

PŘIHLÁŠKA VYNÁLEZU

Zveřejněná podle §31 zákona č. 527/1990 Sb.

(21) Číslo dokumentu:

2012-719

(13) Druh dokumentu: **A3**

(51) Int. Cl.:

G06K 9/00

(2006.01)

(19)
ČESKÁ
REPUBLIKA



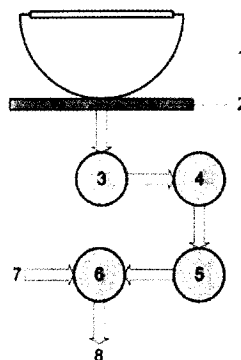
ÚŘAD
PRŮMYSLOVÉHO
VLASTNICTVÍ

(22) Přihlášeno: **23.10.2012**

(40) Datum zveřejnění přihlášky vynálezu: **21.05.2014**
(Věstník č. 21/2014)

(71) Přihlašovatel:
Vysoké učení technické v Brně, Brno, CZ

(72) Původce:
doc. Ing. Martin Drahanský, Ph.D., Brno -
Žabovřesky, CZ
Ing. Antonín Homola, Rakvice, CZ



(54) Název přihlášky vynálezu:
**Způsob detekce živosti v biometrických
systémech pomocí bezpečnostního senzoru
na základě tepové frekvence**

(57) Anotace:
Vynález se týká způsobu detekce živosti biometrických systémů pomocí bezpečnostního senzoru s výpočetním modulem zahrnujícího detekční plochu (2), na kterou se přitiskne bříško prstu (1). Na opačné straně detekční plochy (2) je proti bříšku prstu (1) umístěn optický systém (3) spojený s barevnou kamerou (4) se snímací rychlostí alespoň 20 snímků za sekundu a s čipem. Kamera (4) senzoru načítá pořízené snímky otisku bříška prstu (1) v průběhu času. Poté softwarová jednotka (5) pro zvýraznění dynamických změn v RGB barevném modelu vypočte pomocí extrakčního algoritmu průměrnou hodnotu intenzity barevné složky pro každý barevný kanál (RGB) a jasové složky všech bodů každého snímku. Následně se průměrné hodnoty intenzit jednotlivých bodů snímků v závislosti na čase vynesou do grafu a pomocí porovnávací softwarové jednotky (6) se porovnají s kontrolním grafem závislosti průměrných hodnot intenzit RGB barevného modelu na čase v databázi, které odpovídají tepové frekvenci živého člověka, nasnímané jako kontrolní pro biometrický systém. Podle předem definovaného korelačního prahu shody grafů se stanoví, zda se tedy jedná o živého člověka.

CZ 2012 - 719 A3

Způsob detekce živosti v biometrických systémech pomocí bezpečnostního senzoru na základě tepové frekvence

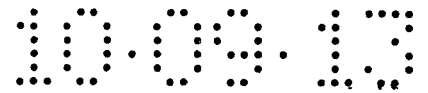
Oblast techniky

Vynález se týká způsobu detekce živosti v biometrických systémech pomocí přídatného bezpečnostního senzoru s výpočetním modulem na základě načtení snímků otisku bříška prstu v průběhu času a porovnání rozsahu závislosti průměrných hodnot intenzit barevné složky pro každý barevný kanál (RGB) a jasové složky všech bodů na čase s kontrolním rozsahem průměrných hodnot intenzit v databázi biometrického systému, které odpovídají tepové frekvenci živého člověka.

Dosavadní stav techniky

V současné době existuje celá řada bezpečnostních biometrických systémů založených na rozpoznávání vlastností otisků prstů. Přesto, že je těchto systémů spousta, jen málokteré se zabývají testováním živosti [1, 2] u právě snímaného biometrického nosiče (např. prstu). V současnosti se pro snímání otisků prstů používá několik typů senzorů [1]. Převážná většina z nich neobsahuje mechanismy testování živosti přiloženého prstu. Detekce živosti se zabývá analýzou různých vnitřních projevů lidského těla, které neovlivnitelně generuje, nebo se jedná o reakce na vnější podněty. Patří sem např. testování odporových vlastností kůže, teplotní vlastnosti, srdeční činnost, světelné vlastnosti kůže atp. Podnět (pro testování u otisků prstů) musí být vydáván v rámci snímané plochy senzoru, a ze zřejmých důvodů musí být dotekový [4, 5].

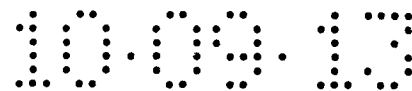
Testování živosti je doplňková funkce biometrického systému. Sama o sobě neurčuje identitu jedince, pouze podává informaci o tom, zda se u senzoru nachází živá osoba [2]. Systémy bez testování živosti je snadné oklamat přiložením uměle vyrobeného falzifikátu, některé typy umožňují dokonce reaktivaci latentního otisku prstu [1, 2, 3]. Ovlivnitelné reakce nemá prakticky smysl testovat, jedinou možností jsou tedy neovlivnitelné reakce. Testování živosti představuje doplňkovou funkci pro snímače otisků prstů [2] (příp. pro rozpoznávání geometrie ruky), na základě níž je možno rozpoznat, zda je prst živý či nikoliv. Toto testování se používá jen v málo případech, důvodem jsou především větší rozměry výsledného senzoru a samozřejmě i výrobní náklady, je však důležitou součástí biometrického bezpečnostního systému, přičemž jeho význam roste i se současným rozšířením biometrických systémů (např. biometrické osobní doklady).



Při testování živosti se doposud využívalo snímání srdeční činnosti, případně některých dalších vlastností prstu. V USA vyvinuli metodu detekce živosti založenou na rozpoznání, zda se prst potí či nikoliv. Výhodou této metody je čistě softwarová implementace, nevýhodou je však špatná práce se suchými nebo vlhkými prsty. Dále je možné využít spektrálních vlastností tkání. Na tomto principu je založena detekce živosti firmy Lumidigm (USA) [3], hardwarově implementovaná v podobě multispektrálního optického senzoru. Z principu metody vyplývá, že by se mohl objevit problém s velmi tenkým falešným otiskem prstu přilepeným na skutečný živý prst. Další možností je zjištění reakce na nějaký podnět. Detekci živosti lze také založit například na tepu a na nasycenosti krve kyslíkem. V medicíně je již vyzkoušený například princip pulzní oxymetrie. Nevýhodou je dlouhá doba měření, která činí senzor s tímto druhem detekce živosti prakticky nepoužitelným.

Reference

1. Dražanský M.: *Fingerprint Recognition Technology – Related Topics*, Saarbrücken, DE, LAP, 2011, s. 172, ISBN 978-3-8443-3007-6.
2. Dražanský M.: *Liveness Detection in Biometrics*, Advanced Biometric Technologies, Rijeka, HR, InTech, 2011, s. 179-198, ISBN 978-953-307-487-0; <http://www.intechopen.com/books/show/title/advanced-biometric-technologies>
3. URL – Lumidigm Solution; 2011; <http://www.lumidigm.com/liveness-detection/>
4. URL – BioSAL; 2011;
<http://people.clarkson.edu/projects/biosal/research/spoofingliveness.html>
5. PDF – CITeR (Liveness Detection); 2003;
http://www.biometrics.org/bc2002/2_bc0130_DerakhshabiBrief.pdf



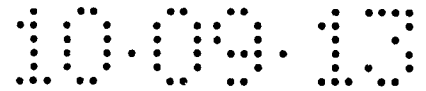
Podstata vynálezu

Nevýhody výše uvedených provedení řeší způsob detekce živosti v biometrických systémech podle vynálezu pomocí přídavného bezpečnostního senzoru s výpočetním modulem zahrnujícího detekční plochu, na kterou se přitiskne bříško prstu, přičemž na opačné straně detekční plochy je proti bříšku prstu umístěn optický systém spojený s barevnou kamerou se snímací rychlostí alespoň 20 snímků za sekundu a s čipem. Kamera senzoru načítá pořízené snímky otisku bříška prstu v průběhu času, po dobu nejméně 5 sekund, poté jednotka pro zvýraznění dynamických změn v RGB barevném modelu vypočte pomocí extrakčního algoritmu průměrnou hodnotu intenzity barevné složky pro každý barevný kanál (RGB) a jasové složky všech bodů každého snímku, následně se průměrné hodnoty intenzit jednotlivých bodů snímků v závislosti na čase vynesou do grafu a pomocí porovnávací jednotky se porovnájí s kontrolním grafem závislosti průměrných hodnot intenzit (RGB) na čase v databázi, které odpovídají tepové frekvenci živého člověka, nasnímané jako kontrolní pro biometrický systém a podle předem definovaného korelačního prahu shody grafů se stanoví, zda se jedná o živého člověka.

Výpočetní proces tedy kromě identifikace/verifikace osoby provádí analýzu tepové frekvence dle výše popsaného principu za účelem získání informace o tom, zda se jedná o živého člověka na vstupu tohoto biometrického systému.

Způsob detekce živosti u biometrických systémů podle vynálezu umožňuje při snímání bříška prstu provádět detekci živosti v reálném čase, kdy doba snímání otisků závisí na očekávané míře přesnosti měření. Jedním z kritérií živosti může být frekvence tlukotu srdce. Způsob podle vynálezu je založen na detekci změn barvy kůže způsobených vlivem tepu srdce, které je možné pozorovat po přiložení prstu na detekční plochu senzoru.

Pro zrychlení vyhodnocování není nutné analyzovat úplně každý bod snímku, je možné zvolit vhodnou matici. Záleží na grafickém rozlišení snímací kamery. Pro zrychlení je možné provádět výpočet s každým (druhým, třetím, atd.) bodem pořízeného snímku. Analýza probíhá v reálném čase. Kamera s optikou nepřetržitě snímá detekční plochu senzoru. Jakmile je na ni přiložen prst, detekuje systém tuto skutečnost a začne snímání, to znamená, že se analyzuje zaznamenávaná sekvence snímků. Z každého snímku je vybráno dostatečné množství hodnot pro barevný kanál a intenzitu a výpočetní modul, který je součástí bezpečnostního senzoru, vypočte průměrnou hodnotu. V paměti bezpečného senzoru je uložena srdeční frekvence statisticky významného počtu osob (z biometrických systémů). Vypočtené průměrné hodnoty bodů snímků se porovnájí s uloženou průměrnou kontrolní tepovou frekvencí a zjistí se, zda odečtená tepová frekvence srdce odpovídá intervalu tepu srdce člověka. Stanovení živosti záleží na nastavení prahu vzájemné shody



křivek (předem uložené z určité živého prstu s aktuální křivkou neznámého vzorku) uživatelem.

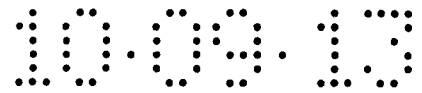
Lidský prst má červenorůžovou barvu a po přitlačení proti pevnému podkladu dochází ke změně barvy, kdy kůže zesvětlá. Tato vlastnost kůže je stejná pro celou populaci. Vlivem tepu srdce dochází v celém kardiovaskulárním systému s každým úderem srdce ke zvýšení a následnému snížení tlaku krve. Vzhledem k tomu, že dochází k barevným změnám pouze v místě přiložení prstu proti pevnému podkladu, je možné tyto vlastnosti pozorovat pouze na detekční ploše senzoru. Pokud se prst volně položí na plochu snímače a nebude na něj vyvíjen další tlak, lze pozorovat drobné barevné změny způsobené pravidelným tepem srdce. Ten způsobuje i změny tlaku na kůži v konečcích prstů, kde dochází k nejvýraznějším změnám barvy kůže. Ačkoliv jsou změny velmi malé, přesto jsou pozorovatelné. Po ustálení dochází k cyklicky se opakujícím změnám barvy kůže odpovídající tepové frekvenci srdce. Barevné změny nastávají u všech barevných složek obrazu RGB (Red-Green-Blue). Nejvýraznější jsou v oblasti zelené složky obrazu (G), zde se pohybují v řádu jednotek. Méně výrazné změny jsou pak měřitelné u červené složky (R) a nakonec i modré složky (B). Výhodou řešení podle vynálezu je využití RGB složky světla v dynamickém režimu.

Přídavný senzor bezpečnostních biometrických systémů podle vynálezu zahrnuje optický systém, který by měl dostatečně zvětšit a zaostřit středovou část bříška prstu, aby bylo možné detekovat co nejpřesněji barevné změny na povrchu kůže.

Přídavný senzor dále zahrnuje barevnou kameru s vysokým obrazovým rozlišením obsahující například čip CCD (Charge-Coupled Device), případně čip jiné technologie, RGB s odpovídající barevnou škálou a musí mít také nízkou hodnotu obrazového šumu. Kamera nepřetržitě snímá detekční plochu senzoru vyrobenou nejlépe ze skla nebo průhledného plastu a zachycuje změny barvy pokožky po přiložení prstu. Lidské srdce může bít rychlostí až 200 tepů za minutu, proto musí kamera disponovat dostatečnou snímací rychlostí (alespoň 20 snímků / s).

Vzhledem k tomu, že na detekční plochu senzoru může být vyvíjen tlak, měl by mít senzor dostatečně pevnou konstrukci pro případ, že by některý uživatel aplikoval více síly než by bylo vhodné. Zvýšení bezpečnosti odpovídá navýšení ceny senzoru.

Pro analýzu změny barvy kůže vlivem tepu srdce by stačilo zachytit pouze dva snímky, před a po úderu srdce, ale není zcela nemožné vyrobit odpovídající „dvoubarevný“ umělý prst a použít jej k oklamání senzoru. Proto je třeba zajistit, aby senzor snímal změnu barvy kůže prstu v reálném čase (živé video), aby bylo možné určit tepovou frekvenci. To vylučuje možnost pořízení snímku před a po úderu srdce.



Výsledkem analýzy je tepová frekvence. Tato tepová frekvence je následně porovnána s intervalem uložené průměrné tepové frekvence (dle nastavených mezí) pro člověka. Aby byl prst detekován jako živý, musí být analyzovaná tepová frekvence v mezích nastavené tepové frekvence člověka. Pokud se tepová frekvence nachází v předdefinovaném intervalu, je vzorek ohodnocen procentuální hodnotou, do jaké míry leží ve středu patřičného rozsahu (čím více k okraji hodnota leží, tím menší procentuální hodnoty nabývá; za hranicemi je skóre porovnání záporné), a rozhodne se (dle nastaveného prahu) o celkovém výsledku, tj. zda je biometrický nosič (např. prst či ruka) živý. V případě záporného výsledku musí uživatel přiložit biometrický nosič znovu na snímač (příp. je informována ostraha objektu o potenciálním narušiteli).

Tato metoda eliminuje použití některých materiálů pro výrobu umělých prstů oproti již známým metodám, neboť po zvýšení tlaku na prst u nich nedochází k současným odpovídajícím barevným a dilatačním změnám.

Biometrický bezpečnostní systém, který obsahuje senzor detekce živosti podle vynálezu, může být výhodně provozován v režimu bez kontroly pracovníkem (nebo s pouhým dohledem), zatímco u systému bez detekce živosti by bylo nutné použít dozoru pracovníka. U uživatelů senzoru detekce biometrických systémů podle vynálezu tedy není třeba kontrolovat, zda nepoužívá falzifikát biometrického nosiče (prstu/ruky).

Objasnění výkresů

Obr. 1: Obecné schéma základních částí senzoru bezpečnostních biometrických systémů

Obr. 2: Schéma základních částí senzoru bezpečnostních biometrických systémů s vyznačením jednotek pro zpracování a vyhodnocení měřených signálů

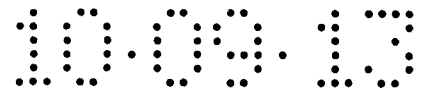
Obr. 3: Grafy analyzované tepové frekvence pro jednotlivé barevné kanály RGB a jejich součet; osa x reprezentuje čas v sekundách, osy y reprezentují hodnoty intenzity barevných kanálů.

Vynález je dále popsán pomocí příkladu, který však neomezuje rozsah provedení dle patentových nároků.

Příklad uskutečnění vynálezu

K detekci živosti biometrického systému se použil senzor bezpečnostních biometrických systémů (obr. 2) s výpočetním modulem zahrnující detekční plochu 2 ze skla, na kterou se přitisklo bříško 1 prstu. Na opačné straně detekční plochy 2 senzoru byl proti bříšku 1 prstu umístěn optický systém 3 spojený s barevnou kamerou 4 pro záznam videosignálu se snímací rychlostí 20 snímků za sekundu a s čipem. Kamera 4 senzoru načetla pořízené snímky otisku bříška 1 prstu během 15 s, přičemž softwarová jednotka 5 pro zvýraznění dynamických změn v RGB barevném modelu (obr. 3) vypočetla pomocí extrakčního algoritmu průměrnou hodnotu intenzity barevné složky pro každý barevný kanál (RGB) a jasové složky všech bodů každého snímku odpovídající tepové frekvenci biometrického systému. Průměrné hodnoty intenzit jednotlivých bodů snímků v závislosti na čase se pak vynesly do grafu a pomocí porovnávací softwarové jednotky 6 se tato data porovnala s uloženým vzorem kontrolního rozsahu průměrných hodnot intenzit odpovídajících tepové frekvenci člověka v databázi s externím vstupem 7.

Analyzovaná tepová frekvence ležela v předdefinovaném kontrolním intervalu s prahovou shodou s kontrolní křivkou v okolí 70 %, proto byl analyzovaný biometrický systém na výstupu 8 vyhodnocen jako živý.



Průmyslová využitelnost

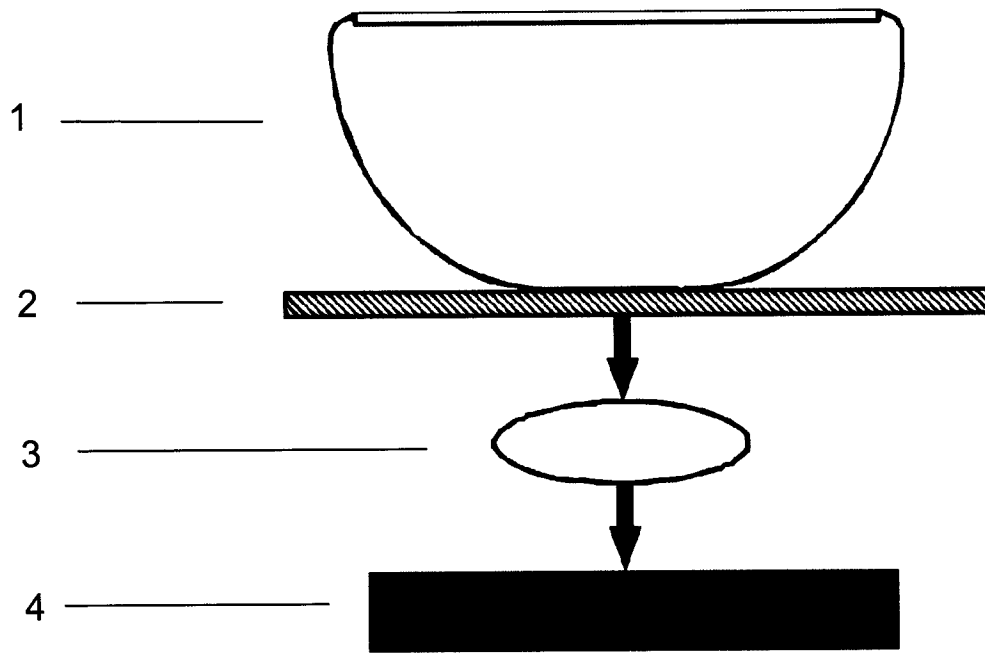
Senzor bezpečnostních biometrických systémů nalezne uplatnění ve všech oblastech využívajících bezpečnostní biometrické systémy, jako například v armádě či letištní dopravě. Přináší doplňkovou funkci pro snímače otisků prstů, případně pro rozpoznávání geometrie či jiných atributů ruky, na základě nichž je možno rozpoznat, zda je biometrický nosič živý či nikoliv. Testování živosti je proto důležitou součástí biometrického bezpečnostního systému, umožňuje rozpoznat použití uměle vyrobeného falzifikátu a není třeba osobní kontrola při detekci.

Seznam vztahových značek

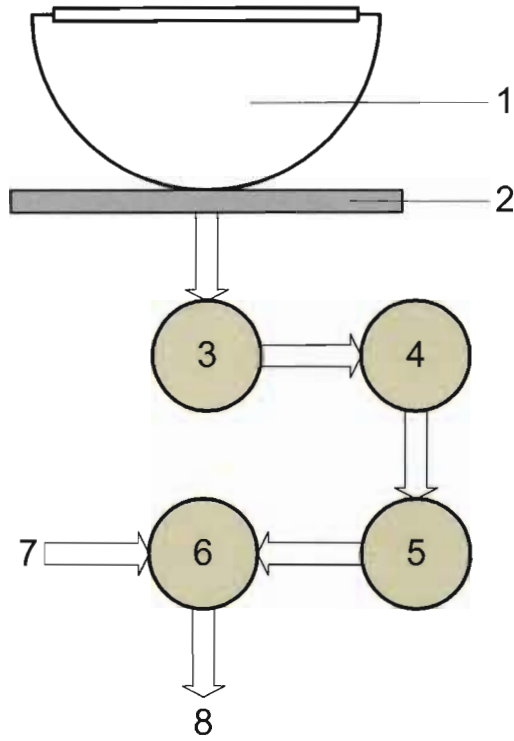
- 1 – bříško prstu
- 2 – detekční plocha senzoru
- 3 – optický systém
- 4 – barevná kamera s čipem
- 5 – softwarová jednotka pro zvýraznění dynamických změn v RGB
- 6 – porovnávací softwarová jednotka
- 7 – externí vstup kontrolního rozsahu tepové frekvence
- 8 – výstup výsledku porovnání živosti

PATENTOVÉ NÁROKY

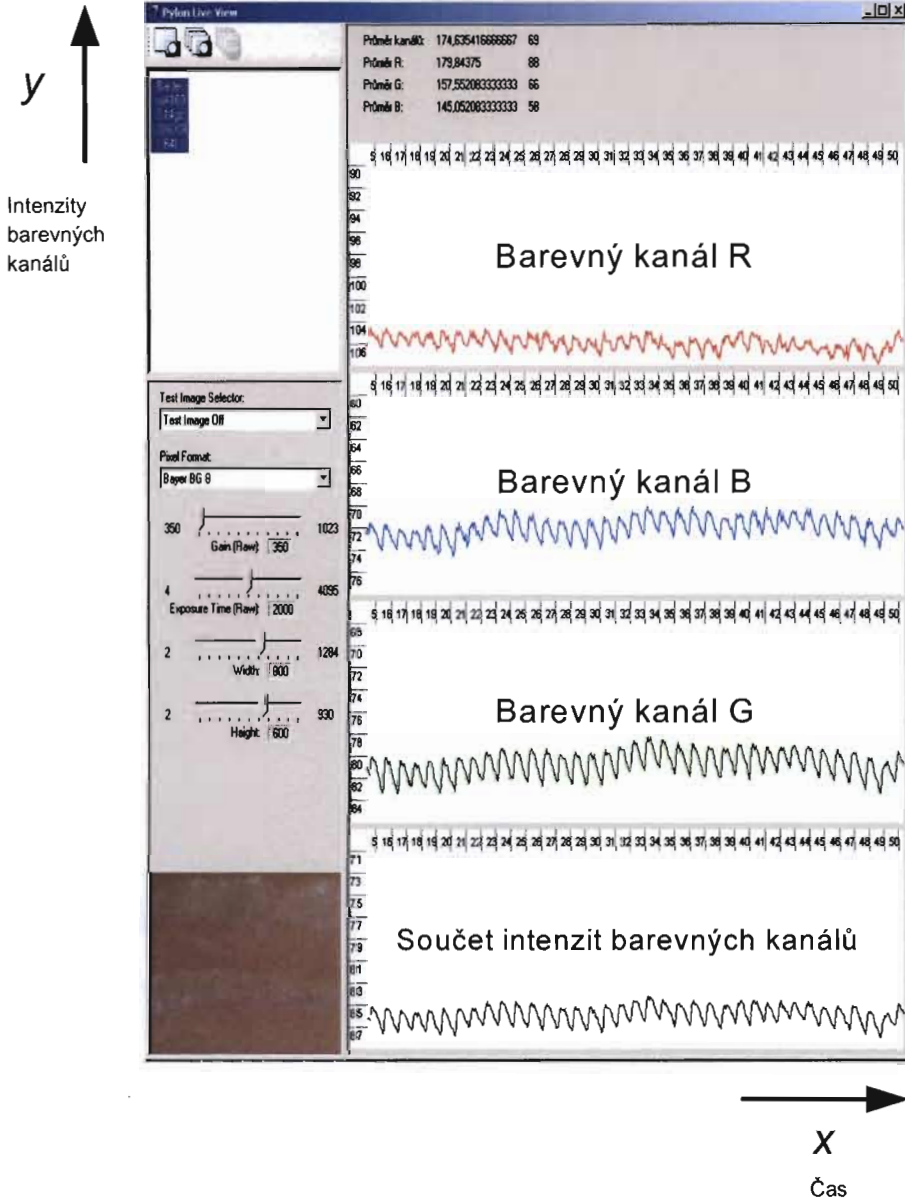
1. Způsob detekce živosti biometrických systémů pomocí bezpečnostního senzoru s výpočetním modulem zahrnujícím detekční plochu (2), na kterou se přitiskne bříško prstu (1), přičemž na opačné straně detekční plochy (2) je proti bříšku prstu (1) umístěn optický systém (3) spojený s barevnou kamerou (4) se snímací rychlostí alespoň 20 snímků za sekundu a s čipem, **vyznačující se tím**, že kamera (4) senzoru snímá pořízené snímky otisku bříška prstu (1) v průběhu času, nejméně po dobu 5 sekund a poté softwarová jednotka (5) pro zvýraznění dynamických časových změn v RGB barevném modelu vypočte pomocí extrakčního algoritmu průměrnou hodnotu intenzity barevné složky pro každý barevný kanál (RGB) a jasové složky všech bodů každého snímku, následně se průměrné hodnoty intenzit jednotlivých bodů snímku v závislosti na čase vynesou do grafu a pomocí porovnávací softwarové jednotky (6) se porovnají s kontrolním grafem závislosti průměrných hodnot intenzit v RGB barevném modelu na čase v databázi, které odpovídají tepové frekvenci živého člověka, nasnímané jako kontrolní pro biometrický systém a podle předem definovaného korelačního prahu shody grafů se stanoví, zda se jedná o živého člověka.



Obr. 1



Obr. 2



Obr. 3