Dream place essay

Cryptography can provide piracy protection during the transmission process, but when content is received and decrypted for display it can be illegally copied and redistributed. Digital watermarking is a promising technology that can provide lifetime protection by adding any traces of piracy to the content. Watermarks can represent information, such as the ID of the recipient and the time and place of delivery, which are transparently embedded into the content, by slightly changing the pixel values of the video frame, for example.

This information can later be extracted room an unauthorized copy to identify the source of the leak. Unfortunately, current watermarking schemes are vulnerable to a type of attack, called a collusion attack, launched by a group of users with different copies of the same content. Our research focuses on designing watermarking schemes that can resist collusion attacks. One branch of our work aims to construct code based on abstract assumptions about the embedding layer. L Another is embedding-focused and does not explore code structures. Our study shows that the code-based strategy has the advantage of low mutational complexity, but the embedding-based scheme holds the benefit of high collusion resistance, which is measured by the number of colludes that can be caught within a certain probability of detection. We describe a design that considers both coding and embedding layers to realize the combined advantages of each approach. To achieve this goal, we construct a two-layer code by combining a q-ray (using a number system where q is a positive integer of not less than 2) outer code with an inner binary code, shown in Figure 1. A resulting codeword is then assigned o one user and embedded into that user’s copy

prior to distribution. Illicit copying is detected when a watermark is extracted from suspicious content and correlated with the watermark of each legitimate user. A user with a correlation higher than the threshold limit is declared to be a colluded. An additional hard detector can also be employed depending on the detection confidence required. 4 Figure 1 . A framework for Jointly coding and embedding digital watermarking.

More specifically, we employ a traceability code as the q-ray outer code, which can be instructed with a large minimum distance using an additional error-correcting code. To embed a codeword we use mutually orthogonal (independent) sequences to modulate the q symbols. At present, the sequence corresponding to each symbol in a user’s codeword is usually embedded into one segment of the multimedia content. In our alternative design, we divide each sequence into subsequences and randomly permute these subsequences before embedding. The same permutation applies to all user content Ana Is reversed at ten detector sloe.

Hogue 2 snows a comparison AT he performance of our scheme under a collusion attack against a conventional scheme. 3 We measure the probability of catching one colluded PDP during collusion attacks against different numbers of colludes. The results show that if we require PDP to be close to 1, the proposed scheme increases the collusion resistance from 6 to 24, a threefold improvement. We have also tested the performance of the proposed scheme under minority collusion attacks, and the collusion resistance has been increased from 3 to 20. 4 Figure 2. Resistance comparison of our forensic marking strategy under collusion attack.

Protecting multimedia content from unauthorized redistribution is a challenging task in the modern digital era. Digital watermarking is an emerging technology that can address the problem by recording evidence of illegal activity that later can be retrieved forensically, and therefore function as a deterrent. Our research shows that significant advantages in security can be achieved by using jointly coded and embedded digital watermarks. Our future work is aimed at further improving the design for lower computational complexity, and increasing resistance to a large number of colludes.