Traitor tracing is an essential mechanism for discouraging the piracy in digital content distribution. An adversarial model is identified as rebroadcasting the content encrypting keys or the content in the clear form. It is possible to fight against these piracy models by employing a fingerprinting code that gives a way to differentiate the encryption capability of each individual. We point three important characteristics of a fingerprinting code that affects its deployment in traitor tracing scheme against pirate rebroadcasting: (i) A robust fingerprinting code tolerates an adversary that chooses not to rebroadcast some messages. (ii) A tracing algorithm for fingerprinting code that does not require a priori upper-bound on coalition size to be successful in detecting a traitor. (iii) Extending the length of the fingerprinting code which refers to traitor-identification procedure of the code that doesn't depend on the length of the code or the distribution of the markings over the code.

We presented the first traitor tracing scheme with formal analysis of its success in traitor-identification that doesn't assume a priori bound on a traitor-coalition size while at the same time it is possible to extend the code without degrading the success of traitor identification due to non-extended part. This construction also supports the robustness without requiring a high pirate rebroadcasting threshold.