupního zařízení určí sekvenci elementů tajné informace, které vytvoří zadávanou tajnou

informaci.

Podstata způsobu zadávání tajné informace uživatelem do elektronického digitálního zařízení prostřednictvím vstupně/výstupního zařízení, spočívá zejména v tom, že elektronické digitální zařízení přiřadí každému elementu tajné informace element multimediální informace určené k interakci, přičemž elektronické digitální zařízení zobrazí uživateli při zadávání informace multimediální informaci určenou k interakci obsahující elementy multimediální informace určené k interakci tak, že jejich vzájemný vztah k ovládacím prvkům elektronického digitálního zařízení je mezi jednotlivými zobrazeními proměnný, uživatel pak vybere elementy multimediální informace určené k interakci přiřazené elementům tajné informace, takže vybráním elementů multimediální informace určené k interakci uživatel vybere k nim přiřazené elementy tajné informace v daném pořadí.

Elektronickým digitálním zařízením může být například počítač, mobilní telefon, tablet, jiné komunikační elektronické digitální zařízení, atd.

Multimediální informace určená pro interakci je multimediální informace, která je pro uživatele snadno zapamatovatelná a kterou snadno rozpozná a může ji podle svých individuálních schopností a technického vybavení vstupního zařízení jednoznačně vybrat z ostatních multimediálních informací určených k interakci. Tato informace může být do elektronického zařízení vložena při jeho výrobě, dodatečně při jeho nastavování či personalizaci, může to být informace pořízená přímo uživatelem. Elementem multimediální informace určené pro interakci může být například písmeno, číslice, grafický znak, či jiný typografický znak, kresba, obrázek, videosekvence, zvuková sekvence, vibrace nebo jiný pohyb, atd.

Termín „zobrazí“, resp. „zobrazení“, znamená takovou formu interpretace informace, která odpovídá danému typu média multimediální informace, a zejména zahrnuje zobrazení grafické a vizuální informace, zobrazení (přehrání) zvukové informace, zobrazení (přehrání) videosekvence, mechanické přenesení senzorické informace (vibrace či jiný pohyb), či odpovídající interpretaci jiného typu multimediální informace vhodné pro interakci s uživateli.

Elementy tajné informace jsou zpravidla informací s vysokou entropií, kde každý element tajné informace je pevně propojen s příslušným elementem multimediální informace určené k interakci. Jde o informaci zcela odlišnou od elementu multimediální informace určené k interakci, nebo o informaci odvozenou z elementu multimediální informace určené k interakci. Elementy tajné informace nejsou pevně vestavěné při výrobě zařízení ani při instalaci programového vybavení, ale jsou vytvářeny při individuálním nastavování či personalizaci zařízení takovým způsobem, aby obsahovaly vysokou entropii informace.

V důsledku určení správné sekvence elementů informace určené k interakci uživatelem je také určena správná sekvence elementů tajné informace. Přitom uživatel pracuje s jemu známou a snadno zapamatovatelnou multimediální informací, kterou určuje při jednotlivých zadáváních většinou odlišným ovládaním vstupního zařízení.

Předkládaný vynález poskytuje zabezpečení proti prolomení tajné informace, jako je například přístupové heslo, s využitím např. kamerového záznamu sledujícího pohyb prstů při zadávání tajné informace, protože při každém zadávání je rozmístění elementů informace jiné. Dále nejsou přímo zadávány elementy tajné informace, ale jsou zadávány elementy informace určené k interakci, takže nelze prolomit heslo při přístupu z jiného přístroje, a to i když je útočníkům známo, jaká je kombinace elementů informace určené k interakci.

Objasnění výkresů

Obr. 1 ukazuje zobrazení vazeb mezi informacemi 1 určenými k interakci, elementy 2 tajné

informace, vstupním zařízením 3, ovládacím programem 4 pro zadání tajné informace a ovládacími prvky 5 vstupního zařízení 3.

5 Příklady uskutečnění vynálezu

Příklad 1

10 Způsob zadávání tajné informace do elektronických digitálních zařízení prostřednictvím běžného vstupního zařízení je založen na použití digitálních obrázků, včetně digitálních fotografií, použitých jako Elementy 1 informace určené pro interakci. Elementy 2 tajné informace mohou být odvozeny z použitých obrázků jejich náhodnou modifikací nebo mohou být vygenerovány nezávisle a propojeny pevně s Elementy 1 informace určené pro interakci.

15 Vstupní zařízení 3, pomocí kterého Uživatel 6 zadává tajnou informaci, je dotykový displej nebo počítačová myš ve spojení s klasickým displejem. Ovládací program 4 pro zadání tajné informace zobrazí na displeji náhodně uspořádané Elementy 1 informace určené pro interakci, tedy digitální obrázky a/nebo digitální fotografie, Uživatel 6 zadávající tajnou informaci vybere z této nabídky
20 příslušné Elementy 1 informace určené pro interakci v příslušném pořadí a zadá je pomocí ovládacích prvků 5 vstupního zařízení 3. Podle toho Ovládací program 4 použije ve stejném pořadí Elementy 2 tajné informace a tím vygeneruje příslušnou tajnou informaci.

Při dalším zadávání Ovládací program 4 pro zadání tajné informace zobrazí na displeji většinou
25 jinak uspořádané Elementy 1 informace určené pro interakci, tedy například stejná fotografie bude zobrazena na jiném místě displeje a Uživatel 6 musí většinou zadat jiné pozice pomocí vstupního zařízení 3, aby zadal stejné pořadí Elementů 1 informace určené pro interakci a tím určil stejnou tajnou informaci složenou z Elementů 2 tajné informace.

30 Příklad 2

Jiným příkladem provedení vynálezu je použití digitálních videosekvencí jako Elementů 1 informace určené pro interakci. V takovém případě může být jako vstupní zařízení 3 použito
35 jediné tlačítko či klávesa, tedy jediný ovládací prvek 5. Ovládací program 4 pro zadání tajné informace v náhodném pořadí přehraje jednotlivé Elementy 1 informace určené pro interakci a Uživatel 6 pomocí vstupního zařízení 3 vybere ve správném pořadí jednotlivé Elementy 1 informace určené pro interakci a na základě toho určí tajnou informaci složenou z Elementů 2 tajné informace.

40 Příklad 3

Jiným příkladem provedení vynálezu je použití zvukových nahrávek jako Elementů 1 informace určené pro interakci. V takovém případě může být jako vstupní zařízení 3 použito jediné tlačítko
45 či klávesa, tedy jediný ovládací prvek 5. Ovládací program 4 pro zadání tajné informace v náhodném pořadí přehraje jednotlivé Elementy 1 informace určené pro interakci a Uživatel 6 pomocí vstupního zařízení 3 vybere ve správném pořadí jednotlivé Elementy 1 informace určené pro interakci a na základě toho určí tajnou informaci složenou z Elementů 2 tajné informace.

Příklad 4

50 Jiným způsobem zadávání tajné informace je použití číslíc jako Elementů 1 informace určené pro interakci. Elementy 2 tajné informace mohou být odvozeny z použitých číslíc tak, že mohou být vygenerovány odvozením z těchto číslíc nebo může jít o číslíce totožné s číslíci tvořící Elementy 1 informace určené pro interakci. Elementy 1 informace určené pro interakci jsou
55 pevně propojeny s elementy 2 tajné informace.

- Vstupní zařízení 3, pomocí kterého Uživatel 6 zadává tajnou informaci, je dotykový displej. Ovládací program 4 pro zadání tajné informace zobrazí na displeji běžnou numerickou klávesnici, avšak s náhodně uspořádanými Elementy 1 informace určené pro interakci, tedy s
- 5 číslicemi v náhodném pořadí. Uživatel 6 zadávající tajnou informaci vybere na takto zobrazené numerické klávesnici příslušné číslice, tedy Elementy 1 informace určené pro interakci v příslušném pořadí a zadá je pomocí ovládacích prvků 5 vstupního zařízení 3. Podle toho ovládací program 4 použije ve stejném pořadí Elementy 2 tajné informace a tím vygeneruje příslušnou tajnou informaci.
- 10
- Při dalším zadávání ovládací program 4 pro zadání tajné informace zobrazí na displeji numerickou klávesnici s Elementy 1 informace určené pro interakci ve většinou jiném pořadí, tedy číslice budou na numerické klávesnici zobrazeny na jiném místě displeje a uživatel musí většinou zadat jiné pozice pomocí vstupního zařízení 3, aby zadal stejné pořadí Elementů 1
- 15 informace určené pro interakci a tím určil stejnou tajnou informaci z Elementů 2 tajné informace.

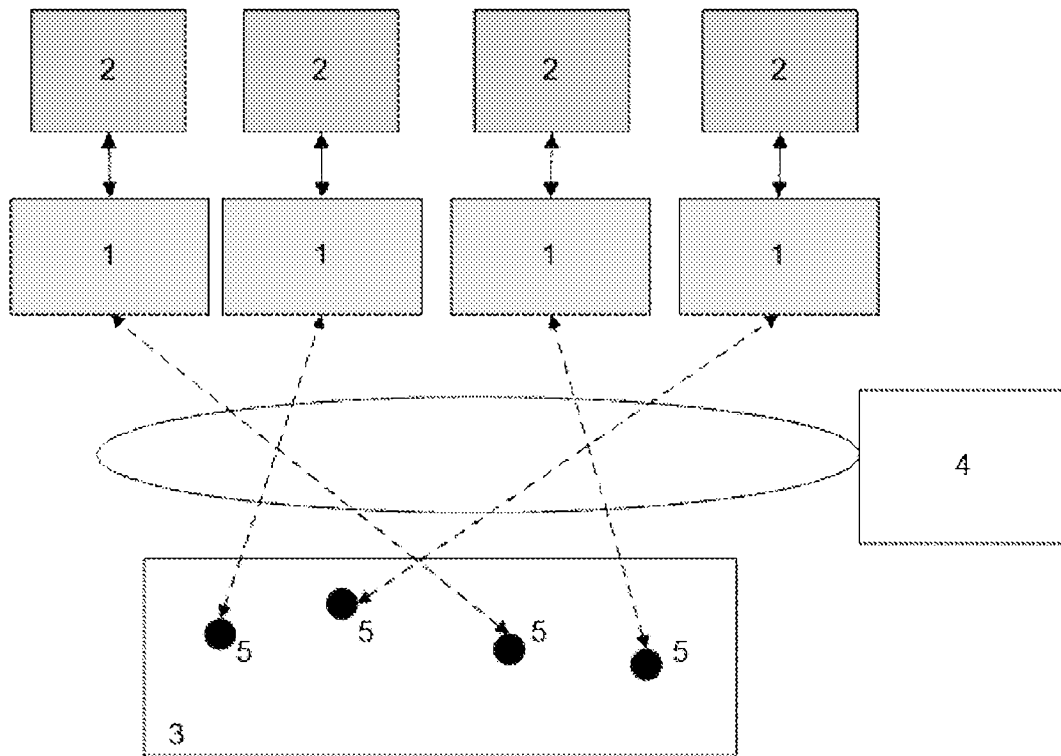
Průmyslová využitelnost

- 20 Vynález je určen všude tam, kde je potřeba zadávání a následné používání tajné informace s vysokou entropií.

PATENTOVÉ NÁROKY

1. Způsob zadávání tajné informace uživatelem do elektronického digitálního zařízení prostřednictvím vstupně-výstupního zařízení, **vyznačující se tím**, že elektronické digitální zařízení přiřadí každému elementu (2) tajné informace element (1) multimediální informace určené k interakci, přičemž elementy tajné informace se vytváří při individuálním nastavování či personalizaci zařízení a přičemž elementy (2) tajné informace jsou odlišné od elementů (1) multimediální informace určené k interakci, přičemž elektronické digitální zařízení zobrazí uživateli při zadávání informace multimediální informaci určenou k interakci obsahující elementy (1) multimediální informace určené k interakci tak, že jejich vzájemný vztah k ovládacím prvkům (5) elektronického digitálního zařízení je mezi jednotlivými zobrazeními proměnný, uživatel pak vybere elementy (1) multimediální informace určené k interakci přiřazené elementům (2) tajné informace, takže vybráním elementů (1) multimediální informace určené k interakci uživatel vybere k nim přiřazené elementy (2) tajné informace v daném pořadí.

I výkres



6

Obr. 1