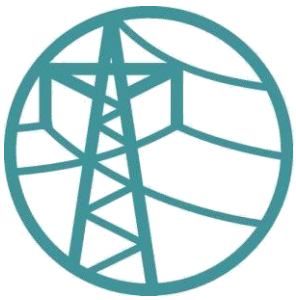


WYDZIAŁ
ELEKTROTECHNIKI
I INFORMATYKI
POLITECHNIKI RZESZOWSKIEJ

Jakub Skrzynecki

Uwierzytelnianie tempem pisania

Spis treści

1 Wstęp

Systemy biometryczne stanowią dynamicznie rozwijającą się dziedzinę zabezpieczeń, oferując alternatywę dla tradycyjnych metod uwierzytelniania, takich jak hasła czy karty identyfikacyjne. Jedną z ciekawszych kategorii jest biometria behawioralna, która analizuje unikalne wzorce zachowań użytkownika. Uwierzytelnianie na podstawie dynamiki pisania na klawiaturze (ang. keystroke dynamics) jest przykładem takiej techniki. Opiera się ona na założeniu, że każdy użytkownik posiada indywidualny i powtarzalny rytm oraz sposób wprowadzania znaków, co może zostać wykorzystane do jego identyfikacji lub weryfikacji. Metoda ta analizuje charakterystyki czasowe, takie jak czas trwania naciśnięcia poszczególnych klawiszy (Tz) oraz czas przerw pomiędzy kolejnymi naciśnięciami (Tp).

Kluczowym aspektem oceny każdego systemu biometrycznego jest analiza jego podatności na błędy, takie jak fałszywe akceptacje (FMR – False Match Rate, czyli wskaźnik błędnej zgodności) oraz fałszywe odrzucenia (FNMR – False Non-Match Rate, czyli wskaźnik błędnej niezgodności). Skuteczność systemu często wizualizuje się za pomocą krzywych ROC (Receiver Operating Characteristic) oraz powiązanych z nimi metryk, takich jak AUC (Area Under Curve, czyli pole pod krzywą) czy EER (Equal Error Rate, czyli współczynnik równego błędu).

Niniejsze sprawozdanie przedstawia analizę systemu uwierzytelniania opartego na tempie pisania, przeprowadzoną w ramach ćwiczenia laboratoryjnego.

2 Cel projektu

Głównym celem przeprowadzonego ćwiczenia była ocena skuteczności metody uwierzytelniania użytkownika bazującej na analizie dynamiki wpisywania przez niego hasła. Cele szczegółowe obejmowały:

1) Analizę charakterystyk czasowych procesu wprowadzania hasła, w tym czasów naciśnięcia poszczególnych znaków (Tz) oraz odstępów czasowych między nimi (Tp) podczas fazy rejestracji wzorca biometrycznego.
2) Wyznaczenie deskryptora biometrycznego użytkownika na podstawie zebranych danych.
3) Porównanie zarejestrowanego wzorca z próbami weryfikacyjnymi pochodzącymi od użytkownika uprawnionego oraz użytkownika nieuprawnionego.
4) Analizę i porównanie skuteczności dwóch różnych komparatorów (Komparator A i Komparator B) wykorzystywanych do oceny podobieństwa wprowadzanych danych do wzorca.

5) Ocenę wydajności komparatorów z wykorzystaniem krzywych ROC, wartości AUC oraz EER.
6) Analizę rozkładów punktacji uzyskanych dla użytkownika uprawnionego i nieuprawnionego oraz wyznaczenie optymalnych progów decyzyjnych dla badanych komparatorów.

3 Realizacja laboratorium

Badanie eksperymentalne przeprowadzono z wykorzystaniem dedykowanego oprogramowania "Tempo pisania", umożliwiającego rejestrację wzorca biometrycznego oraz weryfikację użytkowników na podstawie dynamiki wprowadzania hasła. Hasłem referencyjnym użytym w trakcie eksperymentu było słowo "haslomaslo". Procedura laboratoryjna składała się z następujących etapów:

3.1 Rejestracja wzorca biometrycznego

Pierwszym krokiem było utworzenie wzorca biometrycznego dla użytkownika uprawnionego. W tym celu uruchomiono program "Tempo pisania" i w zakładce "Rejestracja/Weryfikacja" wybrano opcję "Rejestracja". W procesie rejestracji użytkownik wzorcowy wprowadził ustalone hasło "haslomaslo" 25 razy, co zostało dostosowane na potrzeby tego konkretnego ćwiczenia w porównaniu z domyślną liczbą 50 powtórzeń sugerowaną w opisie programu. Każde wprowadzenie hasła było potwierdzane klawiszem Enter. Program rejestrował czasy naciśnięcia poszczególnych klawiszy (Tz) oraz czasy przerw pomiędzy nimi (Tp).

3.2 Weryfikacja użytkownika uprawnionego

Po pomyślnym zarejestrowaniu wzorca przystąpiono do etapu weryfikacji użytkownika uprawnionego. W programie wybrano opcję "Weryfikacja (uprawniony)". Użytkownik uprawniony (ten sam, który dokonywał rejestracji) wprowadził hasło "haslomaslo" łącznie 200 razy. Dla każdej próby program porównywał dynamikę pisania z zapisanym wzorcem, generując punktację odzwierciedlającą stopień podobieństwa. Program był skonfigurowany do zbierania danych dla dwóch różnych algorytmów porównawczych, określonych jako Komparator A i Komparator B.

3.3 Weryfikacja użytkownika nieuprawnionego

Kolejnym etapem była symulacja próby dostępu przez osobę nieuprawnioną. W programie wybrano opcję "Weryfikacja (nieuprawniony)". Inny użytkownik (osoba nieuprawniona) wprowadził to samo hasło "haslomaslo" również 200 razy. Podobnie jak

w przypadku użytkownika uprawnionego, program rejestrował punktację dla każdej próby w odniesieniu do wzorca użytkownika uprawnionego, dla obu komparatorów.

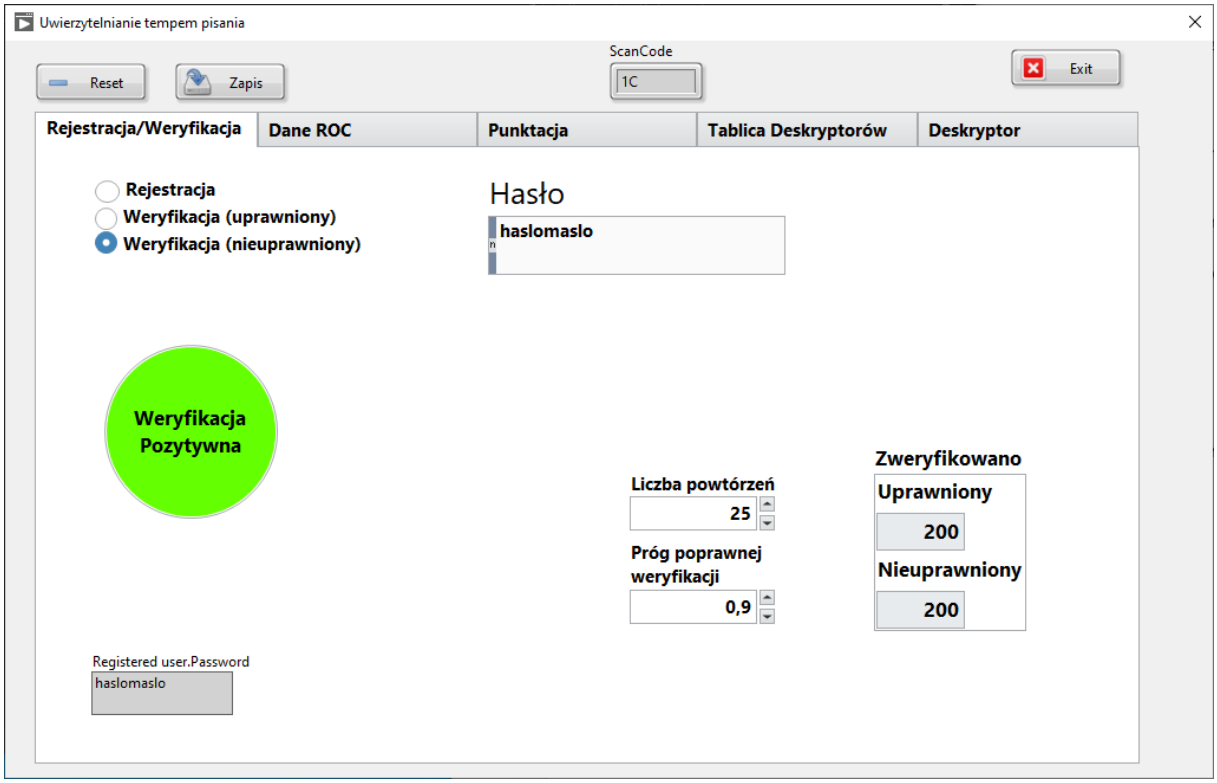
3.4 Zbieranie i zapis danych

Podczas wszystkich etapów weryfikacji (zarówno uprawnionej, jak i nieuprawnionej), program gromadził dane dotyczące punktacji uzyskanej dla każdej próby. Po zakończeniu zbierania danych, wyniki zostały zapisane do pliku tekstowego (wynik_koncowy.txt) za pomocą przycisku "Zapis". Plik ten zawierał m.in. średnie czasy naciśnięcia znaków (Tz) i odstępów między nimi (Tp) z fazy rejestracji, wyliczone deskryptory, a także surowe wyniki punktacji oraz dane niezbędne do wygenerowania krzywych ROC i analizy skuteczności komparatorów. Dodatkowo, program umożliwiał wizualizację histogramów czasów Tz i Tp (widoczne na załączonych rycinach) oraz rozkładów punktacji dla obu komparatorów.

4 Analiza wyników

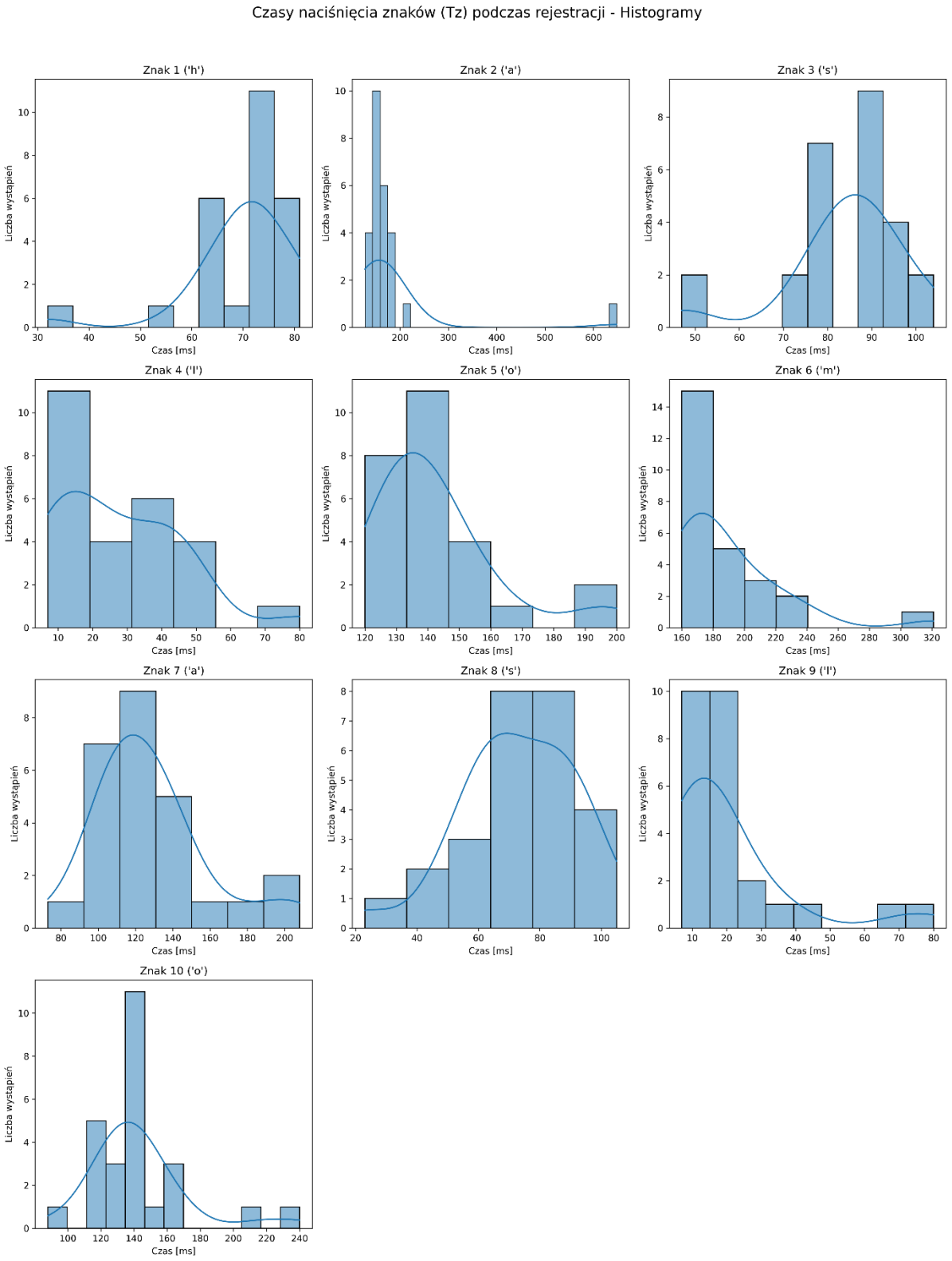
4.1 Analiza czasów naciśnięcia znaków (Tz) i odstępów między znakami (Tp) podczas rejestracji

Faza rejestracji wzorca biometrycznego dla hasła "haslomaslo" (o długości 10 znaków) polegała na jego 25-krotnym wprowadzeniu przez użytkownika wzorcowego. Informacja o zarejestrowanym haśle widoczna jest na Rys. 4.1 w polu "Registered user Password".

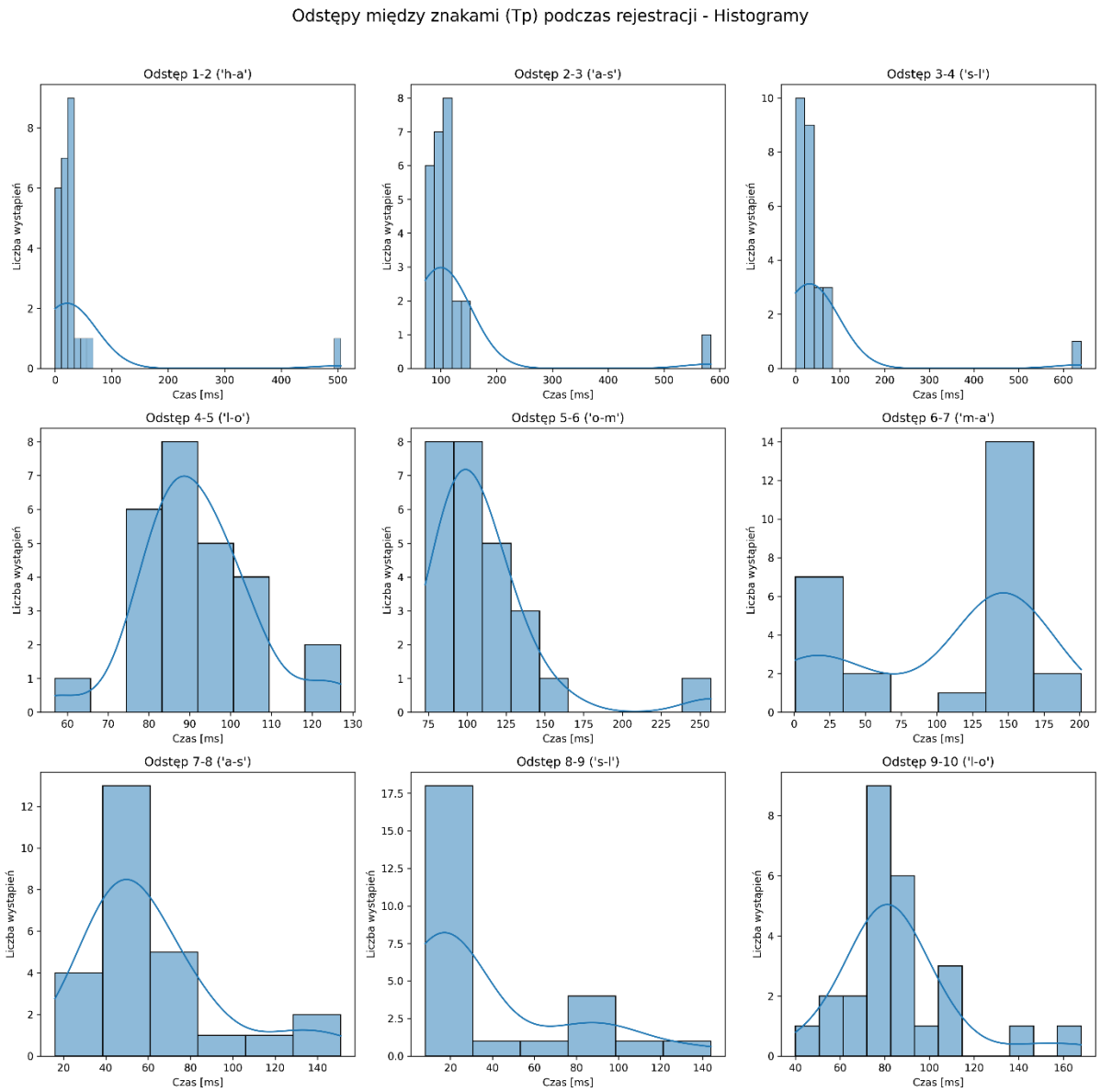


Rys. 4.1. Widok głównego okna programu "Tempo pisania" w zakładce "Rejestracja/Weryfikacja" podczas etapu weryfikacji użytkownika nieuprawnionego.

Na podstawie tych prób wygenerowano histogramy czasów naciśnięcia poszczególnych znaków (Tz) oraz odstępów czasowych pomiędzy nimi (Tp), przedstawione na Rys. 4.2 oraz Rys. 4.3.



Rys. 4.2 Histogramy czasu naciśnięcia poszczególnych znaków



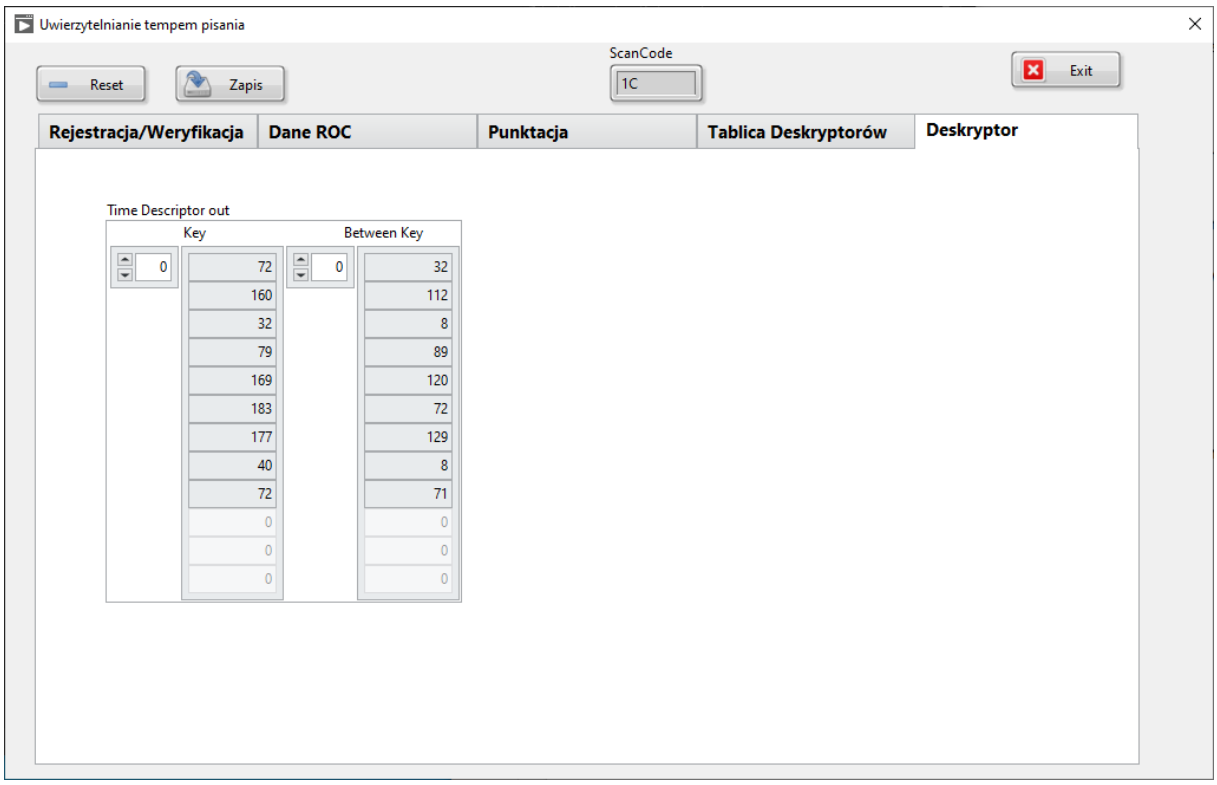
Rys. 4.3 Histogramy odstępów pomiędzy poszczególnymi znakami

Na ich podstawie, po odrzuceniu wartości skrajnych, obliczono średnie czasy charakterystyczne. Dla przykładu, średni czas naciśnięcia pierwszego znaku 'h' (Tz) wyniósł 69,92 ms, drugiego znaku 'a' 176,50 ms, a dziesiątego znaku 'o' 142,92 ms. Analogicznie, średni czas przerwy między pierwszym a drugim znakiem (Tp) wyniósł 40,46 ms, a między dziewiątym a dziesiątym znakiem 86,12 ms.

Program "Tempo pisania" również wygenerował własny deskryptor, którego wartości dla Tz wynoszą: 72, 160, 32, 79, 169, 183, 177, 40, 72 ms, a dla Tp: 32, 112, 8, 89, 120, 72, 129, 8, 71 ms. Różnice między tymi wartościami programowymi a obliczonymi samodzielnie

na podstawie histogramów wahają się dla Tz od 0,04 ms do 52,04 ms, a dla Tp od 2,85 ms do 66,85 ms. Tak znaczące rozbieżności mogą wynikać z różnych algorytmów filtracji wartości odstających zastosowanych przez program lub z odmiennych metod obliczania średnich czasów charakterystycznych.

Rys. 4.4 prezentuje graficzny interfejs deskryptora wygenerowanego przez program.



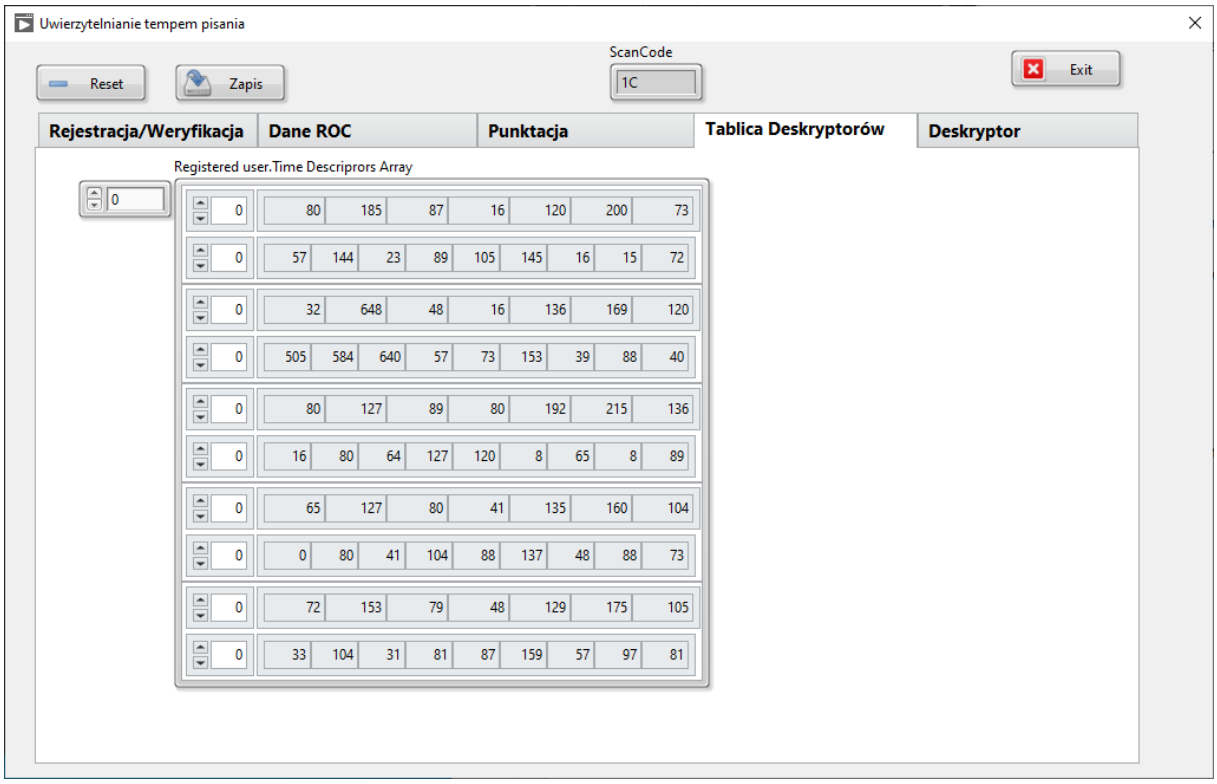
Rys. 4.4 Zakładka "Deskryptor" programu, pokazująca końcowy, uśredniony deskryptor użytkownika

Tabl. 4.1 Porównanie czasów z otrzymanego pliku i deskryptora programowego

Cecha	Wartość [ms]	Wartość z programu [ms]	Różnica [ms]
Znak 1 ('h')	72	69,92	2,08
Znak 2 ('a')	160	176,5	-16,5
Znak 3 ('s')	32	84,04	-52,04
Znak 4 ('l')	79	27,46	51,54
Znak 5 ('o')	169	142,35	26,65
Znak 6 ('m')	183	189,62	-6,62

Znak 7 ('a')	177	127,85	49,15
Znak 8 ('s')	40	75,08	-35,08
Znak 9 ('l')	72	20,42	51,58
Znak 10 ('o')	-	142,92	-
Odstęp 1-2	32	40,46	-8,46
Odstęp 2-3	112	119	-7
Odstęp 3-4	8	55,38	-47,38
Odstęp 4-5	89	91,85	-2,85
Odstęp 5-6	120	110,27	9,73
Odstęp 6-7	72	105,88	-33,88
Odstęp 7-8	129	62,15	66,85
Odstęp 8-9	8	38,42	-30,42
Odstęp 9-10	71	86,12	-15,12

Zauważalne są istotne rozbieżności między deskryptorem wyświetlanym w Tabl. 4.1 a deskryptorem programowym użytym do dalszych obliczeń skuteczności. Szczególnie wyraźne różnice występują dla znaków 3, 4, 7 i 9, gdzie różnica przekracza 49 ms, oraz dla odstępów 3-4, 6-7, 7-8 i 8-9, gdzie różnica wynosi od 30,42 ms do 66,85 ms. Różnice te mogą wynikać z zastosowania różnych metod filtracji danych lub z odmiennego algorytmu obliczania średnich czasów charakterystycznych.



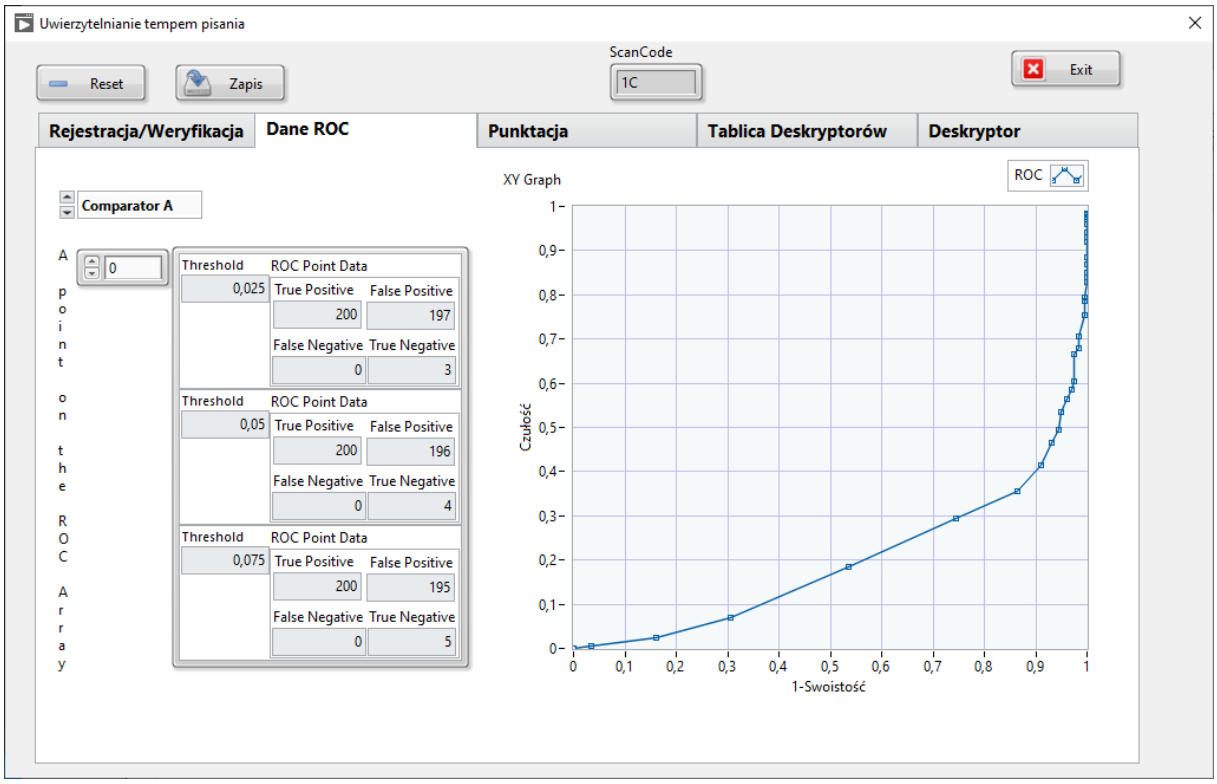
Rys. 4.5 Tabelaryczne zestawienie danych czasowych poszczególnych powtórzeń hasła

Rys. 4.5 ilustruje tabelaryczne zestawienie surowych danych czasowych dla poszczególnych powtórzeń hasła podczas fazy rejestracji, które stanowią podstawę do wyliczenia uśrednionego deskryptora. Dla oceny wydajności komparatorów kluczowe są jednak metryki wynikowe takie jak FMR, FNMR i AUC.

4.2 Analiza skuteczności Komparatora A

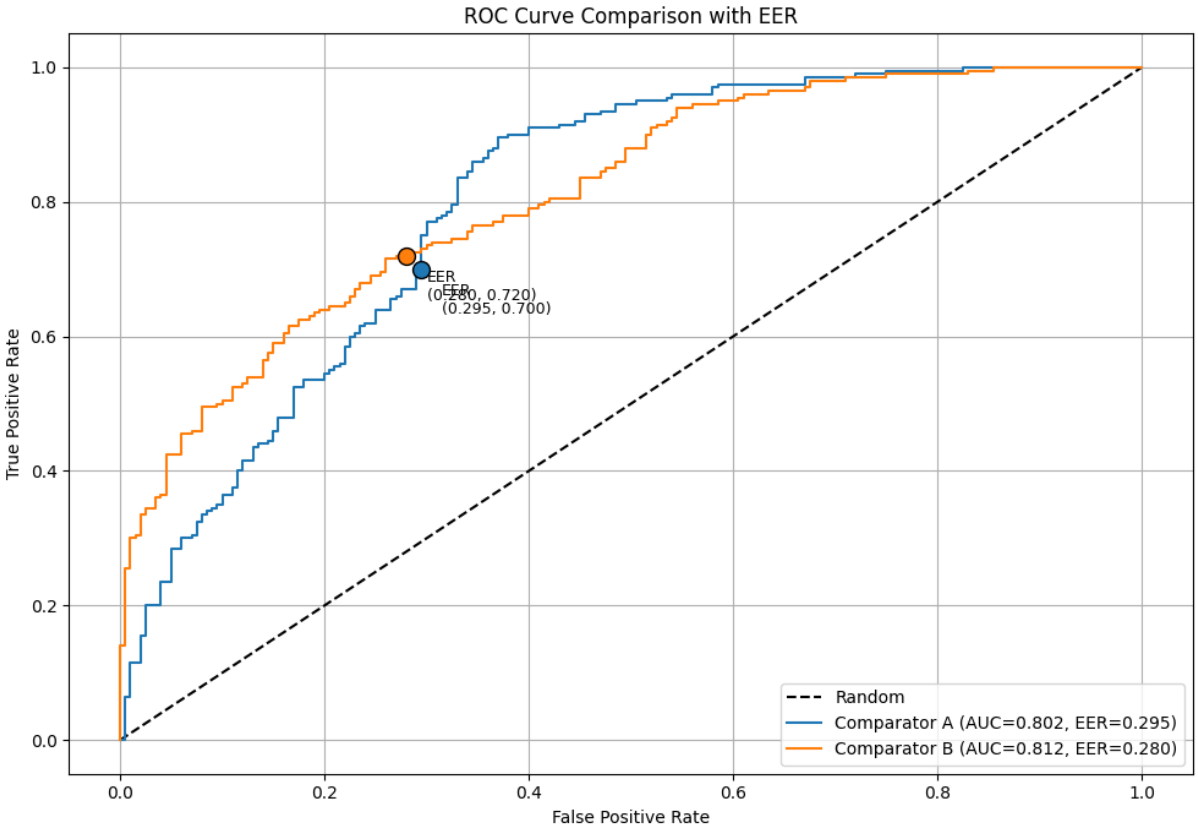
Skuteczność Komparatora A została oceniona przy użyciu standardowych metryk biometrycznych.

Krzywa ROC i AUC: Zbiorczy wykres krzywych ROC, przedstawiony na Rys. 4.6, ukazuje charakterystykę działania Komparatora A (linia niebieska). Pole powierzchni pod tą krzywą (AUC) dla Komparatora A wynosi 0,802. Wartość ta, zgodnie z przyjętą heurystyką klasyfikacji skuteczności systemów biometrycznych (gdzie wartości AUC > 0,8 uznawane są za bardzo dobre), plasuje skuteczność komparatora w kategorii "Bardzo dobra".

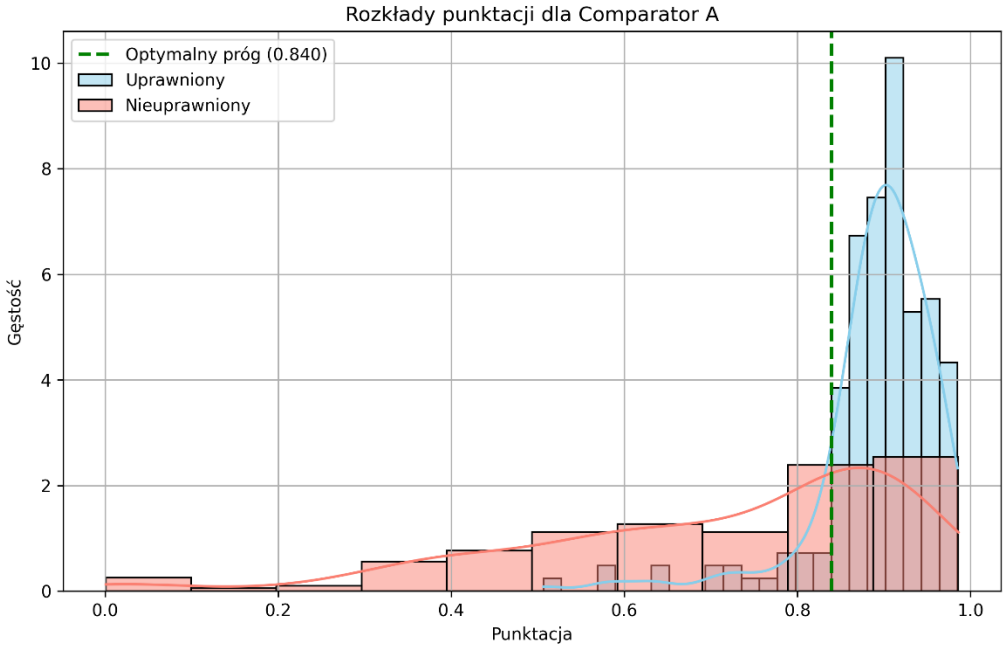


Rys. 4.6 Okno programu przedstawiające krzywą ROC komparatora A

Błąd EER (Equal Error Rate): Zgodnie z Rys. 4.7, wyznaczony błąd EER dla Komparatora A wynosi 0,295. Jest to punkt, w którym krzywa ROC przecina linię FMR = FNMR (lub jest najbliżej niej). EER został wyznaczony jako punkt przecięcia krzywej ROC z przekątną wykresu, czyli punkt, w którym wartości FMR i FNMR są sobie równe.



Rys. 4.7 Krzywa ROC z przedstawionymi punktami EER



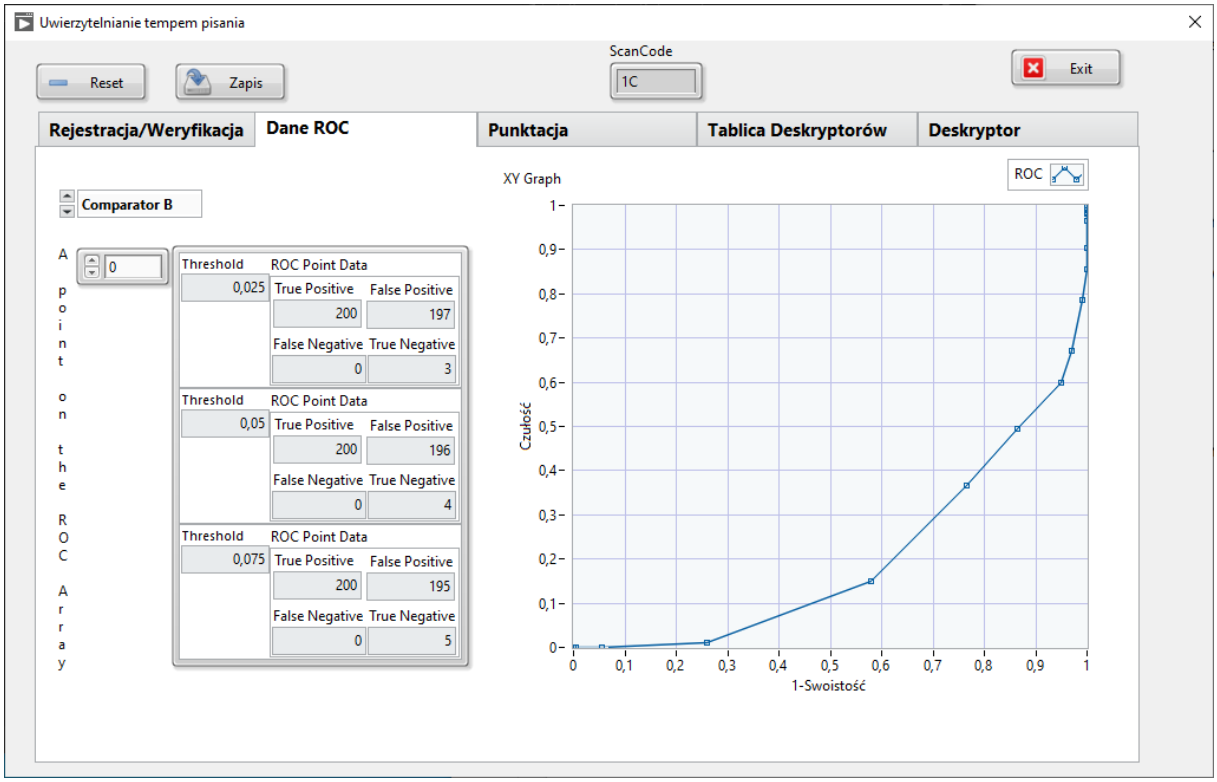
Rys. 4.8 Rozkład punktacji dla komparatora A

Rozkład punktacji i optymalny próg: Dystrybucja punktacji uzyskanych przez użytkownika uprawnionego i nieuprawnionego dla Komparatora A została przedstawiona na Rys. 4.8. Optymalna wartość progu akceptacji, wyznaczona przy założeniu FNMR ≤ 10% i minimalizacji FMR, wyniosła 0,8398 (na rycinie z rozkładem zaznaczona jako 0,840). Dla tego progu, wskaźnik fałszywych akceptacji (FMR) osiągnął 0,3800 (38%), a wskaźnik fałszywych odrzuceń (FNMR) 0,1000 (10%).

4.3 Analiza skuteczności Komparatora B

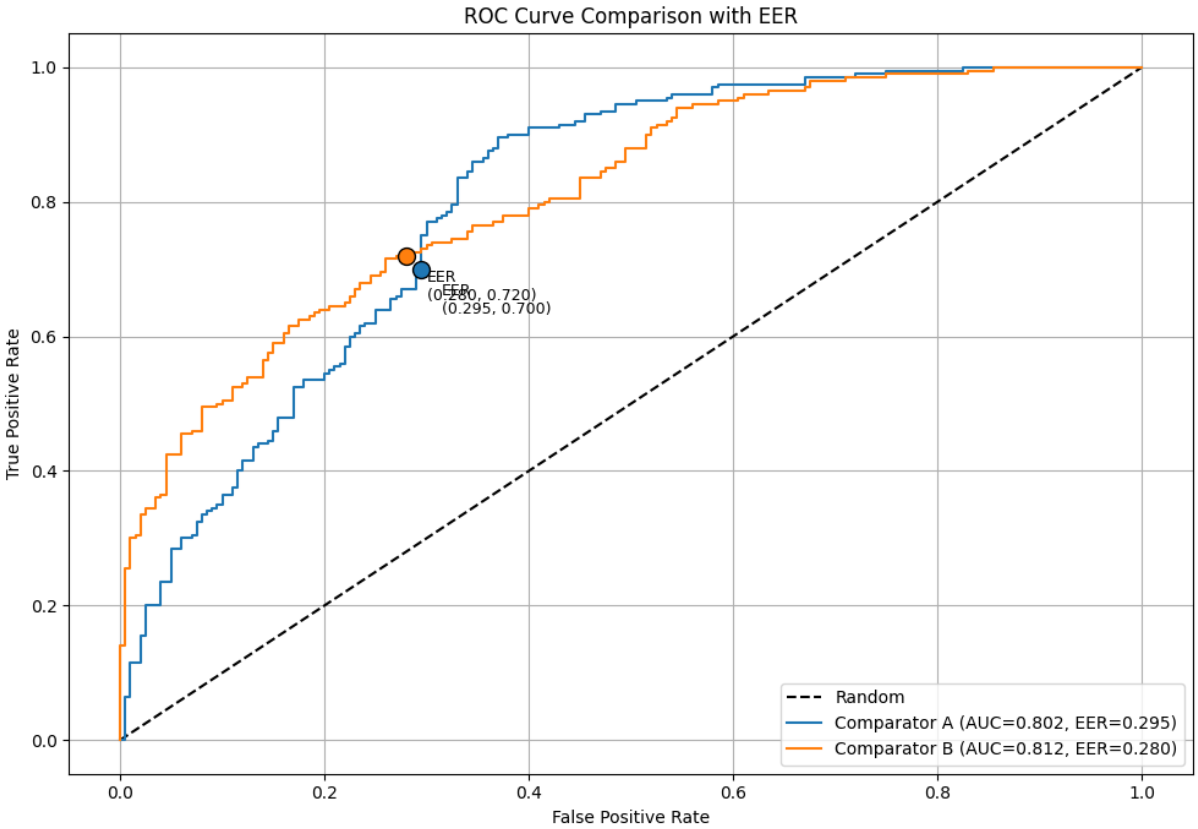
Analogiczne badania przeprowadzono dla Komparatora B.

Krzywa ROC i AUC: Wartość AUC dla Komparatora B wyniosła 0,8115, co również świadczy o "Bardzo dobrej" skuteczności i jest to wynik nieznacznie przewyższający Komparator A. Krzywa ROC dla tego komparatora, wraz z danymi punktowymi, jest zaprezentowana na Rys. 4.9.



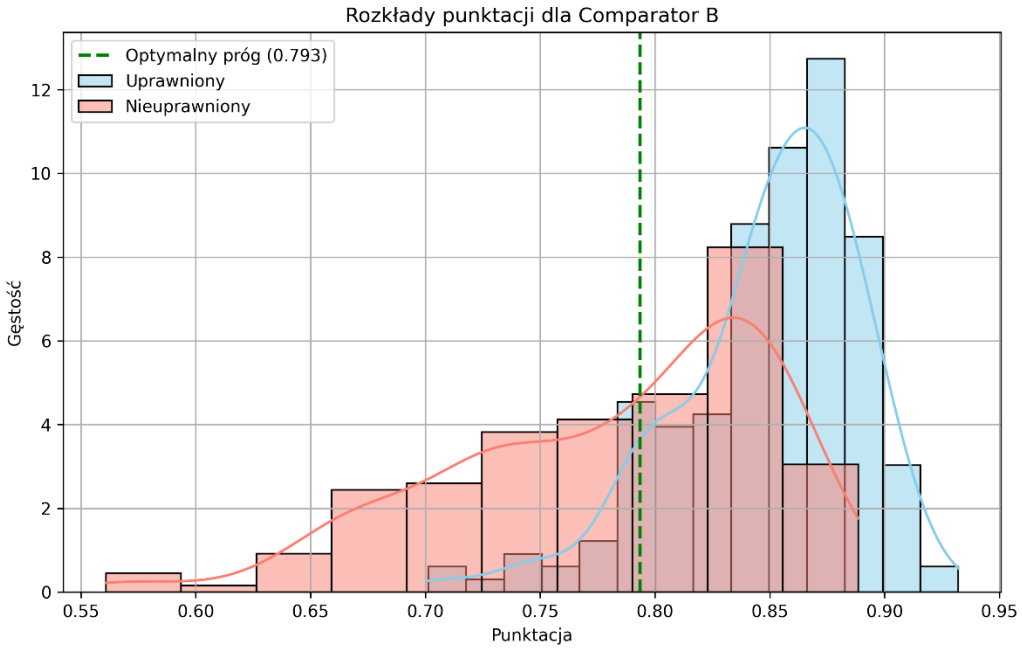
Rys. 4.9 Krzywa ROC komparatora B w programie

Błąd EER: Zgodnie z Rys. 4.10, wyznaczony błąd EER dla Komparatora B wynosi 0,280. EER został wyznaczony jako punkt, w którym wartości FMR i FNMR są sobie najbardziej zbliżone, czyli punkt, w którym różnica pomiędzy tymi dwoma wskaźnikami jest minimalna.



Rys. 4.10 Krzywa ROC z przedstawionymi punktami EER

Rozkład punktacji i optymalny próg: Rozkłady punktacji dla Komparatora B zilustrowano na Rys. 4.11. Optymalny próg akceptacji dla Komparatora B, przy tych samych kryteriach (FNMR ≤ 10%, minimalizacja FMR), ustalono na 0,7935 (na rycinie z rozkładem zaznaczony jako 0,793). Przy tym progu, FMR wyniósł 0,5150 (51,5%), przy FNMR równym 0,1000 (10%).



Rys. 4.11 Rozkład punktacji dla komparatora B

4.4 Porównanie komparatorów i ogólna ocena

Obydwa analizowane komparatory, A i B, charakteryzują się "Bardzo dobrą" ogólną zdolnością do rozróżniania użytkownika uprawnionego od nieuprawnionego, co potwierdzają wysokie wartości AUC (0,8018 dla A i 0,8115 dla B).

Porównując wartości EER obliczone z surowych danych ROC, Komparator B (0,2800) wykazuje nieznacznie lepszą wydajność niż Komparator A (0,2975).

Istotne różnice między komparatorami ujawnia analiza przy ustalonym akceptowalnym poziomie FNMR ≤ 10%. W takim scenariuszu Komparator A, przy FNMR = 10%, osiąga FMR na poziomie 38%. Dla Komparatora B, utrzymanie FNMR na poziomie 10% skutkuje znacznie wyższym FMR, wynoszącym 51,5%. Oznacza to, że jeśli priorytetem jest zapewnienie wygody użytkownikowi uprawnionemu (niski FNMR), Komparator A oferuje wyższy poziom bezpieczeństwa (niższy FMR).

5 Uwagi i wnioski

Przeprowadzone ćwiczenie laboratoryjne pozwoliło na praktyczną analizę systemu uwierzytelniania biometrycznego opartego na dynamice pisania oraz ocenę skuteczności dwóch różnych algorytmów porównawczych. Na podstawie uzyskanych wyników można sformułować następujące uwagi i wnioski:

1) Potencjał biometrii behawioralnej: Analiza czasów naciśnięcia klawiszy (Tz) oraz przerw między nimi (Tp) wykazała istnienie indywidualnych wzorców pisania, co potwierdzają wygenerowane rozkłady czasowe i deskryptory użytkownika. Wartości AUC dla obu komparatorów (odpowiednio 0,802 i 0,812) wskazują na "Bardzo dobrą" zdolność systemu do odróżniania użytkownika uprawnionego od nieuprawnionego, co potwierdza potencjał dynamiki pisania jako cechy biometrycznej.
2) Charakterystyka czasów pisania: Analiza histogramów czasów Tz i Tp ujawniła znaczącą różnorodność w sposobie wprowadzania poszczególnych znaków hasła. Na przykład, średnie czasy naciśnięcia klawiszy wahały się od ok. 20 ms do niemal 190 ms, a odstępy między naciśnięciami od 8 ms do 120 ms. Taka różnorodność może sprzyjać skuteczności systemu biometrycznego.
3) Rozbieżności w deskryptorach: Zaobserwowano istotne różnice między wartościami deskryptora obliczonymi na podstawie histogramów a wartościami wykorzystanymi przez program. Szczególnie duże rozbieżności (powyżej 50 ms) dotyczą znaków 3, 4, 7 i 9 oraz odstępu 7-8. Kwestia ta wymaga dalszej analizy w celu identyfikacji źródła rozbieżności.
4) Skuteczność komparatorów: Oba komparatory osiągnęły wartości AUC powyżej 0,8, co klasyfikuje je jako "Bardzo dobre". Wartość EER wyniosła odpowiednio 0,295 dla Komparatora A i 0,280 dla Komparatora B, co wskazuje na lepszą ogólną skuteczność Komparatora B.
5) Kompromis bezpieczeństwo-wygoda: Przy założeniu priorytetu wygody użytkownika (FNMR ≤ 10%), Komparator A oferuje istotnie lepszy poziom bezpieczeństwa (FMR = 38%) niż Komparator B (FMR = 51,5%). Oznacza to, że wybór optymalnego komparatora zależy od specyficznych wymagań aplikacji.
6) Znaczenie progu decyzyjnego: Analiza rozkładów punktacji podkreśla krytyczną rolę progu decyzyjnego w balansowaniu między bezpieczeństwem a wygodą systemu. Optymalne progi wyznaczone dla FNMR ≤ 10% (0,8398 dla A i 0,7935 dla B) stanowią kompromis, który wciąż dopuszcza stosunkowo wysoki poziom fałszywych akceptacji.
7) Niedoskonałość separacji klas: Zarówno rozkłady punktacji, jak i wartości FMR/FNMR wskazują, że badany system, mimo dobrych wyników AUC, nie zapewnia idealnej separacji między próbami użytkownika uprawnionego a nieuprawnionego. Istnieje znaczący obszar, w którym punktacje obu grup się pokrywają, co jest typowe dla wielu systemów biometrycznych, szczególnie behawioralnych.

8) Ograniczenia badania: Należy pamiętać o ograniczeniach przeprowadzonego badania, takich jak wykorzystanie jednego konkretnego hasła, ograniczonej liczby powtórzeń w fazie rejestracji (25 zamiast sugerowanych 50) oraz nieuwzględnienie czynników zewnętrznych, które mogą wpływać na dynamikę pisania (zmęczenie, nastrój, typ klawiatury).
9) Kierunki dalszych badań: Wskazane byłoby przeprowadzenie badań na większej grupie użytkowników, z wykorzystaniem różnych haseł oraz analizą stabilności wzorca biometrycznego w dłuższym okresie. Warto również rozważyć zastosowanie bardziej zaawansowanych metod przetwarzania sygnału i algorytmów uczenia maszynowego.

Podsumowując, uwierzytelnianie oparte na dynamice pisania jest obiecującą techniką biometryczną, która może stanowić wartościowe uzupełnienie tradycyjnych metod zabezpieczeń. Jednakże, jak każdy system biometryczny, wymaga starannej kalibracji i uwzględnienia specyfiki zastosowania w celu osiągnięcia optymalnego kompromisu między bezpieczeństwem a wygodą użytkownika.