Biuletyn WAT
Vol. LXII, Nr 4, 2013

Badania weryfikacyjne metody rozpoznawania twarzy

MICHAŁ WIŚNIOS, TADEUSZ DĄBROWSKI, MARCIN BEDNAREK[1]

Wojskowa Akademia Techniczna, Wydział Elektroniki,
00-908 Warszawa, ul. gen. S. Kaliskiego 2, mwisnios@wat.edu.pl,
[1]Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki,
35-959 Rzeszów, ul. Wincentego Pola 2

Streszczenie. W artykule przedstawiono wyniki badań weryfikacyjnych metody rozpoznawania twarzy. Podano tu wynikające z praktycznych testów wartości prawdopodobieństwa poprawnej identyfikacji osób poddanych badaniom na oryginalnej platformie multibiometrycznej. Metoda identyfikacji osób na podstawie obrazu twarzy jest jedną z podstawowych metod zaimplementowanych w tym multibiometrycznym systemie. Stanowi syntezę dwóch algorytmów. Pierwszy to algorytm holistyczny oparty na porównaniu całej twarzy. Natomiast drugi z algorytmów bazuje na cechach lokalnych twarzy [4, 5]. Działanie systemu rozpoznawania twarzy zostało sprawdzone eksperymentalnie na zbiorze dostępnych wzorców. Zgromadzone za pomocą technik informacyjnych dane są przechowywane w zorganizowanej do tego celu bazie danych. W ogólności badania przeprowadzone zostały na grupie 30 osób posiadających swoje szablony biometryczne w bazie danych oraz na grupie 30 osób niezarejestrowanych w bazie. Szczególnie istotnym elementem badań był proces odpowiedniego doboru warunków środowiskowych.
Słowa kluczowe: elektronika, multibiometria, biometria twarzy, wiarygodność identyfikacji

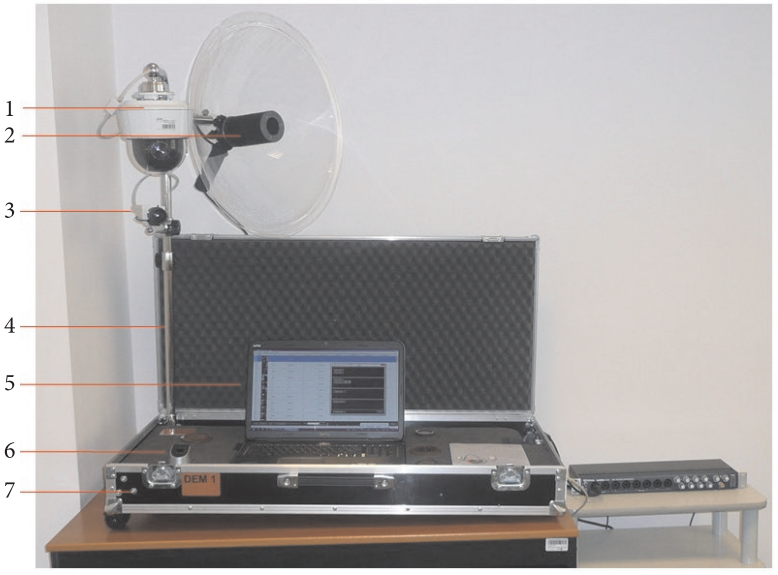
1. Wstęp

Multibiometryczny system identyfikacji osób, opracowany w Instytucie Systemów Elektronicznych Wydziału Elektroniki WAT, składa się następujących modułów: z systemu rozpoznawania na podstawie obrazu twarzy, systemu rozpoznawania na podstawie sygnału głosu, systemu identyfikacji na podstawie odcisków linii papilarnych oraz systemu identyfikacji na podstawie kodu DNA [3]. Metoda identyfikacji osób na podstawie obrazu twarzy jest jedną z podstawowych metod zaimplementowanych w tym multibiometrycznym systemie. Rysunek 1 przedstawia

widok demonstratora opracowanego systemu multibiometrycznego. Zewnętrzne konstrukcyjne elementy tego obiektu oznaczone są następującymi numerami:

1. obrotowa megapikselowa kamera IP PTZ,
2. paraboliczny mikrofon kierunkowy,
3. statyczna kamera IP,
4. maszt instalacyjny do kamer IP oraz mikrofonu,
5. zestaw komputerowy I7,
6. optyczny czytnik linii papilarnych BioMini,
7. obudowa typu „Flightcase".

Idea działania omawianego systemu zakłada, że na pierwszym etapie procesu identyfikacji powinna być realizowana analiza obrazu twarzy. Po przekroczeniu zadeklarowanego, granicznego poziomu podobieństwa osoby identyfikowanej do któregokolwiek z szablonów biometrycznych twarzy przechowywanych w bazie danych systemu, następuje proces kolejnej jej identyfikacji w oparciu o sygnał głosu. Po zastosowaniu fuzji obu tych procedur otrzymuje się poziom wiarygodności identyfikacji bliski 100%. Zdarzają się jednak przypadki, gdy wynik identyfikacji może budzić wątpliwości. Wówczas operator systemu multibiometrycznego posiada możliwość przeprowadzenia identyfikacji inwazyjnej wykorzystującej — w pierwszej kolejności — odciski palców, a w sytuacjach wyjątkowych także materiał DNA.



Rys. 1. Demonstrator systemu multibiometrycznego

2. Metoda identyfikacji osób na podstawie obrazu twarzy

Zaimplementowana metoda identyfikacji osób na podstawie obrazu twarzy jest syntezą dwóch algorytmów rozpoznawania obrazów. Algorytmy te zostały roboczo nazwane: algorytm 1 — holistyczny, algorytm 2 — lokalny.

Idea pierwszego algorytmu, tj. algorytmu opartego na cechach holistycznych, polega na porównywaniu, pobranego w procesie identyfikacji, całego wzorca z twarzy z zarejestrowanymi w bazie danych wzorcami (szablonami) [5]. Na podstawie całościowej analizy zarejestrowanego obrazu twarzy wykonywany jest proces klasyfikacji. Głównym ograniczeniem tego algorytmu jest wymóg, by bieżąca rejestracja obrazu twarzy odbywała się pod podobnym kątem, jaki był zastosowany przy tworzeniu szablonu obrazu zapisanego w bazie danych biometrycznych systemu. Natomiast zaletą algorytmu holistycznego jest stosunkowo wysoki poziom wiarygodności identyfikacji w przypadku, gdy bieżąca rejestracja obrazu twarzy odbywa się w warunkach analogicznych do tych, które występowały przy tworzeniu szablonu biometrycznego na potrzeby bazy danych.

Drugi z zaimplementowanych algorytmów oparty jest na analizie wyłącznie deskryptorów cech lokalnych [6]. Algorytm ten zakłada detekcję, na zarejestrowanym obrazie, punktów charakterystycznych, jak np. ciemniejsze punkty na jasnym tle (np. znamię — tzw. „pieprzyk"), punkty narożne, punkty układające się w charakterystyczne kształty (rozwidlenia, złączenia) itp. Algorytmy tego typu są powszechnie stosowane w systemach identyfikacji opartych na odciskach palców.

3. Sposób badań weryfikacyjnych

W celu zweryfikowania jakości działania opracowanej metody identyfikacji przeprowadzono szereg badań właściwości utworzonego systemu. Dla zapewnienia niezmiennych warunków środowiskowych badania zostały przeprowadzone w warunkach laboratoryjnych. Danych pomiarowych dostarczyła grupa 30 osób odnotowanych w bazie danych biometrycznych oraz grupa 30 osób nieodnotowanych wcześniej w tej bazie.

Powszechnie stosowaną miarą porównawczą, pozwalającą na określenie jakości działania systemu biometrycznego, jest zbiór dwóch rodzajów błędów: niesłusznej akceptacji i niesłusznego odrzucenia.

Dla osób, których szablony biometryczne znajdują się w bazie danych, wyznacza się błąd niesłusznego odrzucenia FR (ang. *False Reject*) oraz wskaźnik niesłusznych odrzuceń FRR (ang. *False Reject Rate*) [2]:

$$\mathrm{FRR} = \frac{\mathrm{FR}}{\mathrm{TA+FR}}, \tag{1}$$

gdzie TA (ang. *True Accept*) oznacza poprawną akceptację, natomiast TR (ang. *True Reject*) poprawne odrzucenie.

W przypadku osób nieodnotowanych wcześniej w bazie danych wyznacza się błąd niesłusznego potwierdzenia — FA (ang. *False Accept*) oraz wskaźnik niesłusznej akceptacji FAR (ang. *False Accept Rate*):

$$\mathrm{FAR} = \frac{\mathrm{FA}}{\mathrm{TR+FA}}. \tag{2}$$

W systemach bezpieczeństwa (np. w systemach kontroli dostępu) błędy te pociągają za sobą następujące konsekwencje: błąd FA wywołuje obniżenie zaufania do zastosowanych zabezpieczeń (może wystąpić przyznanie prawa dostępu osobie nieuprawnionej), natomiast błąd FR wywołuje obniżenie komfortu użytkowania systemu zabezpieczeń (bo może wystąpić odmowa prawa dostępu osobie uprawnionej).

Badania weryfikacyjne przeprowadzono następująco. Od każdej z testowanych osób pobrano w procesie akwizycji obraz twarzy. Został on poddany przetworzeniu — oddzielnie przez każdy z zaimplementowanych algorytmów. Następnie dokonano fuzji informacji, zawartej w obu wypracowanych wynikach rozpoznania, w celu pozyskania sumarycznego wyniku procesu identyfikacji. Istotne przy tym jest, że każdy z algorytmów identyfikacji charakteryzuje się własnym progiem odrzucenia oraz wagą określającą wypadkową wiarygodność algorytmu. Na potrzeby badań weryfikacyjnych wagi poszczególnych algorytmów zostały ustawione na równym poziomie. Zabieg taki umożliwia badanie wpływu poszczególnych algorytmów na końcowy wynik fuzji informacji biometrycznej.

Ważnym etapem badań był proces doboru właściwych warunków środowiskowych. Wiadomo, że największy wpływ na wynik procesu rozpoznania na podstawie obrazu twarzy ma oświetlenie zewnętrzne. Na podstawie wstępnie przeprowadzonych badań oraz informacji zawartej w odnośnej literaturze, określono minimalne natężenie oświetlenia w pomieszczeniu akwizycji danych biometrycznych jako 500 lx, przy czym wskazane jest, aby źródło światła oświetlało twarz z przodu. Przy zachowaniu tego wymagania nie powinno występować zagrożenie zjawiskiem powstawania cieni w oczodołach, co negatywnie wpływa na poprawność procesu identyfikacji.

4. Wyniki badań weryfikacyjnych

A. Badanie jednorazowe

Wyniki przeprowadzonych testów, na osobach **odnotowanych** wcześniej w bazie danych systemu, zawiera tabela nr 1. System zwraca wynik identyfikacji w postaci uporządkowanego zbioru do ośmiu osób, których szablony przechowywane w bazie

danych są podobne do metryki biometrycznej osoby badanej z prawdopodobieństwem przekraczającym założony próg wiarygodności.

Cyfry w tabeli 1, od 0 do 8, oznaczają pozycję rozpoznawanej osoby w zwracanym zbiorze, przy czym cyfra 0 oznacza, że identyfikowana osoba nie znalazła się wśród osób wskazanych przez system, tj. nie została zidentyfikowana z wystarczająco wysokim prawdopodobieństwem.

Na podstawie przeprowadzonych badań można stwierdzić, że we wszystkich przypadkach osoba aktualnie identyfikowana znajduje się w „na liście rankingowej" procesu identyfikacji. Wskazanie osoby identyfikowanej na którymkolwiek z kolejnych miejsc listy rankingowej ma sens, zwłaszcza w przypadku gdy identyfikacja może być (lub musi być) oparta na badaniu także innych cech biometrycznych lub proces badania w oparciu o tę samą biometrykę może być wielokrotnie powtórzony. Opisywane badania skoncentrowane były wyłącznie na przypadkach, gdy identyfikowana osoba jest wskazywana na pierwszym miejscu. W tabeli nr 1 błąd FR określony został zapisem „zero/miejsce na liście rankingowej", natomiast poprawna akceptacja — TA oznaczona została cyfrą 1. W omawianym przypadku wartość współczynnika FRR wyniosła **0,03**.

Dodatkowo w tabeli umieszczono kolumnę zawierającą informację o płci identyfikowanej osoby. Wykonane badania sprzyjają twierdzeniu, że płeć nie ma wpływu na błędy procesu identyfikacji biometrycznej na podstawie obrazu twarzy.

Tabela 1

Wyniki identyfikacji osób zarejestrowanych w bazie danych biometrycznych

Lp.	Płeć	Pozycja na liście rankingowej	Podobieństwo Alg. Tw. 1	Podobieństwo Alg. Tw. 2	Podobieństwo sumaryczne
1	m	1	14,50	29,10	21,80
2	m	1	17,20	19,80	18,50
3	m	1	12,79	34,01	23,40
4	m	1	8,26	36,06	22,16
5	m	1	21,42	46,76	34,09
6	m	1	5,17	11,53	8,35
7	m	1	16,95	34,75	25,85
8	m	1	2,93	29,65	16,29
9	m	0/2	4,43	8,33	6,38
10	m	1	10,05	20,31	15,18
11	m	1	5,57	18,33	11,95
12	k	1	16,10	24,56	20,33

cd. tabeli 1

13	m	1	24,97	41,43	33,20
14	m	1	8,88	24,58	16,73
15	k	1	7,61	4,95	6,28
16	m	1	11,04	37,30	24,17
17	m	1	2,73	17,97	10,35
18	m	1	20,27	45,83	33,05
19	k	1	15,12	3,56	9,34
20	m	1	47,00	0,00	23,50
21	k	1	4,24	33,60	18,92
22	k	1	15,79	20,89	18,34
23	m	1	5,96	11,11	8,53
24	m	1	12,8	15,94	14,37
25	m	1	15,03	24,5	19,84
26	m	1	6,84	33,1	19,97
27	m	1	3,86	26,32	15,08
28	k	1	18,71	28,13	23,42
29	k	1	20,76	36,92	28,84
30	k	1	22,45	34,75	28,59

Wyniki procesu identyfikacji przeprowadzonej na grupie osób **nienotowanych** wcześniej w bazie danych biometrycznych zostały przedstawione w tabeli nr 2. Błąd FA określony został tu cyfrą „0", natomiast poprawne odrzucenie TR oznaczono cyfrą „1". W omawianym przypadku wartość wskaźnika błędu FAR wynosi **0,43**. Wartość ta świadczy o tym, że przy zadeklarowaniu niskiego progu odrzucenia w poszczególnych algorytmach identyfikacji system będzie generował znaczącą liczbę fałszywych alarmów.

W celu określenia współczynników podobieństwa osób nienotowanych w bazie danych do osób odnotowanych w bazie ustawiono progi decyzyjne poszczególnych algorytmów na najniższe wartości. Wartości wag poszczególnych algorytmów utrzymano na tym samym poziomie jak w poprzednim badaniu. W rezultacie takiego postępowania uzyskano informację o pożądanych wartościach progów pomiarowych, gwarantujących zmniejszenie wskaźnika fałszywych alarmów do poziomu akceptowalnego. I tak: dla algorytmu identyfikacji „Alg. Tw. 1" próg ten powinien mieć wartość 7,5, a dla algorytmu „Alg. Tw. 2" wartość 12. W takim przypadku możliwe jest uzyskanie współczynnika FAR na poziomie poniżej **0,01**.

Tabela 2

Wyniki procesu identyfikacji osób nienotowanych w bazie danych biometrycznych

Lp.	Płeć	0-FA 1-TR	Podobieństwo Alg. Tw. 1	Podobieństwo Alg. Tw. 2	Podobieństwo sumaryczne „zwycięzcy" Alg. Tw.
1	m	1	0	0	0,00
2	m	0	0	8,33	4,17
3	m	1	0	0	0,00
4	k	0	8,78	3,89	6,34
5	m	0	10,39	0	5,20
6	m	0	6,88	8,59	7,74
7	k	1	0	0	0,00
8	k	0	6,22	3,28	4,75
9	m	1	0	0	0,00
10	m	0	7,3	2,7	5,00
11	k	1	0	0	0,00
12	m	1	0	0	0,00
13	m	0	5,16	3,13	4,15
14	m	0	5,97	9,43	7,70
15	m	1	0	0	0,00
16	m	0	5,8	8,92	7,36
17	m	0	7,15	3,03	5,09
18	m	1	0	0	0,00
19	k	1	0	0	0,00
20	m	1	0	0	0,00
21	m	1	0	0	0,00
22	m	0	9,66	2,94	6,30
23	m	1	0	0	0,00
24	m	0	5,33	12,86	9,10
25	m	1	0	0	0,00
26	m	1	0	0	0,00
27	m	1	0	0	0,00
28	m	0	0	7,93	3,97
29	k	1	0	0	0,00
30	k	1	0	0	0,00

B. Badanie wielokrotne

Badaniami objęto 100 osób notowanych w bazie danych biometrycznych. Wagi poszczególnych algorytmów ustawiono na równym poziomie. Zdjęcia identyfikowanych osób pochodziły sprzed 6 miesięcy. Obrazy dodawane były do bazy przy użyciu standardowej kamery USB HD, natomiast akwizycję obrazów twarzy w czasie aktualnych badań przeprowadzono za pomocą megapikselowej kamery IP. Badanie polegało na 30-krotnym przeprowadzeniu procesu identyfikacji tej samej osoby poprzez jej wejście w pole widzenia kamery rejestrującej. Miało ono na celu określenie powtarzalności działania algorytmu.

Tabela 3

Wyniki 30-krotnej identyfikacji osoby zarejestrowanej w bazie danych

Lp.	Rozpoznanie (0/1)	Pozycja na liście rankingowej	Podobieństwo sumaryczne — pierwszego rozpoznanego	Podobieństwo sumaryczne — prawidłowo rozpoznanego	Podobieństwo alg. 1 — pierwszego rozpoznanego	Podobieństwo alg. 1 — prawidłowo rozpoznanego	Podobieństwo alg. 2 — pierwszego rozpoznanego	Podobieństwo alg. 2 — prawidłowo rozpoznanego
1	1	1	46,3		24,4		21,9	
2	1	1	49,41		8,9		40,5	
3	1	1	42,6		8,5		34,1	
4	1	1	57,2		23,5		33,7	
5	0/1	4	37,8	9,6	28,2	0,0	9,6	9,6
6	1	1	49,3		9,7		39,6	
7	1	1	44,5		12,0		32,5	
8	1	1	62		12,0		50,0	
9	0	–	22	0,0	22,0	0,0	0,0	
10	1	1	50,5		9,5		41,0	
11	1	1	54,5		19,1		35,4	
12	1	1	60		24,0		36,0	
13	0/1	2	34,5	14,9	34,5	0,0	0,0	14,9
14	0/1	3	23,3	17,1	8,7	0,0	14,6	17,1
15	1	1	52,3		15,3		37,0	
16	1	1	22,9		9,7		13,2	

cd. tabeli 3

17	0	–	23,5	0,0	23,5	0,0	0,0	
18	1	1	40,2		9,0		31,2	
19	1	1	70,3		43,0		27,3	
20	1	1	64,9		30,8		34,1	
21	1	1	68,6		18,1		50,5	
22	0/1	2	30,3	25,9	18,5	0,0	11,8	25,9
23	1	1	55,7		13,4		42,3	
24	1	1	45,5		12,1		33,4	
25	1	1	98		36,4		61,6	
26	1	1	52,1		20,0		32,1	
27	1	1	48,6		10,1		38,5	
28	1	1	72,2		27,3		44,9	
29	1	1	65,6		21,2		44,4	
30	0	–	21,4	0,0	21,4	0,0	0,0	0,0

Uzyskane wyniki wskazują, że jeśli za kryterium rozpoznania przyjmie się zdarzenie polegające na znalezieniu się identyfikowanej osoby na pierwszym miejscu listy rankingowej, to wówczas błąd systemu wynosi **23,3%**. Natomiast gdy jako wynik satysfakcjonujący przyjmie się fakt, że osoba identyfikowana jest wymieniona na liście rankingowej osób „wysoce podobnych", wówczas błąd systemu wynosi **10%**. Z punktu widzenia całego systemu multibiometrycznego obydwa te wyniki są satysfakcjonujące, gdyż po zastosowaniu fuzji wielu takich klasyfikatorów błędy identyfikacji lawinowo maleją praktycznie do 0. Dodatkowo zaobserwować możemy, iż we wszystkich przypadkach, gdy identyfikowana osoba jest wskazana na miejscu innym niż pierwsze, różnice pomiędzy podobieństwem do niej a do „zwycięzcy identyfikacji" są stosunkowo niewielkie. Natomiast gdy identyfikowana osoba rozpoznana jest prawidłowo, jej podobieństwo do następnej osoby na liście rankingowej jest istotnie, bo nawet kilkukrotnie niższe.

Na podstawie przeprowadzonych badań możemy również stwierdzić, iż zastosowanie innego typu kamery (m.in. posiadającej odmienną charakterystykę przetwarzania detektora CCD i CMOS) nie ma znaczącego wpływu, na jakość działania systemu identyfikacji. Dzieje się tak za sprawą wstępnego procesu przetwarzania obrazu twarzy, w którym obraz ten jest redukowany do skali szarości.

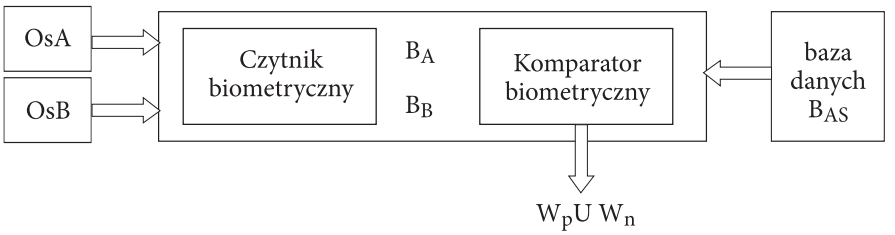
5. Ocena wiarygodności identyfikacji multibiometrycznej [1]

W celu wyznaczenia wartości wiarygodności, tj. prawdopodobieństwa prawdziwości wyniku procesu identyfikacji multibiometrycznej, przeprowadzono badania, zakładając, co następuje:

— procedura rozpoznawania obrazu realizowana jest dwutorowo, tj. zgodnie z algorytmem holistycznym oraz z algorytmem lokalnym;
— zbiór osób poddanych badaniom identyfikacyjnym składa się z osób posiadających swoje szablony biometryczne w bazie danych systemu (osoby **OsA**) oraz z osób nieposiadających takich szablonów (osoby **OsB**);
— liczności zbiorów OsA i OsB są porównywalne i wystarczająco duże;
— multibiometryczność identyfikacji obrazu twarzy polega (poza zastosowaniem dwu algorytmów identyfikacji) także na działaniu obejmującym np.:
  a) co najmniej dwukrotne powtórzenie procedury identyfikacji opartej na tej samej biometryce (np. obraz twarzy pobrany z odległości 2 i 3 metrów),
  b) zrealizowanie procedury identyfikacji opartej na dwu biometrykach tego samego obrazu twarzy (np. obrazu pobranego w świetle widzialnym i w podczerwieni),
  c) zrealizowanie procedury identyfikacji opartej na dwu obrazach twarzy pobranych pod różnym kątem.

Analiza wyników badania wiarygodności została przeprowadzona przy założeniu następujących oznaczeń i zależności:

1. Próbka biometryczna osoby OsA: $\mathbf{B_A}$; szablon biometryczny osoby OsA: $\mathbf{B_{AS}}$; próbka biometryczna osoby OsB: $\mathbf{B_B}$;
2. Wyniki poszczególnych komparacji są niezależne;
3. Możliwe są wyłącznie następujące wyniki komparacji (rys. 2):
   — wynik pozytywny oznaczający akceptację twierdzenia, że porównywana próbka i szablon są identyczne: **Wp**,
   — wynik negatywny oznaczający odrzucenie twierdzenia, że porównywana próbka i szablon są identyczne: **Wn**;



Rys. 2. Ilustracja procedury rozważanej identyfikacji

4. Każdy wynik komparacji może być prawdziwy lub fałszywy z określonym prawdopodobieństwem:
   - — prawdopodobieństwo prawidłowej akceptacji: $\mathbf{P_{p+}}(TA)$,
   - — prawdopodobieństwo nieprawidłowej (fałszywej) akceptacji: $\mathbf{P_{n+}}(FA)$,
   - — prawdopodobieństwo prawidłowego odrzucenia: $\mathbf{P_{p-}}(TR)$,
   - — prawdopodobieństwo nieprawidłowego (fałszywego) odrzucenia: $\mathbf{P_{n-}}(FR)$;
5. Prawdopodobieństwa możliwych wyników porównania biometryk:

$$\mathbf{B_A : B_{AS}}\ P_{p+} + P_{n-} = 1,$$

$$\mathbf{B_B : B_{AS}}\ P_{p-} + P_{n+} = 1,$$

a zatem: $P_{p+} = 1 - P_{n-}P_{p-} = 1 - P_{n+}$;

6. Unormowana wiarygodność jednokrotnego procesu komparacji:

$$W^1_{(B)} = \frac{P_T}{P_T + P_F}, \tag{3}$$

gdzie:

$\mathbf{P_T}$ — wskaźnik prawidłowego wyniku procesu identyfikacji (**prawdy**):

$$\mathbf{P_T} = P_{p+} + P_{p-},$$

$\mathbf{P_F}$ — wskaźnik nieprawidłowego wyniku procesu identyfikacji (**fałszu**):

$$\mathbf{P_F} = P_{n+} + P_{n-};$$

7. Unormowana wiarygodność n-krotnego procesu komparacji:

$$W^n_{(B)} = \frac{\prod_{i=1}^{n} P_{Ti}}{\prod_{i=1}^{n} P_{Ti} + \prod_{i=1}^{n} P_{Fi}}, \tag{4}$$

gdzie:

$\mathbf{P_{Ti}}$ — wskaźnik prawidłowego i-tego wyniku procesu identyfikacji (prawdy):

$$\mathbf{P_{Ti}} = P_{pi+} + P_{pi-},$$

$\mathbf{P_{Fi}}$ — wskaźnik nieprawidłowego *i*-tego wyniku procesu identyfikacji (fałszu):

$$\mathbf{P_{Fi}} = P_{ni+} + P_{ni-}.$$

Uzyskane wyniki

1) Wiarygodność identyfikacji obrazu twarzy przy zastosowaniu fuzji wyników algorytmu 1 (holistycznego) oraz algorytmu 2 (lokalnego) w badaniu jednokrotnym:

$$W^1_{(\text{t alg. 1 i 2})} = \mathbf{0{,}77},$$

2) Wiarygodność identyfikacji obrazu twarzy przy zastosowaniu fuzji wyników algorytmu 1 (holistycznego) oraz algorytmu 2 (lokalnego) w badaniu dwukrotnym zrealizowanym w identycznych warunkach:

$$W^2_{(\text{t alg. 1 i 2})} = \mathbf{0{,}92}.$$

6. Podsumowanie

Przeprowadzone badania i analiza wyników wskazują na to, że:

1. Jednokrotne pobranie próbki biometrycznej i jednokrotna komparacja tej próbki z szablonem przechowywanym w bazie danych biometrycznych nie daje zadowalająco wiarygodnego wyniku identyfikacji.
2. Wiarygodność identyfikacji można znacząco poprawić, stosując:
   — wielokrotne badanie oparte na tym samym rodzaju cechy biometrycznej,
   — wielokrotne badanie oparte na różnych rodzajach cech biometrycznych.
3. Wiarygodność wyniku procesu identyfikacji zależy nie tylko od krotności badania biometrycznego, lecz także m.in. od:
   — efektywności algorytmów tworzenia szablonów biometrycznych,
   — warunków realizacji akwizycji obrazu,
   — poziomu zakłóceń działających na system identyfikacji biometrycznej.

Każde z wymienionych zagadnień wymaga oddzielnej analizy i stosownych przedsięwzięć.

LITERATURA

[1] T. Dąbrowski, M. Bednarek, M, Wiśnios, *Analiza wiarygodności identyfikacji multibiometrycznej*, XLI Zimowa Szkoła Niezawodności, Szczyrk 6-12 stycznia 2013.

[2] R.M. Bolle, J.H. Connell, S. Panakanti, N.K. Ratha, Andrew W. Senior, *Biometria*, WNT, Warszawa, 2008.

[3] Sprawozdanie merytoryczne z realizacji projektu rozwojowego PBR 574/2010 „Multibiometryczny system identyfikacji osób do przeciwdziałania zagrożeniom terrorystycznym", WAT, 2012.

[4] J. Jakubowski, *An assessment of the local descriptors of images for the needs of face recognition system*, Przegląd Elektrotechniczny, 88, 9a, 2012, 217-221.

[5] S. Osowski, K. Sikorska-Łukasiewicz, *PCA transformation and Support Vector Machine for recognition of the noisy images*, Przegląd Elektrotechniczny, 88, 3a, 2012, 4-6.

[6] J. Pacan, J. Jakubowski, M. Wiśnios, *Zastosowanie transformacji SIFT w identyfikacji na podstawie obrazów termalnych twarzy*, Technika Transportu Szynowego, 9, 2012, 1899-1908.

M. WIŚNIOS, T. DĄBROWSKI, M. BEDNAREK

Verification tests of face recognition method

Abstract. This paper presents the results of verification of face recognition method. Due to practical tests, probability values of the correct identification of persons evaluated for the original multi-biometric platform are given. People identification method based on facial image is one of the basic methods implemented in the multibiometric system. Figure 1 shows a developed view of the multibiometric system demonstrator. Implemented in multibiometric system, identification method, based on the image of the face, is a synthesis of two algorithms. The first algorithm is an algorithm based on a comparison of holistic whole face. The second of algorithms is based on local features of the face [4, 5].
Face recognition system performance has been tested experimentally on a set of available patterns. The data accumulated using information technology will be stored in a database organized for this purpose. In general, the tests were carried out on a group of 30 people, who have their biometric templates in the database and on a group of 30 people that was not registered in the database. A particularly important element of the study was the process of selection of suitable environmental conditions.
Keywords: electronic, multi-biometric, facial biometric, reliability of identification