October 7, 1997
RT0307
Rights Management 3 pages

Research Report

IBM Token Method for One-Copy Application

N. Morimoto et. al.

IBM Research, Tokyo Research Laboratory
IBM Japan, Ltd.
1623-14 Shimotsuruma, Yamato
Kanagawa 242-8502, Japan

Research Division
Almaden - Austin - Beijing - Haifa - India - T. J. Watson - Tokyo - Zurich

Appendix to IBM Proposal

IBM TOKEN Method for One-Copy Application

October 7, 1997

OVERVIEW

In order to cover one-copy application, the copy control status is required to be changed, i.e. from "one-copy (allowed)" to "no-more copy". This status change can be done by removing the pre-attached copy permission data. The advantages of this approach are, (1) simple and low cost implementation, and (2) no impact to the image quality. The basic idea of this approach is to attach a copy permission (TOKEN) to the content to represent the permission of copying. When the watermark detector detects (1,0), the detector will then, verify the TOKEN. If the TOKEN is a valid one, the copy will be allowed and the TOKEN will be removed or destroyed when the copy is made. Because the lack of the TOKEN to be represent "No More Copy", and it is hard to re-generate the valid TOKEN without the knowledge of the secret function, the changed status will remain as long as the pre-embedded CCI is detectable. The representation of the copy control status is shown below;

pre-embedded CCI	Copy Control Status
(1,0) + TOKEN	One Copy (Allowed)
(1,0) without TOKEN	No More Copy

Creation and Verification of the TOKEN

The TOKEN is generated and attached to the MPEG data string. It is a binary bit stream generated by applying one-way hash function to the selected subset of the MPEG video data. Then, the TOKEN will be attached to the MPEG video stream (in its user data area). The generation of TOKEN will not cause any change of the MPEG data, therefore there is no impact to the visual quality of the image.

In the receiver side, TOKEN will be tested whether it is a valid TOKEN or not. Note that this operation will be done only if (CCI=1,0) is detected from the subject video content. The verification will be done by taking the same subset of the MPEG data and apply a TOKEN verification function. If the TOKEN is verified, the copy will be allowed and at the same time, the attached TOKEN will be removed or destroyed so that the further copy will not be allowed (i.e. CCI=1,0 without valid TOKEN represents "No More Copy").

In addition to removing/destroying TOKEN, a minimum part of the selected subset of MPEG data will also be modified in order to avoid illegal re-use of the original TOKEN. As the nature of the one-way hash function, any small modification applied to the subjected MPEG video data will result in completely different answer. Therefore, all we need to do is to change a minimum part of the data in the selected subset of data in order to disable the TOKEN. As a consequence, the process is simple and the required processing power is very low (estimated 2k gates), also the impact to the image caused by this change is negligible.

Hardware Requirement

At the recording device, TOKEN verification and removal function is required in addition to the watermark detection. In our proposal, the estimated additional gate-count to the basic detection chip is approximately 2k gates. This is assuming to use a fairly simple one-way hash function in the generation and the verification. The process done in this logic includes TOKEN

read, verification, and removal (or destruction). The logic will be integrated into a hardware detection chip. and the process will be done in real-time.

Application Issues

Given that the One-Copy situation will only occur at the recording device directly connected to the receiver of the broadcasted video, TOKEN is only required to survive up to and no more than the first recording device attached to the video receiver in this method. This will cover all of the digital transmission from the video receiver to the recorders. In this case, the video receiver acts as a passive device and no action or additional device is required. The only exception is the video receiver connected with recorder via analog transmission. In this case, the TOKEN will not be transmitted to the following recorders, i.e. video data would be recognized as "No More Copy". Following are several proposal to deal with this situation;

1. Allow all of the analog copy when the video is marked as (1,0)

The One-Copy content marked as (1,0) will be copied to current analog VCRs and there is no way to protect it. One way to view it is, to accept it, and only protect no more copy in digital domain. As long as the copy/transmission is done via analog signal, there will be a cumulative degradation in video quality and these are not as same quality as digital copy.

2. Use VBI to transmit "Copy Permission Signal"

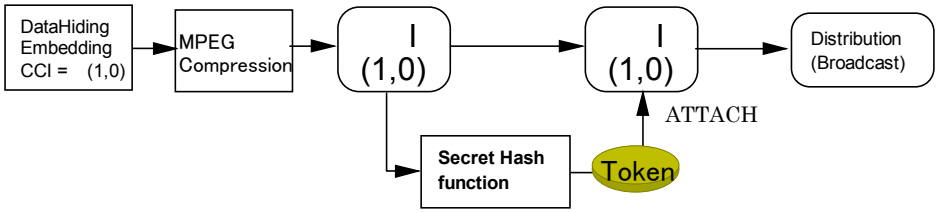
Another option is to use VBI to transmit "Copy Permission" signal to the following recorders. This will require video receivers to have capability to read CCI and verify the TOKEN and generate a "Copy Permission Signal" to be carried in VBI of the analog video. Although the VBI is a vulnerable channel, because of the nature of the signal, no one will try to destroy or remove this "Copy Permission Signal" because that is the only way to make a copy. This signal will be generated by using a same concept as TOKEN, but this time in analog domain. In this case, the video receiver will not be a passive device anymore and required to facilitate detection logic and TOKEN verification function.

Further Security Enhancement

In this proposal, the priority of the TOKEN generation function selection is implementation cost. The security of the TOKEN can be improved in trade with the complexity(cost) of the detection/verification algorithm. For example, the illegal re-generation of the TOKEN can be made very difficult even if a verification function is been known, by applying advanced cryptographic algorithm, such as DES and RSA. In such case, the gate counts will be increased by 10k - 20k or more depending on the complexity of the generation/verification function and the length of the key.

An Example of TOKEN Application Block Diagram

A. Token attachment



B. Token detection for "one copy"