Autor rozprawy doktorskiej: mgr inż. Marcin Bugdol

Tytuł rozprawy doktorskiej w języku polskim:

Metoda multimodalnego wzmacniania kryptografii w aspekcie biometrii behawioralnej

Tytuł rozprawy doktorskiej w języku angielskim:

Method of multimodal cryptography strengthening under the aspect of behavioral biometrics

Promotor rozprawy doktorskiej: dr hab. inż. Andrzej W. Mitas, prof. nzw. w Pol. Śl.

Jednostka prowadząca przewód doktorski:

Politechnika Śląska, Wydział Automatyki, Elektroniki i Informatyki

Słowa kluczowe:

biometria multimodalna, biometria behawioralna, kryptografia biometryczna, EKG, analiza głosu

Streszczenie rozprawy doktorskiej w języku polskim:

Celem pracy jest próba zastosowania metod matematycznych w asocjacji zasadniczo odmiennych technik biometrycznych. Finalnym celem podejmowanych działań jest określenie metody oraz stworzenie narzędzi sprzętowo-programowych do parametryzacji algorytmu pracy liniowego generatora ciągów szyfrujących. W ramach pracy stworzono stanowisko badawcze do pomiaru reakcji osób w odpowiedzi na kontrolowane pobudzenia wizualne i dźwiękowe. Mierzone były dwie modalności: sygnał EKG oraz sygnał dźwiękowy. Na podstawie zarejestrowanych sygnałów zaproponowano współczynniki, które posłużyły do weryfikacji badanych osób. Wykorzystanie metody PCA oraz analizy dyskryminacyjnej Fishera pozwoliło na dobór optymalnego zestawu parametrów. Zaproponowano koncepcję systemu kryptografii biometrycznej łączącego dotychczasowe metody uwierzytelniania (wiedza, posiadanie oraz biometria), w którym klucz szyfrujący jest zarówno zabezpieczony, jak i parametryzowany za pomocą wartości cech biometrycznych. Uzyskana dokładność systemu (około 93% poprawnych weryfikacji) pozwala twierdzić iż cel pracy został osiągnięty.

Streszczenie rozprawy doktorskiej w języku angielskim:

The aim of the thesis is to use the mathematical methods in association with fundamentally different biometric techniques. The final goal is to define the methods and to create hardware and software tools for parameterization operation algorithm of the linear cryptographic keys generator. Within the confines of this work a system which measure the response of people in response to controlled visual and audio stimulation was created. Two modalities were measured: ECG signal and voice. Based on the recorded signals the coefficients were proposed, which were used to verify the subjects. The PCA method and Fisher Discriminant Analysis allowed the selection of an optimal set of parameters. The idea of the biometric cryptography system which combines all currently used recognition methods (knowledge, possession and biometrics) was proposed. In this system the encryption key is both, protected and parameterized, using the biometric. The resulting system accuracy (about 93% correct verification) can claim that the objective of the thesis has been achieved.