Kryptografia wizualna

Jerzy Szymański, specjalność Cyberbezpieczeństwo

1. Charakterystyka problemu badawczego

   Przesyłanie i przechowywanie różnych danych poprzez narzędzia i systemy informatyczne powoduje konieczność zabezpieczania ich (oraz ich transmisji) przed niepowołanym dostępem. Jednym z ważnych typów danych są dane graficzne. Ich zabezpieczenie może być klasyczne (jak szyfrowanie każdych innych danych) lub z wykorzystaniem specjalnych technik związanych z ich wizualizacją. Problemy pokrewne związane są z takimi pojęciami jak dzielenie sekretu, steganografia czy cyfrowy znak wodny.

2. Motywacja/opis instytucji, proponującej współpracę nad projektem

   Bezpieczeństwo obrazów ma wiele ważnych zastosowań, począwszy od zabezpieczenia obrazów wrażliwych (np. medycznych) po problem dowodzenia autorstwa obrazu cyfrowego.

3. Planowane metody badawcze

   Analiza dostępnej literatury, badanie stosowanych metod, tworzenie oprogramowania.

4. Tematy i opis projektów

   - Dzielenie sekretu w grafice
   - Ukrywanie wiadomości w grafice (steganografia)
   - Dowodzenie autorstwa grafiki

5. Literatura

[1] Ateniese, Giuseppe; Blundo, Carlo; Santis, Alfredo De; Stinson, Douglas R. (2001). "Extended capabilities for visual cryptography". *Theoretical Computer Science*. **250** (1–2): 143–161.

[2] Horng, Gwoboa; Chen, Tzungher; Tsai, Du-Shiau (2006). "Cheating in Visual Cryptography". *Designs, Codes and Cryptography*. **38** (2): 219–23