September 2, 1997
RT0306
Rights Management 29 pages

Research Report

IBM DataHiding Proposal Version 1.0, In response to proposal CFP issued by DHSG of the CPTWGl

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

IBM DataHiding™ Proposal

Version 1.0

In response to the Call for Proposal Ver. 1.0 July 1, 1997

Issued by the Data Hiding Subgroup

Of the Copy Protection Technical Working Group

September 2, 1997

IBM Corporation

Preface

Table of Contents

1.Introduction

1.1. Overview

This document is submitted in response to the call for proposals issued by the Data Hiding Subgroup (DHSG) of the Copy Protection Technical Working Group. IBM is proposing the DataHiding™ technology and system as the most effective method for directly embedding Copy Control Information (CCI) into copyrighted digital video content in order to prevent unauthorized copying by consumers. By using the IBM DataHiding™ approach, it is possible to implement all the key functions of 1) copy control, 2) playback control and 3) single copy authorization, both effectively and economically. The use of IBM DataHiding™ can also significantly extend the existing copy protection methods for digital audio/video content:

1) By augmenting the existing Content Scrambling System (CSS) for copy protection of digital content published on read-only Digital Versatile Discs (DVD), the IBM DataHiding™ method presents a further barrier to unauthorized copying, even when the CSS scrambling has been removed. In addition, IBM DataHiding™ also provides a method for detecting and preventing the playback of unauthorized copies should they be made on DVD media.

2) Since the IBM DataHiding™ method applies the CCI data directly to the digital video content stream prior to compression and distribution, it provides protection independent of the digital distribution method, be it via electronic or physical means. Therefore digital content distributed via satellite, cable or to terrestrial broadcast or physical media other than DVD is equally well protected.

The IBM DataHiding™ system results in embedded data which has no perceptible impact on the picture quality of the displayed video, yet has a very high degree of survivability against the commonly employed processes of transmission and signal conversions. Therefore, no special actions are required during content transmission and distribution in order to preserve the delectability of the embedded CCI data within the designated copy and playback devices. Furthermore the embedding process employed in the IBM DataHiding™ system results in a high degree of resistance to unauthorized efforts aimed at disabling the embedded CCI data.

1.2. Target Functions and Devices

The basic functions which are required of IBM DataHiding™ system are copy control and DVD playback control. Copy control must include the capability to support single copy authorization.

Copy Control

Copy control is exerted within the hardware of the designated digital recording devices by detecting the embedded CCI data. If the CCI data is detected as ‘never copy’, then the recording action will be terminated. If the CCI data is detected as ‘single copy’ then, provided that the recorder is so equipped, the recording action is allowed to proceed, but the single copy is made with the CCI data updated to ‘no more copies’. If the recorder is not equipped to update the CCI, then the recording action is terminated. Copying is allowed if the detected CCI data corresponds to 'copy permitted' or if no CCI data is present or detected.

DVD Playback Control

DVD playback control is exerted by detecting the embedded CCI data within the hardware of devices capable of playing back DVD media containing copy protected copyrighted audio/video content. Playback control serves as an additional technical barrier and disincentive to unauthorized copying on DVD. The DVD playback control method is additionally based on the ability of the playback device to physically differentiate between read-only and recordable DVD media, and the response to the detected CCI data depends on the playback source media type.

If the copy protection state is 'never copy', then playback is allowed from read-only media, but disallowed if the media is recordable.

CCI data corresponding to 'single copy' results in termination of playback for both media types. However, if the media type is recordable, and the CCI data is detected as having been updated to reflect the creation of an authorized single copy, then playback is allowed to proceed. Playback is also allowed if the detected CCI data indicates 'copy permitted', or if no CCI data is present or detected.

The definition of which devices will be targeted for incorporation of IBM DataHiding™ detection capability is beyond the scope of this proposal. However, IBM is anticipating that the designated devices could include both DVD products and digital video tape recorders, and is designing detectors that are suitable for integration in either case.

2.Technical Description

2.1. Overview

The IBM DataHiding™ technology is based on a signal processing and statistical analysis technique that may, in general, be applied to digital images, digital video and digital audio. This technology allows for the embedding of invisible, robust, and secure signals directly into the digital video data stream that represents the digitized frame images. One advantage of this image-based data hiding approach results from the fact that the embedding process consists of direct manipulation of the luminance component of the pixels of the frame images. Although the degree of manipulation is held to be sufficiently small as to be imperceptible to the viewer, any electronic process that is applied to the image data which preserves the image quality will also preserve the embedded data. On the other hand, conversion processes which damage or attenuate the embedded data will also tend to have the same effect on the image data and therefore reduce the image quality of subsequent display and viewing of the video content.

The major technical advantages of the IBM DataHiding™ approach are summarized below,

- The method is very flexible in terms of optimizing the overall trade-off between the competing requirements of visibility, data capacity (payload), detection reliability and security.
- The intensity of the embedded data is variable and adapts to the complexity of the picture within each frame.
- The presence of the embedded data introduces no perceptible visual artifacts into the picture quality of the target video content.
- The reliability of detection of the embedded data is maximized through the use of frame accumulation detection methods
- The embedded data survives MPEG compression with minimal attenuation.
- The embedded data survives digital to analog conversion with minimal attenuation.
- Deliberate and unauthorized manipulation or removal of the embedded data is extremely difficult without detailed knowledge of the embedding algorithm process and algorithm, and this information is not required to be wholly contained within the detection hardware.

Finally, while this proposal describes IBM DataHiding™ for the primary purpose of embedding and conveying the CCI data associated with providing copy protection to the content, it is also possible to use our approach to embed data for other purposes associated with extended copyright management objectives and anti-piracy activities.

In the following section, we describe the IBM DataHiding™ technology in more detail , along with the supporting experimental and test data.

2.2. Embedding and Detection Process

2.2.1 Embedding Process

In IBM DataHiding™, the embedding process consists of manipulating the luminance components of each pixel in the image frame, (or field for interlace mode). The exact amount of adjustment for each pixel is determined following a specific set of rules that take into account the local image characteristics within that frame. This automatic and adaptive approach is designed to ensure maximum detectability of the embedded data, while simultaneously ensuring the absence of perceptible effects in the quality of the embedded image.

For the purposes of this application, the digital video frame image may be viewed as a two dimensional array of pixels. The embedding process may be represented by the following expression

$$\mathbf{I}' = \mathbf{I} + \mathbf{P} \qquad (2.2.1\text{-}1)$$

I represents the two-dimensional array of the luminance components of the pixels corresponding to the original digital image and **P** is a two dimensional array called the embedding pattern, or 'mark', which represents the adaptively determined modifications of the luminance components. **I'** represents the modified luminance components of the resultant video frame including the embedded mark.

2.2.2 Detection Process

Detection is the process by which a digital video content stream is analyzed in order to determine the data values associated with the mark, should one be present. There are two significant issues of reliability associated with the detection process, false positive and false negative.

The DataHiding™ detection process for the possible presence of embedded data begins by applying a two-dimensional detection mask, **M**, against the digital frame image from the video content stream. First, a specific correlation operation between the two dimensional array of pixel luminance components, **J** (which may be marked, **J**= **I'**, or unmarked, **J=I**), of the frame image and the detection mask, **M** is calculated. This operation is defined as follows:

$$\mathbf{M} \bullet \mathbf{J} = \sum_{i=1}^{N} m_i \cdot j_i \qquad (2.2.2\text{-}1)$$

Where m_i and j_i represent the i-th array elements of the mask and pixel luminance components, respectively, and N is the total number of the elements. The detection logic then compares the normalized absolute value of the parameter R, see below, to a predefined threshold value T in order to determine whether or not the image frame is marked. The parameter R represents the detected strength of the embedded signal:

if $R = \frac{|\mathbf{M} \bullet \mathbf{J}|}{S} < T$ then, “no mark” (2.2.2-2)

if $R = \frac{|\mathbf{M} \bullet \mathbf{J}|}{S} > T$ then, “mark” (2.2.2-3)

Since

$$\mathbf{M} \bullet \mathbf{J} = \mathbf{M} \bullet \mathbf{I} + \mathbf{M} \bullet \mathbf{P} \qquad (2.2.2\text{-}4)$$

when the frame image contains an embedded mark **P** (i.e. **J= I')**, the second term in the above equation triggers the ‘marked’ condition, otherwise the condition “no mark” is returned

S is a content-dependent normalization factor that is the basis for the statistical detection method employed in the IBM DataHiding™ method..

Multiple Bit Capabilities

Multiple “ bits ” of information can be simultaneously embedded in a single frame by partitioning the frame into multiple subsets, each of which represents one bit of the embedded data. Of course, the number of data bits embedded in the frame is increased, then improved detection strategies must be employed in order to preserve the required reliability of detection for all of the embedded data. One such strategy employed in the IBM DataHiding™ method is frame accumulation, which is described in a later section.

2.3. Image Quality Control

The requirement that the embedded signal does not have a perceptible effect on the visual quality of the marked video content is essential to the acceptability of the scheme to the end-user and the content owner. As noted above, the embedding algorithm employed for the IBM DataHiding™ method adaptively determines the magnitude of the amount by which the luminance component of each pixel can be altered in order to maximize the overall marking strength, while maintaining the highest standards for invisibility.

During the development of the IBM DataHiding™ method, visibility tests were conducted with expert volunteer test subjects and various types of video source material in order to refine the embedding algorithm and determine permissible levels for the overall marking strengths. The most critical of these tests was conducted with the assistance of a major motion picture studio using actual motion picture content which was selected to be broadly representative of the spectrum of content types. The test subjects (observers) were employees of the studio who were professionally involved in the picture quality control aspects of motion picture transfers to digital video.

Visual Test Summary

A total of 7 different uncompressed digital motion picture clips were selected for use in the visual test. A double-blind test was conducted according to the procedures defined in the ITU recommended practice of visual quality measurement. The basic format of the test consisted of showing a pair of identical video clips to the observer , each of 20 seconds duration. The video clip pair was repeated a second time, and the observer was asked to rank the visual quality of the second clip in the pair compared to the first. One or other of the clips in the pair was marked using the IBM DataHiding™ method, but whether it was shown first or second in the pair sequence was unknown to the observer, and determined at random. In addition, the strength of the embedded mark was varied over a range, including zero strength, and the various strength levels were randomly sequenced throughout the test series. The entire test consisted of 40 individual pairs of video clips, and took each subject approximately 50 minutes to complete. The professional test subjects reviewed the test material in isolation on a 20-inch professional grade monitor in a darkened professional video editing suite. The observers received no specific education other than the instructions required to fill out the response sheets.

At total 11 observers were asked to score their response on a numeric scale ranging from –3 (much worse) to +3 (much better), where a score of +/-1 corresponded to slightly better/worse. The results summary for the test is shown in Figure 2.3-1, where the total range of the responses averaged over all observers for all tested video clips are indicated as a function of the mark strength for the levels of 0, 4, 6, 8 and 10 which were used in the test. The results shown in the Figure 2.3-1 interpreted as a relative score of the marked image as compared to the non-marked image.

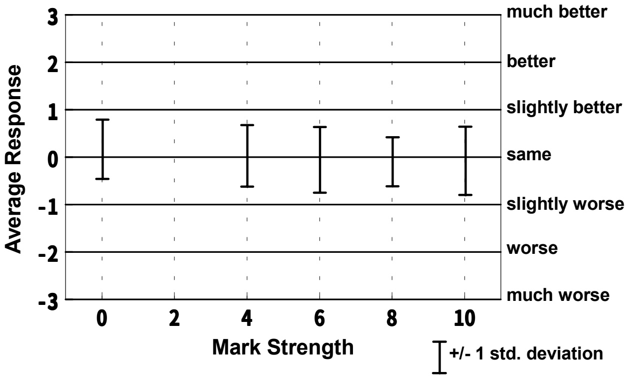

Figure 2.3-1 Image Quality Evaluation Scores Summary

These results indicate that, even with an embedding strength of 10, there is no significant agreement amongst the observers as to whether marked images are "better" or "worse" than non-marked image. Almost equal numbers of observers concluded that the unmarked image was very slightly inferior to the marked image, as concluded that it was slightly superior. The range of responses is not significantly different in the case of comparing clips with and without the most intense marking level of 10, as it was in the case when neither of the clips was marked (a fact which was unknown to the observers). We therefore conclude that the variability in the response to the marked clips reflects individual factors associated with the observers which are not correlated to the presence or absence of the embedded mark, which is imperceptible at all levels examined in this test.

The following figure shows the results in more detail , including the average scores recorded as a function of the individual clips. Once again no significant trends are observed in the data, and there appears to be no dependence on the gross pictorial characteristics of the content itself. (The range of clips was deliberately selected to include animation, black and white, title and credit sequences, low light, sunlight and interior shots.)

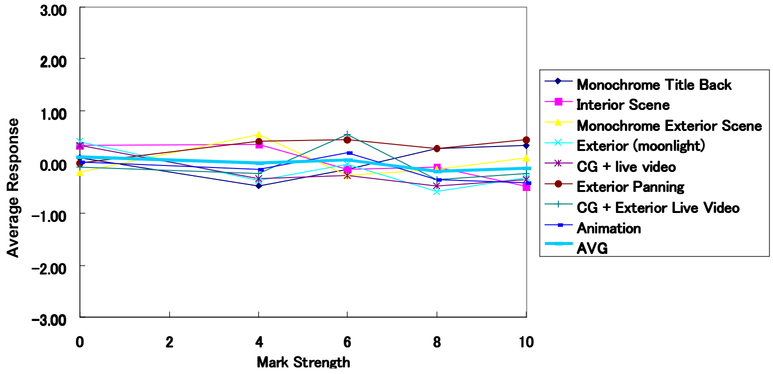

Figure 2.3-2 Average scores for various embedding levels and various type of video clip

In the visual testing described above, the original digital video signals were directly marked and then viewed without any other intervening processes. In practice the consumer will view the marked image only after it has passed through MPEG compression and decompression followed by conversion to the analog TV signal. In this case the quality difference between marked and non-marked images will become even less noticeable as the quality of the original video signal is slightly degraded. In this respect, the test described above was relatively stringent compared to the 'real-world' conditions, and the results can be treated as a "worst case evaluation" of the impact of our embedding process on the perceived image quality

2.4. Reliability of Detection

False positive error means that occur whenever the detector misinterprets a non-marked image to be a marked one. The false positive error is potentially a serious problem since it would tend to confuse and frustrate the consumer as they are prevented from making authorized copies, and could lead to unwarranted customer dissatisfaction with the operation of the recording and playback devices included in the copy protection system. False positive errors can be reduced by increasing the threshold level, *T*, for mark detection. On the other hand, as the threshold value is set higher, then the probability of a false negative error is increased,. An occasional false negative error does not significantly undermine the barrier to unauthorized copying, since the detector will analyze the video content repeatedly every several seconds throughout the duration of the content. Therefore, the probability of successive false negative detection results becomes vanishingly small as the number of detection attempts rises and the unauthorized copy is prevented within a few detection periods (typically less than one minute). However, optimal setting of the threshold value is one of the most important elements in determining the overall reliability performance of the system.

The key aspect of the IBM DataHiding™ system is the fact that the embedding and detection processes are both ultimately controlled and governed according to statistical criteria which are directly related to the detection reliability requirements. The embedding algorithm determines the value of mark strength in order to result in a detection level which is distinguishable by a predetermined statistical distance (i.e. reliability) from the distribution of detected " signals " that naturally occurs for the set of all unmarked frame images. The detection algorithm calculates this statistical distance in terms of the standard deviation of the distribution for the unmarked images.

2.4.1 False Positive Error

Based on the mathematical model we have developed for the DataHiding^{TM} technology, it is possible to quantitatively predict the probability for false positive detection errors as a function of the threshold parameter T, (see equation. 2.2.2-2.) and the total number of bits embedded in the frame. The numerical results of the model are summarized in the Table 2.4.1 below which shows the required threshold as a function of the required probability ratio for false positive detection. The Table includes data for the case where 4 bits are embedded, as well as when 8 bits are embedded in each frame. The table shows that a false positive probability requirement of 10^{-7} (corresponding to a mean time between false positive detection events of about 28,000 hours (10 seconds detection period assumed) or approximately 10 years when the record or playback device is used for 6 hours every day) will require a threshold setting of 6.2. This value for the threshold may be compared to the fact that even at embedding strength level 10, no perceptible effect on the picture quality was observed. In addition, whereas the data shown in the Table is based on single frame detection, we plan to use a multiple frame accumulation detection method which will improve the reliability even further.

Target False positive Error ratio	Threshold (*T*) for 4-bit embedding	Threshold (*T*) for 8-bit embedding	Mean time between false positive error detection [hours]
10^{-5}	5.3	6.1	280
10^{-6}	5.8	6.5	2,800
10^{-7}	6.2	6.9	28,000
10^{-8}	6.6	7.3	280,000

Table.2.4.1 Threshold Value (*T*) False Positive for Single Frame Detection

2.4.2 False Negative Error

Ultimately, the threshold level for any data hiding scheme must be determined by the need to reduce the probability of false positives below the required level. This is because the distribution of natural signals, which will be detected even in unmarked content is a function only of the embedding algorithm and the spectrum of naturally occurring image content. Ideally the strength of the embedded mark should be as large as possible compared to this threshold, in order that it be reliably detected, even after the attenuation which may occur as a result of various signal transformations between initial distribution and attempted unauthorized copying or playback. Since the constraint of imperceptibility ultimately limits the strength of the embedded mark, the only free design parameter which remains available to maximize the reliability of detection is the detection period itself. In the IBM DataHiding™ system, this is implemented in the multiple frame accumulation detection method.

2.4.3 Frame Accumulation Detection Method

In this method, the detected signal is accumulated over several frames duration. Since the detection process described above is based on statistical analysis, accumulation of the detected embedded signal strength over more than one frame leads to increased confidence levels in the "mark" or "no mark" decision made at the detector. This capability is also an important part of the robustness characteristics of the IBM DataHiding™ method. Embedded marks which have been attenuated through the effects of multiple conversions or transmissions may still be reliably detected, simply by extending the decision time until the desired level of confidence has been reached at the detector. This concept illustrated in the Figure 2.4.3.

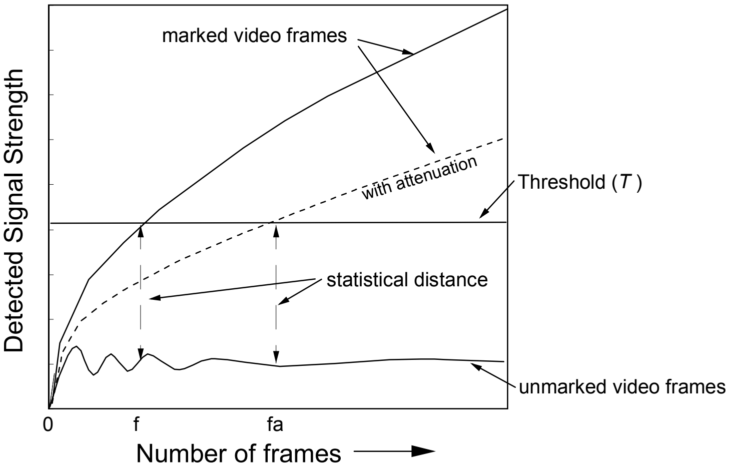

Figure 2.4.3 Frame Accumulation Effect

As the number of accumulated detected frames prior to the decision point is increased, the detection signal strength from the “marked” video increase where the signal strength from the “unmarked” video will be converged to a constant lower value. Thus the statistical distance between the detected signal strength derived from the“ marked ”and the‘ unmarked ’video frames increases. This results in greater certainty in the detectors ability to discriminate between the two cases , and avoid either false negatives or false positives.

As already discussed, setting the requirement for probability of false positive detection determines the threshold value, *T*. The upper curve shows the increasing strength of the detected signal, obtained from the “marked” video frames, as the number of accumulated frames increases. When the signal is attenuated, the curve will be reduced, as shown by the dotted line. However, the frame accumulation effect will still cause the detected signal to increase with the number of frames accumulated. The net result is that an equivalent detection reliability (i.e. statistical distance) can be achieved for the attenuated signal just by increasing the number of frames accumulated. The additional number of frames required to achieve equivalent detection reliability for attenuated signal can be simply expressed as follows;

$$f_a = \frac{1}{r^2} f \qquad (2.4.3)$$

Where the r represents the attenuation ratio of the detected signal strength after the signal transformation, f represents the number of the frames requires for the detection before the attenuation and the f_a is the number of frames required for the detection after the signal attenuation. In both cases, the target reliability is same. According to this equation, for example, if the signal is attenuated to 70%, the ratio, approximately twice as many as frames will be required for the detection if the same detection reliability is required.

2.5. Robustness

There are two aspects to be considered when characterizing the robustness of the IBM DataHiding™ method. The first concerns the ability of the embedded signal itself to survive the specified signal processing sequences. The second is the capability of the detection logic to reliably detect the residual signal. This may be limited either by the degree of attenuation which may have occurred, or by detection ambiguities introduced as a result of the particular sequence of processes, even when the embedded mark retains it's full original strength.

The IBM DataHiding™ method is technically capable of detecting the residual embedded signal in all of the cases outlined in the requirements section of the CFP. However, in practice some determination may be necessary concerning the actual capabilities included in the detection logic in order to achieve a reasonable balance between the cost and performance which is acceptable to all parties.

2.5.1 Embedded Signal Attenuation

Digital Noise Reduction and Aperture Correction

In general, those processes that include low pass filtering of the digital video signal may also lead to some attenuation of the embedded signal strength. This is because some of the higher frequency components of the embedded signal may not be passed through the low pass filter stage. Digital Noise Reduction (DNR) is an example of a process which results in a low pass filter effect. Aperture correction, on the other hand, is an image processing algorithm used to enhance the edges, and sharpen the image. Table 2.5.1-1 below shows that the largest signal attenuation caused by the digital noise reduction and the aperture correction processes we have examined is approximately 15% and 10% respectively. This result indicates that if the process preserves more of the image , then it will also preserve more of the embedded signal.. In the IBM DataHiding™ system this reduction may be compensated either by increasing the initial embedding signal strength, or extending the detection period.

Type of video processing	Detected signal strength
Embedded Source	100%
Aperture Correction	90%
Digital Noise Reduction	85%

Table 2.5.1-1 Signal Survivability after Video Processing

MPEG compression

The robustness of the embedded signal under MPEG compression is obviously extremely important, since virtually all digital motion picture content will be distributed in the compressed form. Relatively speaking, the I-frames of the MPEG Group of Pictures (GOP) are compressed to a lesser degree than either the P or B frames, since only intra-frame compression techniques are employed. As a result the embedded signal is also preserved to the highest degree within the I frames, and so it is the I frames that are used exclusively during the detection of the signal embedded by using IBM DataHiding™ algorithm directly from MPEG compressed streams. . During the I frame compression process there is a quantization of the coefficients of the Discrete Cosine Transformation (DCT) sub-blocks, which is a lossy process (i.e. one which is not perfectly reversible and therefore also capable of damaging the embedded signal.) Our compression testing indicates that the embedded signal strength may be reduced by about 10% to 30% as a result of MPEG compression, depending on the specifics of the compression algorithm. Increased attenuation will occur as the degree of compression is increased. Obviously, increasing the degree of compression will also negatively affect the picture quality of the restored digital video content.

Table 2.5.1-2 below summarizes the test results obtained using the IBM DataHiding™ method on samples of marked digital video which were subjected to MPEG compression applied at a Constant Bit Rate (CBR) of 4.0 Mbps. The embedded signal strength detected only from the I-frames shows less attenuation than when all the frames are included in the detection.

	With MPEG2 compression
Embedded Source	100%
Detection from I-frames	80%
Detection from all types of frames	68%

Table 2.5.1-2 Signal Survivability after MPEG2 Compression

Digital to Analog Conversion

Conversion from digital to an analog TV signal such as NTSC has an adverse effect on the embedded signal due to the low-pass filtering. This is a direct consequence of the inability of the bandwidth of the analog signal to carry all of the information represented in the original digital signal at the rate of 720 pixels per line. Experimental tests designed to measure the effect of the NTSC conversion shows that the embedded signal has been attenuated to 94% on average. This result is in excellent agreement with the theoretical analysis which predicts 93.8% attenuation, assuming that the net effect of the low pass limiting caused by analog signal conversion is equivalent to two neighboring pixels being averaged and merged into one.

In order to detect the embedded signal which is contained within an analog video signal, it is first necessary to perform an analog-to-digital conversion, because the current IBM DataHiding™ method performs the primary extraction only when the content is represented within the digital domain. However, if the original digital video stream has been subjected to a full digital-analog-digital sequence of conversions a new digital image is created after re-sampling. The detection of the original embedded signal within the newly re-sampled digital stream now requires additional computational capability in the detector circuits. The re-sampling may cause either or both a registration error and a scaling (size) mismatch between the original mask**, P**, used to insert the embedded signal, and the detection mask, **M**. If these effects are left uncompensated in the detector will both lead to decrease of the detected signal intensity and reduced detection reliability.

The IBM DataHiding™ method can solve this problem by adding function to the detection circuit which will enable the detector to adaptively maximize the correlation between the masks. However such functionality will increase both the cost and complexity of the detector chip. The relative complexity of dealing with these effects is increased still further when detecting directly within the MPEG compressed digital domain.

2.5.2 Summary of Design Trade-off

Table 2.5.2-1 summarizes the degrees of embedded signal attenuation caused by the kinds of signal processing discussed above.

Processing	Noise reduction	MPEG	D/A and A/D	TOTAL (worst case)
Attenuation rate	85%	68%	94%	54%

Table 2.5.2-1 Worst Case Analysis of the Embedded Signal Attenuation

The worst case estimate, 54% residual signal, for the embedded signal attenuation for video content which is subjected to every one of these processes is obtained simply multiplying all of the individual attenuation factors.

As already stated, there are two ways by which to compensate for the attenuated signal and to retain the required level of detection reliability. We can increase the initial embedded signal strength to pre-compensate for the potential attenuation, but this will eventually result in visible artifacts in the marked content. Alternatively, in order to keep the embedding intensity to be as low as possible and satisfy the detection reliability, the frame accumulation detection method is used. As described in section 2.4.2, this method is to maintain the detection reliability by extending the detection period and increase the number of frames for accumulation detection.

A key strength of the IBM DataHiding™ method is that it's design is highly flexible with respect to optimizing the overall reliability, robustness and even security performance according to the total set of functional requirements of the application. The final design point will be set collaboratively with the users of the system, following the completion of in-depth technical testing and mutual evaluation of the key operational parameters.

2.6. Security Aspects

[The full description of the security aspects of the IBM DataHiding™ method will be disclosed under NDA]

In developing the IBM DataHiding™ approach, the security of the approach against unauthorized removal, alteration or attenuation of the embedded signal has been a major consideration. Even though it is not practically possible for any technological means to withstand, over time, every conceivable attack, IBM DataHiding™ method includes several key aspects which strengthen it's 'tamper-resistant' capabilities, and offer significant impediments to a professional hacker whose objective might be to learn or derive sufficiently detailed information so as to create a cost effective "mark removal box" or a simple to use "mark removal" software.

The types of threat which we have considered in designing the security aspects of the IBM DataHiding™ method are categorized as follows:

Level-1: Resistance to Empirical attack in the digital domain to reveal embedding pattern

- Techniques involving additive random noise, digital filtering and pixel shifting, etc.
- Frame by frame summation and averaging in order to detect and remove the embedded data pattern

Level-2: Knowledgeable attack

- Knowledge from the publicly available documents.
- Situations where the attacker has gained unauthorized direct access to the core logic library of the detector, or has otherwise reverse engineered the detector chip

Level-3: Security against unauthorized use of licensed embedding systems

- Situations in which the attacker is using a licensed embedding system to overwrite the original embedded data in order to circumvent the original CCI conditions

3.IBM DataHiding^{TM} System

3.1. System Overview

IBM DataHiding™ system consists of two main elements, the embedding system installed at the content owners facility and the detection hardware which is built into the designated recording and DVD playback devices. The CCI data will be embedded into the digital video content stream prior to MPEG compression, and the embedding process used is completely separated from the compression stage. The IBM DataHiding™ embedding system will first be implemented in the form of a specialized hardware adapter installed on a dedicated computer system. Our objective is to meet the requirements of the content owner in terms of providing real-time and in-line marking capability as well as to provide a system which is flexible in terms of future enhancements as the overall processing power increases. A software implementation of the embedding function is planned, permitting even greater integration with network based digital video production systems and processes.

The detection of the CCI is primarily performed by direct analysis of the MPEG compressed digital video content data. The detection algorithms and overall functional capability of the IBM DataHiding™ detection systems have been designed to provide maximum functionality at minimum cost impact on the recording and playback devices. Our objective is to facilitate the manufacturers of the recording and playback devices with IBM DataHiding™ detection capability on the earliest possible schedule. Those manufacturers may have the option to purchase the hardware from IBM, use IBM designs to fabricate their own hardware, or implement the licensed detection logic and algorithms within their own design and have these design fabricated.

For the purposes of the discussion in this chapter, the CCI data is assumed to be the 8-bit payload specified in the essential requirements of the CFP.

3.1.1 Copy Control and Playback Control with embedded CCI

The proposed system will embed invisible and secure Copy Control Information (CCI) directly into the digital video content in order to effect the basic copy control and playback control functions defined in the CFP, i.e. “Never copy”, “One copy” and “No more copy”. The logical definitions for response to copy control and playback control data are summarized in Tables 3.1.1-1 and 3.1.1-2 below in terms of the required action within the recording and/or playback devices, depending on the data carried by the CCI. These Tables assume that the CCI is based on the conventions that originated in the Copy Generation Management Scheme (CGMS). Furthermore, the Tables are based on the following set of assumptions:

1. All content distributed by DVD-ROM media are either marked (1,1), (0,0) by DataHiding^{TM} or no mark
2. All content distributed by DVD-ROM media marked (1,1) is protected by CSS
3. Content distributed by electronic means may be marked (1,1), (1,0), (0,0) by DataHiding^{TM} or no mark
4. DVD playback devices are able to distinguish recordable media from read-only media
5. “No more copy” state is allowed to be on recordable media only

Copy Control Definitions

Detected CCI	Definition in CFP	Response of Recorder
1,1	Never copy	Prevent Copy
1,0	One-copy	Allow Copy and add Copy Mark
1,0 with Copy Mark	No more copy	Prevent Copy
0,0 or no mark	Copy allowed	Allow Copy

Table 3.1.1-1 Definition of CCI and required Response for Copy Control in recording devices

Table 3.1.1-1 summarizes the logical copy control response of the recording device. Note that when the content is marked as "One-Copy" or (1,0), the CCI status in the copy must be changed to indicate "No More Copy". This change is logically represented by the addition of the 'Copy Mark' to the original (1,0) value embedded in the incoming video stream. The 'Copy Mark' function is performed within the recording device, immediately prior to the creation of the single authorized copy, and is implemented as part of the IBM DataHiding™ system.

DVD Playback Control

The purpose of DVD playback control is to prevent play back of unauthorized "in the clear" copies of compressed digital video content from DVD media, which would otherwise be directly viewable following MPEG decoding alone. Table 3.1.1-2 summarizes the logical control elements of DVD playback control, again based on the CCI codes originated in CGMS, and based on our current understanding of the requirements.

Detected media type	Detected CCI	Response of the device
DVD-ROM	1,1	Prevent playback*
	1,0	Prevent playback
	1,0 with Copy Mark	Prevent playback
	0,0 or no mark	Allow playback
DVD-RAM or DVD-R	1,1	Prevent playback
	1,0	Prevent playback
	1,0 with Copy Mark	Allow playback
	0,0 or no mark	Allow playback

*** CCI (1,1) detected from DVD-ROM media without CSS protection indicates unauthorized copying. DVD-ROM playback is not prevented when CSS scrambling is present.**

Table 3.1.1-2 Definition of CCI and Response for Playback Control in DVD Players

Note: The actual implementation of the logical copy and playback controls with IBM DataHiding™ will match the final specification which is agreed to by the parties involved. It is also assumed that additional data, such as APS trigger bits, may be defined as part of the overall CCI data and these, also, will be included in the payload and implementation, as required.

3.2.Embedding System

3.2.1 Embedding Procedure Description

The embedding process for a single frame image is shown in following flow-chart;

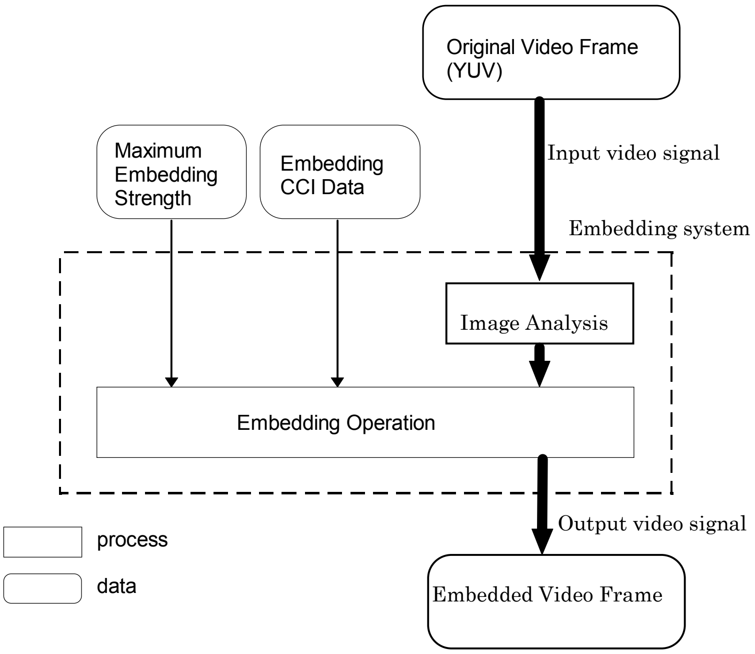

Figure 3.2.1 Process Flow of Data Embedding

The input image is uncompressed CCIR601 (YCbCr), and the embedding process will result in a small modification only to the Y component. The user will be able to select the upper limit of the embedding signal strength, in order to satisfy imperceptibility of the mark. The user also specifies the values for the CCI data to be embedded. The CCI-marked output image will be generated in the same format as the input.

The IBM DataHiding™ embedding system first performs image analysis on the original video frame in order to analyze and compute the optimum adjustment level for each pixel, consistent with the user specified maximum embedding strength, and the content dependent algorithm. The computed embedding pattern is then applied to the original image in order to produce the marked image ready for output.

3.2.2 Integration of the Embedding Process within the Production Sequence

Although the embedded data could survive the various video production processes, the effect will only be to reduce the embedded signal to some degree. Therefore, it is preferable to perform the embedding function as the final action (Case A in Fig. 3.2.2) before the MPEG compression.

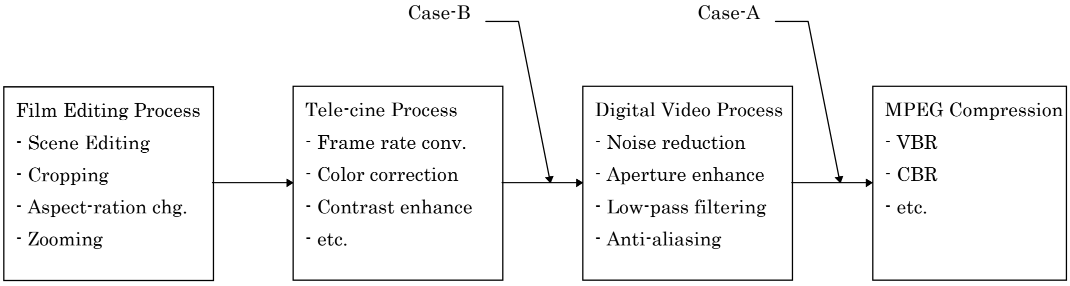

Figure 3.2.2 Optimum Embedding Location

3.2.3 Embedding System

The first implementation of the IBM DataHiding™ embedding system consists of a stand alone computer system connecting to two digital VCRs, one for the source input and the other for recording of the output (embedded) video content. The computer system basically functions as the controller unit for the embedding system processes. A Digital video interface card is required for the I/O to digital VCRs and a customized board is required for the real-time embedding process. An example of configuration of the system is shown in the following figure. Provision may be included in the system for delaying any audio stream associated with the incoming digital video, in order to maintain audio-video synchronization at the output.

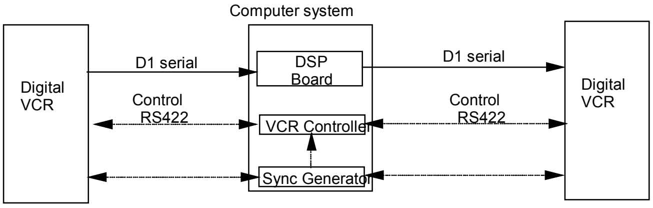

Figure 3.2.3 Standalone Embedding System

The embedding system performance is based on the computation efficiency of the custom board and processing power required for the embedding.

The implementation of the embedding system is not limited to that described above. The total system may be constructed with several standalone systems, connected via Local Area Network, each one processing part of the content in parallel. In the future,. as the processor power increases, the embedding system may be implemented entirely by software, without any special hardware, depending on the content owner ' s requirements. IBM DataHiding^{TM} Technology is flexible for implementation on any platform.

3.3. Detection System

The least cost implementation of the IBM DataHiding™ detection methods and algorithms will be achieved through integration of this function with semiconductor systems already present within the recording and/or playback devices. From this point of view, the details of the implementation will be highly dependent on the manufacturer involved. However, we have conducted an internal design analysis concerning the logic design and gate size estimation, which will be presented as part of this section,

3.3.1 Detection Procedure Description

As already discussed, the detection process consists fundamentally of applying pre-defined detection mask operations to the digital image data, so as to detect the specific statistical characteristics that are due to the embedded mark (when one is present). The detection may be done on the uncompressed digital video stream, or by directly processing in the domain of the compressed MPEG video data. The detected CCI data is fed to the control logic to determine what action will occur to represent the copy or playback control response. The basic detection process flow is shown in Figure 3.3.1.

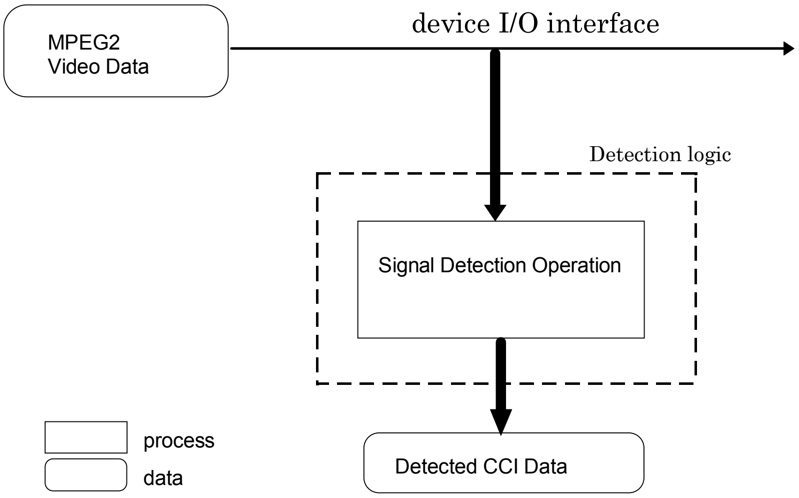

Figure 3.3.1 Process Flow of Detection Process

In the case of DVD playback control, one of the major requirements for the detection is the capability to detect the embedded data from the MPEG data string. This is possible using the IBM DataHiding™ method, provided some pre-processing is performed in advance of the core mark detection process.

In situations where the embedded signal must be detected starting with an analog video signal, it is necessary to perform an analog to digital conversion prior to the detection process. The detection then can be proceeded on the uncompressed digital frame images.

3.3.2 Detection Hardware Overview

The IBM DataHiding™ hardware is built into the designated recording and DVD playback devices, but the exact function depends on the nature of the host device, for example DVD-ROM, DVD recording device, DVC recorder or other designated recording and/or DVD playback devices. Currently we are planning to implement three different IBM DataHiding™ detection hardware designs, optimized for the main copy and playback scenarios as described below.

Chip-1: For applications requiring DVD playback control only

Chip-1 is for the applications requiring only DVD playback control, including DVD players and DVD-ROM drives. This chip will perform detection directly on the MPEG data stream to verify whether the content is marked or not, and determine the CCI. The detected CCI will be used by the controller of the DVD playback device to exercise the appropriate playback control according to the definition of playback control in section 3.1.

Chip-2: For applications requiring both copy control and DVD playback control

Chip-2 is for the applications requiring both copy control and DVD playback control including DVD recorder, DVD-RAM drive and DVD-R drive. Chip-2 contains the same logic as Chip-1 for the function of playback control but in addition, Chip-2 has the ability to detect the CCI and support the copy control function as defined in section 3.1. Chip-2 is also suitable for DVC recorder applications requiring just copy control (though not required, the DVD playback control response functions integrated into chip-2 represent minimal added gate count over the core detection logic and copy control functions). Chip-2 will have the capability to perform the function, or a function equivalent to, the addition of a “Copy Mark” to the contents at the time of recording when the content is marked as “one copy allowed”. Details of the implementation method for the Copy Mark requirement will be disclosed later.

Chip-3: For applications requiring copy control on recorders with analog video input

Chip-3 is for copy control on stand-alone devices such as DVC recorders or DVD-based video recorders which have an analog video input (or possibly an uncompressed digital video input). Chip-3 receives the uncompressed digital video data, converted internally within the device from the analog input video signal, and performs the detection process. If it is marked, the chip will detect the embedded CCI data and make it available to the controller of the device for the appropriate copy control action.

The Fig. 3.3.2 below shows schematically the application and logical location of each chip in the target device applications, and Table 3.3.2 below summarizes the function and estimated gate count for each detection logic.

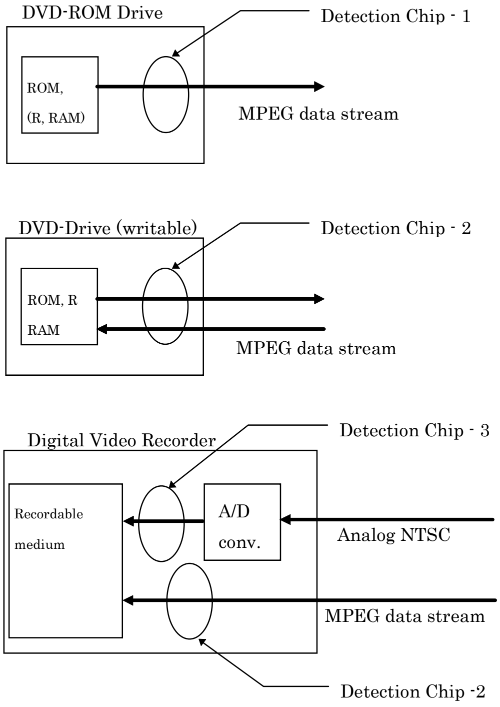

Figure 3.3.2 Logical Location of DataHiding^{TM} Detection chips

Type	Purpose	Description	Gate Counts	Device
Chip-1	Playback Control	Detection only. Detect CCI from MPEG data stream and send the result to the device controller. (This is a subset of chip-2.)	<40k Gates*	DVD player, DVD-ROM drive DVD playback only devices
Chip-2	Playback Control Copy Control	Detection of pre-embedded CCI from MPEG data stream and additional copy mark function.	<50k Gates*	DVD-RAM drive DVD-R drive Stand alone DVC and DVD recorder (not PC attached)
Chip-3	Copy Control	Detect embedded CCI from uncompressed digital video. Calibration and alignment of the digitized video signal is included prior to the detection. Process.	<30k Gates	Standalone digital recorders with analog video input, e.g. DVC recorder DVD recorder

*the gate count estimation are based on proposed functions described in the specification table 3.4.1.

Table 3.3.2 Function and Gate count Summary of DataHiding^{TM} Detection chips

Gate count Breakdown

The main element of the detection chips consist of memory (ROM, buffer), core detection logic and data/control signal I/O. For chip-2, additional output MPEG stream handling logic is required. MPEG string handling is not required for chip-3. The following list summarizes the estimated gate count allocation for the detection logic.

	Chip-1	Chip-2	Chip-3
Memory (ROM, buffer)	24	26	14
Detection Core Logic	8	10	10
Data/Signal I/O	8	14	6
Total	40	50	30

(k gates)

Table 3.3.2 Summary of Gate Count of Detection Chip

These gate sizes were estimated based on IBM technical information believed to be reliable as of 9/02/97, but do not necessary represent the future product specification, and are subject to change.

3.4. Cost/Performance Analysis

In this section, the specification of detection hardware is shown to illustrate cost and effectiveness balance of IBM DataHiding^{TM} system. The analysis is based on the detection chip-1 and chip-2 described in section 3.3.

3.4.1 Summary of Proposed Detection Hardware Specification

CFP Section	Description	Requirement in CFP	Proposed Function	Note
A-1	Image quality	not noticeable to viewers	Yes	Video is viewed after MPEG and D/A conversion
A-2	Cost	low cost impact (<50k gates)	Yes	Refer to section 3.3
A-3	Detection	MPEG2 (PES)	Yes	MP@ML (all Main Profile)
A-3		MPEG2 program/transport string	Yes	Including MPEG de-multiplex
A-3		logical sector data	Yes	Designated format only
A-3		Uncompressed YUV (YCbCr)	(2)	With separate detection logic (chip-3)
A-4	'Single copy'	Capability to support 'single copy'	Yes	Will be described later
A-5	Reliability	Low false positive ratio	Yes	Refer to section 2.4
A-6	Reliability	False negative (50% protection)	Yes	Refer to section 2.4
A-7	Survivability	Color/Gamma Correction	Yes	
A-7		Digital Noise Reduction	Yes	Low pass filter
A-7		Aperture Correction	Yes	High pass filter (aperture enhancement)
A-7		MPEG2 compression	Yes	Above specified data ratio
A-7	Transmission	De-comp. > re-MPEG2	Yes	
A-7		Decompress (YcbCr)	(2)	With separate detection logic (chip-3)
A-11	Data payload	CCI + APS trigger bits	Yes	Transmission of APS to NTSC required
A-11		+ Control data (8-bits maximum)	Yes	Trade off (reliability and detection period)
A-11		+ private data embedding (32-bits)	(1)	Continuous detection not require
A-12	Embedding	Uncompressed video	Yes	Real-time w/ custom hardware
A-12		Software implementation	Yes	Refer to section 3.2
A-13	Data rate	Data rate equivalent to DVD	Yes	

CFP Section	Description	Requirement in CFP	Proposed Function	Note
B-1		Analog TV signal (NTSC)	(2)	With separate detection logic (chip-3)
B-2	Transformation	Geometrical transformation	(3)	Cropping, scaling
B-2/A-7		De-comp. > ANALOG > A/D	(2)	With separate detection logic (chip-3)
B-2/A-7		De-comp. > ANALOG > VHS > A/D	(2)	With separate detection logic (chip-3)
B-2/A-7		Analog image processing	(2)	NR, Echo Cancellation, 3D filter etc.
B-2/A-7		De-comp. > Analog > re-compress	(4)	Additional calibration logic required
B-2/A-7		> Analog > letter box conversion	(5)	480 lines to 360 lines conversion
B-2/A-7		> Analog > pan/scan conversion	(6)	720 to 540 pixel conversion
B-3	Detection period	Seconds rather than minutes	Yes	Refer to section 2.4
B-4	Security	Not easy to circumvent	Yes	Refer to section 2.6

Table 3.4.1 Summary of Proposed Detection Hardware Specification

Above table shows the list of the basic function requirement summarized and categorized from the design point of view. It is created to show specification of the embedding and detection system/hardware recommended proposed by IBM concerning the balance of effectiveness of the system and cost for the solution. The boxes marked “yes” in proposing spec. column indicates the items are covered by the recommending spec. and the boxes by numbers in parenthesis are the items that required some kind of trade-off that are discussed in the following section.

3.4.2 Discussions of trade-off

(1) 32bit private data embedding

If embedding and detection of this private information is done and used independently from the overall CCI, the additional cost can be minimized. In this case, the only trade off is the image degradation because we need to add another layer of information on the content. Also, the detection will be done off-line using independent software or custom hardware board. This information may or may not survive the video processing depending on the requirement. Again, the survivability of this additional information is a trade-off factor with the possible image degradation.

(2) Analog TV signal and uncompressed video signal detection

In order to satisfy this requirement, we need to use chip-3 as described in section 3.3.

(3) Robustness against geometrical transformation

Geometrical transformation includes cropping, rotating and zooming operations, etc. applied to the original frame images. The proposing specification, does not have robustness against those transformations. In order to satisfy this requirement, a restoration function is required to be added to the point prior to the detection to restore the video signal distortions caused by transformation. This will require more than 100k gates in our gate count estimation, and the additional embedding intensity or longer detection period will also be needed because of the higher distortion will be occur to the video content.

(4) Decompression - analog and re-compression

In the case where the second MPEG compression follows an analog stage for the video, the detection process begins with the de-compression step, in order to deal with the synchronization problem. Since the analog to digital conversion must always proceed the MPEG compression, we recommend placing the detection logic (chip-3) before the MPEG stage and detecting the embedded signal from the uncompressed digital image.

(5) Letterbox Conversion

This transformation occurs only when the image is decompressed and transmitted to analog TV signal domain. The detection from letter box converted image requires restoration of the decimated lines and, although it can be done without having full frame buffer, it will require a significant additional gates in the detection logic. Also, since the effective number of lines of the picture are decimated in the ratio 3/4, the image quality is significantly degraded and the detection reliability will be decreased. Therefore, this requirement would result in a higher embedding signal strength, which may cause visible artifacts in the image.

(6) Pan/Scan Conversion

This transformation also occurs only when the image is decompressed and transmitted to analog TV signal domain. Pan/Scan can be covered by applying additional embedding layer on top of the pre-embedding layer. This will introduce additional preparation burden and a reduction of the overall detection reliability, assuming that no perceptible image degradation is permitted.

3.5.Availability

IBM has been working on developing operational prototype encoders and decoders for the last few months. We anticipate that we will be able to meet the dates specified in the CSS license agreements, specifically the section “robustness of software de-scramble implementations”. However, the schedule for development, test and manufacture of prototype products is dependent upon requirements becoming stabilized and frozen by the CPTWG or the CSS technical committee. Thus, a detailed product schedule is not available at this time.

A more detailed representation of the DataHiding™ product schedule will be provided during the presentation of the solution at the CPTWG meetings.

4. Conclusion

4.1. Self-Evaluation Matrix

In this section, applicability of IBM DataHiding™ technology against the requirements listed in the DHSG CFP is summarized and discussed. Our definition of the mark is that “fully satisfied” means the technology fully comply with the requirement, “ substantially satisfied ” means that the IBM DataHiding™ technology complies with the requirement with some conditions, for example potential cost issue.

A.	Essential Requirements	Self-Evaluation	Reference Section
A-1.	Transparency	Fully satisfied	2.3
A-2.	Low cost digital detection	Fully satisfied	3.4
A-3.	Digital detection domain	Fully satisfied	2.5
A-4.	Generation copy control for one copy	Fully satisfied	3.1
A-5.	Low false positive detection	Fully satisfied	2.4
A-6.	Reliable detection	Fully satisfied	2.4
A-7.	WM will survive normal video processing in consumer use	Substantially satisfied	2.5
A-8.	Licensable under reasonable terms	Fully satisfied	4.2
A-9.	Export/Import	Fully satisfied	4.2
A-10.	Technical maturity	Fully satisfied	4.2
A-11.	Data payload	Fully satisfied	4.2
A-12.	Minimum impact on content preparation	Fully satisfied	4.2
A-13.	Data rate	Fully satisfied	4.2
B.	Desirable requirements		
B-1.	Detection in analog domain	Substantially satisfied	2.5.1
B-2.	Survivable in transformations	Substantially satisfied	3.4.2
B-3.	Detection period	Fully satisfied	2.5.2
B-4.	Not easy to render ineffective or circumvent	Fully satisfied	2.6
B-5.	Disclosure of technical approach	Fully satisfied	4.2

4.2. Discussion

4.2.1 Essential Requirements

A-1 Transparency Self-evaluation : Fully satisfied

According to the initial test results conducted with professional observers, there was no statistically significant degradation of the image quality caused by the IBM DataHiding™ process, see section 2.3. In addition, IBM DataHiding™ allows the content owner to control the embedding signal strength.

A-2 Low cost digital detection Self-evaluation : Fully Satisfied

The basic cost for the detection implementation is indicated by a gate count estimate for the detection logic hardware. In this proposal, the estimated size of the detection logic was less than 50k gates. (refer to section 3.3 for the cost analysis and the trade-off between the cost and the function)

A-3 Digital detection domain Self-evaluation : Fully satisfied

The proposed detection chip (chip-1 and chip-2) is designed to detect embedded data from MPEG data stream (compressed elementary data, program/transport string). Detection from uncompressed source data is done by chip-3. Please refer to section 2.5.

A-4 Generation copy control for one copy *Self-evaluation : Fully Satisfied*

Refer to section 3.1 and 3.3. Details of the method will be described later.

A-5 Low false positive detection Self-evaluation : Fully Satisfied

IBM DataHiding^{TM} technology offers extremely low rates for false positive detection (one error in 28,000 operation hours, refer to section 2.4 for detail). We believe that the false positive detection error rate should be low enough that the inclusion of the DataHiding™ capability into the device should have no significant effect on the overall reliability of operation, as perceived by the consumer. In the CFP, the specification called for one error occurs in only 400 hours of operation

A-6 Reliable detection Self-evaluation : Fully Satisfied

Refer to section 2.4

A-7 Watermark will survive normal video processing in consumer use

Self-evaluation : Substantially Satisfied

Data embedded by IBM DataHiding^{TM} technology would be detectable after all of the image processing suggested in the CFP, except that in certain cases (see section 3.4) the implementation might result in either potentially excessive logic gate counts or unacceptably long detection periods. The summarized specification considering the balance between the robustness, effectiveness and the cost are described and discussed in the of the section 3.4.

A-8 Licensable under reasonable terms *Self-evaluation : Fully Satisfied*

The solution for watermark encoding, which is intended to be used in content preparation process, will be provided by licensing the encoder technology to content owners for the purpose of marking their digital works. IBM plans to develop hardware and software to perform the embedding system functions and intends to provide education, training and service for such system solutions. The Embedding algorithm will also be licensable for embedding system developers on fair, reasonable, and non-discriminatory terms, accompanied by special NDA.

The IBM Motion Picture DataHiding (watermark) decoding method will be licensed for use in detecting the marks. It is also contemplated that IBM will license the specific circuit design to chip makers for inclusion into other semiconductor products. Licenses for design information will offered to all parties on fair, reasonable, and non-discriminatory terms under NDA. The Decoding Solution Offering will also cover watermark decode functions with encoding capability for DVD Recordable devices. The Business model IBM is planning will allow CE licensees to realize the lowest cost implementation.

Proprietary technologies included are the algorithm to embed and detect the watermark and the copy control information used for the copy protection and playback control.

A-9 Export/Import Control Self-evaluation : Fully Satisfied

There is no encryption algorithm involved in the IBM DataHiding^{TM} scheme, therefore it is not applicable to current export control applied to the encryption algorithms. Data embedded in the video stream by the IBM DataHiding^{TM} method is pre-defined copy control data and not intend to transmit arbitrary message from one party to another.

A-10 Technical Maturity Self-evaluation : Fully Satisfied

IBM has been conducting research in data hiding technology for application to the needs of copyright management for two years. The technology development specifically addressing the copy control and playback control of digital video application has been the main focus of the project for the last 14 months. The prototype software embedding and detection algorithm had been developed and was demonstrated at the end of 1996 to the CPTWG meeting. Since then the technology has been further refined by conducting joint evaluation tests with the assistance of a major motion picture studio using actual motion picture content.

A-11 Data payload Self-evaluation : Fully Satisfied

As described in the CFP document, the current proposal provides for a maximum of 8-bits of data for the real-time detection. The embedding of all 8-bit is done to every single frame. IBM DataHiding^{TM} also has a capability of embedding additional data into the same picture which contains the pre-embedded CCI. This additional embedding may require a trade-off with the embedding signal strength (or image quality) and the detection reliability, depending on the implementation requirement of these additional bits.

A-12 Minimum impact to content preparation Self-evaluation : Fully Satisfied

The IBM DataHiding^{TM} system will provide for real-time embedding, and the embedding process is independent from the MPEG compression stage in the overall digital production sequence.

A-13 Data rate Self-evaluation : Fully Satisfied

The current estimated maximum data rate is 16.6 Mbps, which exceeds the stated requirement (11.08 Mbps for DVD, 25 Mbps for ATV).

4.2.2 Desirable Requirements

B-1 Detection in analog domain Self-evaluation : Substantially satisfied

Detection from analog video signal has been tested and demonstrated at the CPTWG meetings. Detection in the analog domain requires digital to analog conversion as a pre-process. The cost of the detection is dependent on the implementation and required survivability (or reliability of detection from each specified transformation, such as letterbox conversion and pan/scan conversion, etc.. (see section 3.4.2)

B-2 Survivable in transformations Self-evaluation : Substantially satisfied

Refer to A-7 and section 3.4.2.

B-3 Detection period Self-evaluation : Fully Satisfied

In IBM DataHiding^{TM} technology, detection period depends on the residual signal level after the video processing and transmission process. The nominal detection period is within 10 seconds and maximum is less than one minute.

B-4 Not easy to render ineffective or circumvent Self-evaluation : Fully Satisfied

As long as the casual copying protection is consider, the minimum level of protection required for the system is to make the circumvention and devaluation of the system to be difficult. The level of security protection built into the IBM DataHiding^{TM} method is defined generally in Section 2.6. Our approach allows for the incorporation of the security features via an optimization of the total design, including the overall detection reliability, detection period and imperceptibility requirements. The details of the security features will be provided under non disclosure agreement and the need - to-know basis, in order to avoid unnecessary disclosure of the confidential information in the public domain.

B-5 Disclosure of technical approach Self-evaluation : Fully Satisfied

We plan to provide as much information as possible concerning the design approaches used in the IBM DataHiding^{TM} method. However, complete disclosure of the technical approach, particularly in the area of security design, may only be made available under restricted conditions.

Glossary

Terms	Explanation
APS trigger bit	2-bit information used for selection of multiple analog copy protection schemes provided by Macrovision™ APS
Copy Control	Verify the embedded CCI of the incoming contents at the recorder device and decide whether or not to proceed the recording process.
Copy Mark	Information carried by the content which is used to identify whether or not the content is an authorized copy.
Copy Control Information	data bit to be embedded into video content to represent the copy control status,
data hiding	General term to embed additional information into other medium such as image, video and audio in a manner that is invisible or inaudible, and robust to editing and signal transformations.
DataHiding^{TM}	A suite of data-hiding technologies developed by IBM that may be applied to still image, video and audio signals.
DVC	digital video cassette
Marked Image	Image that is been subjected to data embedding by using data -hiding technology.
One Generation Copy	An authorized copy, permitted under the scope of the overall copy protection system. A one generation copy, or 'single copy' may not itself be copied, and must be marked as such.
Playback Control	Detect the embedded CCI of the contents during playback within the playback device, and determine whether or not to proceed the playback process.

Reference Documents

1. Visual test standards CCIR-500
2. MPAA requirement delivered at CPTWG on Apr. 9, 1997.
3. CEMA requirement delivered at CPTWG on Apr. 9, 1997.
4. IBM data-hiding presentation from Jun. 1996 - Feb. 1997
5. Data Hiding for Copy Control, Alan Bell, presented at CPTWG, Aug. 19, 1997.

Contact Information

Contact in Japan

Norishige Morimoto
IBM Tokyo Research Laboratory,
1623-14, Shimotsuruma, Yamato-shi,
Kanagawa-ken, 242
Japan

TEL (+81)462-73-2562
FAX (+81)462-73-7413
noly@jp.ibm.com

Contact in the United States

Daniel Sullivan
Director of Licensing Development,
IBM Corporation
500 Columbus Avenue
Thronwood, NY 10594
U.S.A.

TEL 914-742-6278
FAX 914-742-6718
dansull@us.ibm.com