ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2013
Seria: ORGANIZACJA I ZARZĄDZANIE z. 64 Nr kol. 1894

Ireneusz J. JÓŹWIAK
Michał SZCZEPANIK
Politechnika Wrocławska
Instytut Informatyki

WYDAJNOŚĆ I NIEZAWODNOŚĆ WIELOMODUŁOWYCH SYSTEMÓW BIOMETRYCZNYCH

Streszczenie. W artykule opracowano metodologię szacowania niezawodności w wielomodułowych systemach biometrycznych. Analizie poddano zarówno jednomodułowe systemy z wieloma klasyfikatorami, jak i wielomodułowe systemy biometryczne. Proponowane rozwiązania umożliwią opracowanie algorytmu decyzyjnego, bazującego na wielu klasyfikatorach analizujących jedną lub kilka cech biometrycznych. Opracowano algorytm wyliczający prawdopodobieństwo błędu badanego systemu weryfikacji biometrycznej.

PERFORMANCE AND RELIABILITY OF MULTIMODAL BIOMETRIC SYSTEMS

Summary. A methodology for assessing the reliability in multi-modular biometric systems has been elaborated in this thesis. Single-module systems with multiple classifiers, as well as multi-modular biometric systems were analyzed. Suggested solutions will allow an elaboration of a decision algorithm basing on multiple classifiers that analyze one or more biometric features. An algorithm calculating the probability of an error in the biometric verification in the analyzed system has been presented.

1. Wprowadzenie

Systemy biometryczne do autentykacji lub identyfikacji wykorzystują cechy fizyczne [4] oraz cechy behawioralne. Do cech fizycznych zalicza się: strukturę tęczówki oka, układ linii papilarnych, układ naczyń krwionośnych, kształt twarzy, rozkład temperatur na twarzy, kształt i rozmieszczenie zębów oraz kod DNA. Do cech behawioralnych [1] zaliczamy te,

które są związane z zachowaniem, czyli, sposób chodzenia, podpis odręczny, sposób pisania na klawiaturze komputera.

Większość cech biometrycznych jest indywidualna i uznawana za niezmienna. Niestety, takie twierdzenie jest nieprawdziwe. Prawdopodobieństwo wystąpienia osób z identycznym rozkładem linii papilarnych wynosi $4*10^{-7}$ [15, 16], gdyż rozkład ten nie zależy tylko od genów, ale także od stopnia ukrwienia płodu podczas okresu wykształcania się linii papilarnych, dlatego nawet bliźniaki nie mają identycznych linii papilarnych [6, 7, 8]. Niezmienność zależy głownie od uszkodzeń linii papilarnych, gdyż rany oraz blizny mogą okresowo zaburzyć ich układ [18]. Cechy behawioralne [5] uzależnione są od stopnia zmęczenia organizmu, ewentualnie stopnia świadomości, spowodowanego zażywaniem leków lub innych środków odurzających. W przypadku tęczówki oka, która była uznawana za jedną z bezpieczniejszych cech biometrycznych, zespół naukowców z University of Notre Dame pod kierownictwem prof. Kevina Bowyera wykazał, że jest ona wrażliwa na procesy starzenia [14]. Powoduje to, że z czasem systemy do jej rozpoznawania będą w przypadku tej samej osoby generować coraz więcej błędów.

Każdy algorytm bądź system biometryczny można ocenić pod względem użyteczności oraz bezpieczeństwa [3, 9]. Bezpieczeństwo określone jest przez parametr FAR (ang. *False Acceptance Rate*). Jest to prawdopodobieństwo zakwalifikowania wzorca do danej klasy, mimo iż przynależy on do innej. W systemach biometrycznych jest to prawdopodobieństwo przyznania dostępu do systemu, mimo braku stosowanych uprawnień. Użyteczność określa parametr FRR (ang. *False Rejection Rate*). Jest to prawdopodobieństwo niezakwalifikowania wzorca do danej klasy, mimo iż do niej należy. W systemach biometrycznych jest to prawdopodobieństwo nieprzyznania dostępu do systemu, mimo posiadania uprawnień. Tabela 1 prezentuje skuteczność popularnych systemów biometrycznych. Na jej podstawie można zauważyć, że najbezpieczniejszą metodą identyfikacji jest ta, która bazuje na siatkówce oka. Jednak jest ona mało użyteczna.

Tabela 1

Porównanie popularnych metod biometrycznych
Comparison of popular biometric methods

	FRR	FAR
Linie papilarne	0,2000%	0,0100%
Geometria dłoni	0,2000%	0,2000%
Siatkówka oka	10,0000%	0,0010%
Tęczówka oka	0,0005%	0,0050%
Geometria twarzy	1,0000%	0,5000%

Źródło: [2]

Nieskuteczność niektórych metod biometrycznych przyczynia się do wzrostu popularności wielomodułowych systemów biometrycznych [14], które wykorzystują kilka systemów biometrycznych jedocześnie, znacznie zwiększając prawdopodobieństwo prawidłowej autentykacji bądź identyfikacji w systemie. Analizowanie dwóch cech

biometrycznych przez system biometryczny umożliwia działanie systemy nawet, gdy jedna z analizowanych cech jest uszkodzona.

2. Wielomodułowe systemy biometryczne

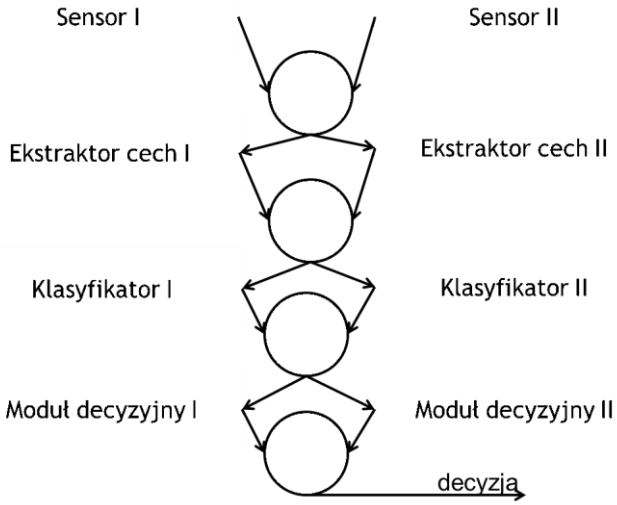
Wielomodułowe systemy biometryczne są nazywane też wieloklasowymi (ang. *multiple classifier*) lub wielomodalnymi (ang. *multimodal*). Wielomodułowe systemy biometryczne wykorzystują dane z jednego lub wielu czujników pomiarowych dla jedej lub wielu różnych cech biometrycznych. Przykładem takiego systemu jest system biometryczny, bazujący na odciskach palców oraz rozkładzie żył [10, 11, 12] lub system rozpoznawania twarzy na podstawie dwóch algorytmów. Ross [13, 14] rozróżnił trzy typy wielomodułowych systemów biometrycznych, bazujących na jednej cesze biometrycznej, ze względu na poziom fuzji:

- wieloalgorytmowy system biometryczny,
- wielosensorowy system biometryczny,
- system hybrydowy.

Dla wielu cech rozróżnił dwa główne typy:

- system z wieloma dedykowanymi sensorami,
- system z jednym sensorem, rozpoznającym wiele cech.

Na podstawie tych podziałów widać wyraźnie, że połączenie systemów biometrycznych może być zrealizowane przez różne moduły (rys. 1), czyli moduł sensora, moduł ekstraktora cech, moduł klasyfikatora oraz moduł decyzyjny.



Rys. 1. Fuzja w wielomodułowych systemach biometrycznych [źródło: opracowanie własne]
Fig. 1. Fusion in multimodal biometrics systems

3. Podejmowanie decyzji w wielomodułowych systemach

Wielomodułowe systemy biometryczne rozróżnia się także ze względu na sposób działania systemu decyzyjnego. Wyróżnia się kilka systemów decyzyjnych ze względu na zależności miedzy modułami:

- system z wagami,
- system z głównym decydentem.

System z wagami podejmuje decyzje na podstawie wyników kilku pojedynczych modułów decyzyjnych, z których każdy należy do określonego modułu biometrycznego. Każdy wynik jest wyrażony w wartości procentowej, określającej stopień zgodności badanej cechy biometrycznej ze wzorcem. Do każdego wyniku przypisana jest także waga danego modułu w ostatecznej decyzji. W przypadku systemu z dwoma modułami, system z wagami opisany jest wzorem (1):

$$d=p_A w_A+p_B w_{B,} \tag{1}$$

gdzie:

p_A- stopień zgodności cechy z oryginałem dla modułu A: <0,1>,

p_B- stopień zgodności cechy z oryginałem dla modułu B: <0,1>,

w_A- waga modułu A: <0,1>,

w_B- waga modułu B: <0,1>.

System z głównym decydentem stosowany jest, gdy jeden lub kilka modułów (w przypadku określonej wartości decyzji) podejmuje decyzje za cały system, bez względu na decyzje pozostałych modułów. Ma on zastosowanie, gdy jeden z modułów ma pomijalny (można uznać, że system jest nieomylny) jeden ze współczynników oceny FAR lub FRR w porównaniu do pozostałych. Reprezentacje tego typu systemu przedstawia tabela 2. W tym przypadku moduł 1 podejmuje za cały system decyzje odrzucenia, nawet w sytuacji, gdy pozostałe dwa systemy zaakceptowały potencjalnego intruza.

Tabela 2

Tabela decyzyjna dla systemu z jednym decydentem
Decision table for a system with a single decision maker

Moduł 1	**Moduł 2**	**Moduł 3**	**Decyzja**
Zaakceptowano	Zaakceptowano	Zaakceptowano	Zaakceptowano
Zaakceptowano	Zaakceptowano	Odrzucono	Zaakceptowano
Zaakceptowano	Odrzucono	Zaakceptowano	Zaakceptowano
Odrzucono	Zaakceptowano	Zaakceptowano	Odrzucono

cd. tabeli 2

Zaakceptowano	Odrzucono	Odrzucono	Odrzucono
Odrzucono	Zaakceptowano	Odrzucono	Odrzucono
Odrzucono	Odrzucono	Zaakceptowano	Odrzucono
Odrzucono	Odrzucono	Odrzucono	Odrzucono

Źródło: opracowanie własne

4. Niezawodność wielomodułowych systemów biometrycznych

Przez niezawodność systemu biometrycznego rozumiemy prawdopodobieństwo jego poprawnego działania przez czas co najmniej t, w określonych warunkach. Oznacza to, że z wyznaczonym prawdopodobieństwem, w określonym czasie t system będzie poprawianie identyfikował bądź odrzucał użytkownika.

Niezawodność każdego systemu biometrycznego można określić na podstawie niezawodności sensora oraz algorytmów przetwarzających i rozpoznających cechy biometryczne. Na niezawodność sensora mają wpływ trzy podstawowe zdarzenia:

- fizycznej awarii sensora (Z_A),
- uszkodzenia cechy biometrycznej (Z_{UC}),
- złego odczytu cechy biometrycznej, np. wskutek zabrudzeń (Z_{BO}).

Zdarzenie awarii sensora można wyrazić wzorem (2):

$$Z_{AS}=Z_A \cup Z_{UC} \cup Z_{BO}\,. \tag{2}$$

Na nieprawidłową decyzję, podjętą w wyniku działania algorytmu mają wpływ następujące zdarzenia:

- błędu algorytmu filtracji/korekcji szumów (Z_{AF}),
- błędu klasyfikatora (Z_{AP}),
- błędu algorytmu decyzyjnego (Z_{AD}).

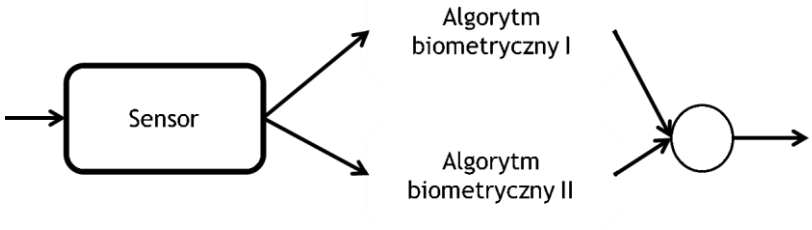
Zdarzenie błędu algorytmu można wyrazić wzorem (3):

$$Z_{BA}=Z_{AF} \cup Z_{AP} \cup Z_{AD} \tag{3}$$

Na podstawie tych zdarzeń można opracować model niezawodności dla każdego typu wielomodułowego systemu biometrycznego.

4.1. Niezawodność wieloalgorytmowego systemu biometrycznego

Wieloalgorytmowy system biometryczny (rys. 2) wykorzystuje jeden sensor do zebrania danych o cesze, a następnie te dane są przetwarzane przez dwa niezależne algorytmy. W przypadku algorytmów rozpoznawania odcisków palców mogą to być np. algorytm bazujący na wzorcach (*ang. Pattern-Based Templates*) oraz elastycznego dopasowania minucji (*ang. Elastic minutiae matching*).



Rys. 2. Schemat wieloalgorytmowego systemu biometrycznego [źródło: opracowanie własne]
Fig. 2. Multi-algorithm biometric system schema

Zdarzenie awarii wieloalgorytmowego systemu biometrycznego określone jest wzorem:

$$Z_{ASB}=Z_{AS}\cap(Z_{BAI}\cup Z_{BAII}), \tag{4}$$

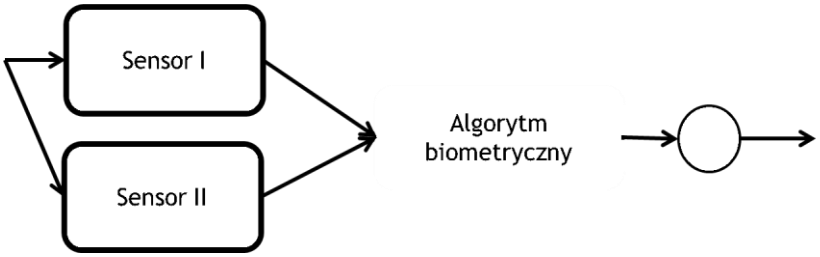
$$Z_{ASB}=(Z_{A}\cup Z_{UC}\cup Z_{BO})\cap(Z_{AFI}\cup Z_{API}\cup Z_{ADI}\cup Z_{AFII}\cup Z_{APII}\cup Z_{ADII}), \tag{5}$$

gdzie: Z_{BAI} – zdarzenie błędu algorytmu pierwszego,

Z_{BAII} – zdarzenie błędu algorytmu drugiego.

4.2. Niezawodność wielosensorowego systemu biometrycznego

Wielosensorowy system biometryczny (rys. 3) to taki, w którym do zebrania jednej cechy biometrycznej użyte są dwa niezależne sensory, np. dla odcisków palców analizowane są dwa palce, każdy niezależnym czytnikiem. Czytniki te mogą być identyczne, jednak zwiększa to ryzyko awarii spowodowanej wadą fabryczna, bądź różne – dla naszego przykładu jeden pojemnościowy drugi ultradźwiękowy. W kolejnej fazie porównywania do analizy cechy biometrycznej wykorzystywany jest jeden algorytm.



Rys. 3. Schemat wielosensorowego systemu biometrycznego [źródło: opracowanie własne]
Fig. 3. Multi-sensors biometric system schema

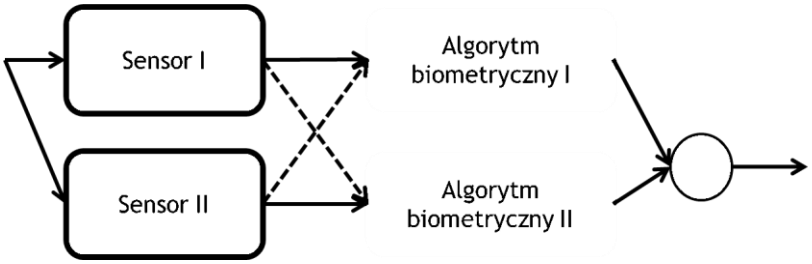
Zdarzenie awarii tego systemu określone jest wzorem:

$$Z_{ASB}=(Z_{ASI}\cup Z_{ASII})\cap(Z_{BA}), \quad (6)$$

$$Z_{ASB}=(Z_{AI}\cup Z_{BOI}\cup Z_{AII}\cup Z_{BOII}\cup Z_{UC})\cap(Z_{AF}\cup Z_{AP}\cup Z_{AD}). \quad (7)$$

4.3. Niezawodność hybrydowego system biometrycznego

System hybrydowy (rys. 4) to taki, który ma kilka sensorów i algorytmów do rozpoznawania jednej cechy biometrycznej. Każdy z algorytmów może analizować dane tylko z jednego sensora bądź z kilku. Jest to obecnie najczęściej stosowany typ wielomodułowych systemów biometrycznych dla jednej cechy.



Rys. 4. Schemat hybrydowego systemu biometrycznego [źródło: opracowanie własne]
Fig. 4. Hybrid biometric system schema

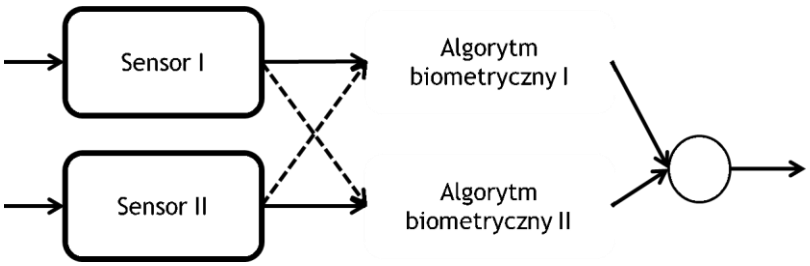
Zdarzenie awarii takiego system określone jest wzorem:

$$Z_{ASB}=(Z_{ASI}\cup Z_{ASII})\cap(Z_{BAI}\cup Z_{BAII}), \quad (8)$$

$$Z_{ASB}=(Z_{AI}\cup Z_{BOI}\cup Z_{AII}\cup Z_{BOII}\cup Z_{UCI}\cup Z_{UCII})\cap(Z_{AFI}\cup Z_{API}\cup Z_{ADI}\cup Z_{AFII}\cup Z_{APII}\cup Z_{ADII}). \quad (9)$$

4.4. Niezawodność systemu z dedykowanymi sensorami

System ten ma dwa niezależne sensory (rys. 5). Dane z każdego sensora przetwarzane są przez niezależne algorytmy.



Rys. 5. Schemat systemu z wieloma dedykowanymi sensorami [źródło: opracowanie własne]
Fig. 5. Multi dedicated sensors system schema

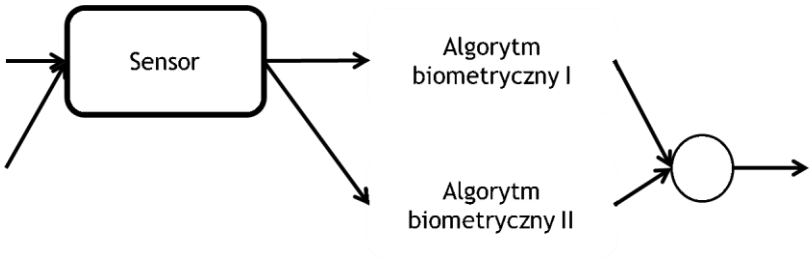
Zdarzenie awarii takiego system określone jest wzorem:

$$Z_{ASB}=(Z_{ASI}\cup Z_{ASII})\cap(Z_{BAI}\cup Z_{BAII}), \quad (10)$$

$$Z_{ASB}=(Z_{AI}\cup Z_{BOI}\cup Z_{AII}\cup Z_{BOII}\cup Z_{UCI}\cup Z_{UCII})\cap(Z_{AFI}\cup Z_{API}Z_{ADI}\cup Z_{AFII}\cup Z_{APII}\cup Z_{ADII}). \quad (11)$$

4.5. Niezawodność systemu z jednym sensorem

System z jednym sensorem ma tylko jeden fizyczny sensor (rys. 6), analizujący dwie cechy biometryczne, np. skaner dłoni wysokiej rozdzielczości, który umożliwia także odczyt układu linii papilarnych.



Rys. 6. Schemat systemu z jednym sensorem [źródło: opracowanie własne]
Fig. 6. Multi instance biometric system schema

Zdarzenie awarii takiego systemu określone jest wzorem:

$$Z_{ASB}=(Z_{ASI})\cap(Z_{BAI}\cup Z_{BAII}), \quad (11)$$

$$Z_{ASB}=(Z_{A}\cup Z_{UCI}\cup Z_{UCII}\cup Z_{BO})\cap(Z_{AFI}\cup Z_{API}\cup Z_{ADI}\cup Z_{AFII}\cup Z_{APII}\cup Z_{ADII}). \quad (12)$$

5. Eksperyment

Opracowany system należy do grupy systemów biometrycznych z dedykowanymi sensorami. Składa się z modułu opartego na czytniku linii papilarnych oraz z modułu rozpoznawania układu żył w palcu – Hitachi Finger Vein H1 Unit. Czytnik linii papilarnych wyposażony jest w algorytm bazujący na rozpoznawaniu grup minucji [17, 19, 20]. Tabela 3 prezentuje wyniki dla każdego z modułów pojedynczo oraz całego systemu. Moduł decyzyjny bazuje na wagach, których wartości to odpowiednio 0,4 i 0,6. Jak widać system hybrydowy ma znacznie lepsze wyniki FAR i FRR niż każdy z systemów samodzielnie.

Tabela 3

Wyniki badań dla opracowanego systemu
The results of the developed system

System	FAR	FRR
Rozpoznawania odcisków palców na podstawie grup minucji	0,25%	0,09%
Rozpoznawania rozkładu naczyń krwionośnych palca	0,05%	0,80%
System hybrydowy (wielomodułowy)	0,03%	0,08%

Źródło: opracowanie własne

6. Podsumowanie

Wielomodułowe systemy biometryczne zwiększają niezawodność oraz bezpieczeństwo całego systemu. Najskuteczniejsze są systemy bazujące na kilku cechach jednocześnie, są one jednak kilkakrotnie droższe od standardowych jednomodułowych systemów. Ich główną zaletą jest trudność oszukania przez potencjalnego intruza. Dość znaczącą wadą jest użyteczność, gdyż systemy te wymagają znacznie więcej czasu na analizę cech.

Podziękowanie

Badania są współfinansowane przez Unię Europejską w ramach Europejskiego Funduszu Społecznego. Finansowanie uzyskano w ramach projektu przedsiębiorczy doktorant.

Bibliografia

1. Wayman J.L., Jain A.K., Maltoni D., Maio D.: Biometric Systems. Technology, Design and Performance Evaluation, 1st Edition. Springer 2005.
2. Błoński G.: Hardware hacking – oszukiwanie zabezpieczeń biometrycznych, Hakin9 PL 7/2007, s. 26-30.
3. Maltoni D., Maio D., Jain A.K.: Prabhakar S. Handbook of Fingerprint Recognition, 2nd Edition. Springer 2009.
4. Jain A.K., Ross A., Nandakumar K.: Introducing to biometrics. Spinger 2011.
5. Ratha N.K., Govindaraju V.: Advances in Biometrics: Sensors, Algorithms and Systems. Springer 2007.
6. Chikkerur S., Govindaraju V., Cartwright E.N.: K-plet and coupled bfs: A graph based fingerprint representation and matching algorithm. LNCS Springer 2006, p. 309-315.

7. He Y., Ou Z.: Fingerprint matching algorithm based on local minutiae adjacency graph, Journal of Harbin Institute of Technology 10/05, 2005, p. 95-103.
8. Pankanti S., Prabhakar S., Jain A.K.: On the individuality of fingerprints, Proceedings of Computer Vision and Pattern Recognition (CVPR) 2001.
9. Bazen A.M., Gerez S.H.: Fingerprint matching by thin-plate spline modeling of elastic deformations, IEEE Pattern Recognition. 2003.
10. Cappelli R., Lumini A., Maio D., Maltoni D.: Fingerprint Classification by Directional Image Partitioning, IEEE Transactions on Pattern Analysis Machine Intelligence, Vol. 21, No. 5, 1999, p. 402-421.
11. Bebis G., Deaconu T., Georgiopoulos M.: Fingerprint Identification Using Delaunay Triangulation, IEEE ICIIS 1999, p. 452-459.
12. Parziale G., Niel A.: A fingerprint matching using minutiae triangulation. Proc. of ICBA, 2004.
13. Ross A., Dass S.C., Jain A.K.: A deformable model for fingerprint matching, Pattern Recognition 38(1), 2005, p. 95-103.
14. Ross, A., Nandakumar K., Jain A.K.: Handbook of Multibiometrics (International Series on Biometrics), Springer 2011.
15. Grzeszyk C.: Kryminalistyczne badania śladów linii papilarnych. Wydawnictwo Centrum Szkolenia Policji, Legionowo 1992.
16. Hicklin A., Watson C., Ulery B.: How many people have fingerprints that are hard to match, NIST Interagency Report 7271, 2005.
17. Huk M., Szczepanik M.: Multiple classifier error probability for multi-class problems. Maintenance and Reliability 3, 2011, p. 12-17.
18. Szczepanik M., Szewczyk R.: Algorytm rozpoznawania odcisków palców. KNS, tom 1, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2008, s. 131 -136.
19. Hong L., Wan Y., Jain A. K.: Fingerprint image enhancement: Algorithm and performance evaluation, IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, p. 777-789.
20. Ross, A., Nandakumar K., Jain, A.K.: Handbook of Multibiometrics (International Series on Biometrics). Springer 2011.

Abstract

In this paper authors compare different types of multimodal biometric systems. Multimodal biometric systems is system which take input from one or multiple sensors and analysis it using one or more different biometric characteristics. There are five types of these systems: Multi algorithmic biometric system (MABS), Multi sensorial biometric system (MSBS), Multi biometric characteristic system (MBCS), Multi instance biometric system

(MIBS), Hybrid multi-modal biometric system (HMMBS). MABS take data from a single sensor and process it using two or more different algorithms. MSBS take data about the same biometric characteristics from two or more different sensors. MBCS take data about two or more biometric characteristics from two different sensors. MIBS systems use one or more sensors to capture samples of two or more different instances of the same biometric characteristics. HMMBS connecting two or more different type of multiple classifier. Authors propose Hybrid multi-modal biometric system and compare reliability and quality of it with standard biometric system. Results of experiment is presented in Table 3.