The Case for HCRC Verification
1 March, 2007

Over the years, it has become apparent that files in transfer, whether electronically or via physical media, have the potential for data corruption. Historically the optical disc industry has also observed that files left on a hard drive (not being transferred) have the potential for flipped bits.

In either case, plants are faced with the challenge of how to catch data corruption errors as early as possible in the manufacturing process, before the replica leaves the facility. In the past, plants have relied on bit-to-bit comparison, using the source image ("gold" master) as the reference for the replica. However, several factors reduce the value of the source image as a reference source, including:

1) Source images can be rather large and put a burden on the network to transfer the full source for a bit-to-bit comparison.
2) Security concerns may actually prevent the source image from being present on the plant floor for verification, creating inefficiencies in verification, by only allowing verification to occur at the location of the source image.
3) Since a source image is essentially a string of random hexadecimal characters, it contains no mechanism to validate itself. This fact reduces the value of the source image as a reference source.

To address item 1, several plants have already moved to utilizing CRCs, checksums or signatures, as a way to approximate the source image without needing to have the source present. CRCs and their variants are substantially smaller (less than 1% of the source image size) than the source itself, so they achieve the goal of reducing network burdens.

Plants have also looked to CRCs and variants to take care of item 3; however, traditional CRCs, checksums and signatures all contain the same problem as the source image, in that there is no 'self-referential' value for those items, so corruption within a CRC cannot be detected while doing a verification.

DCA's HCRC archive was designed specifically to be:

a) **a more robust reference** than the source image, since the HCRC file itself is self-validating (the HCRC archive contains CRCs for each sector and a hierarchal checksum over the collection of CRCs),
b) **a more specific reference** than traditional checksums or signatures, since the HCRC can pinpoint errors within the source image by sector address, replica radius point and file name, since the archive file is a collection of CRCs from each sector of the source,
c) **an easier reference** to use on the plant floor, since operators can verify the integrity of their data anywhere in the plant, without need for access to the original source data, and
d) **a failsafe reference** since the HCRC value is tied to the image it references by way of the DiscTag.

Technical Facts Regarding Bit-for-Bit, Checksums, Signatures & HCRCs

Traditional validation of content has been through a combination of bit-for-bit verification and checksums or signatures computed over the entire image. Bit-for-bit verification provided the user insight into the error location, and the CRC or signature served as a broad Go/No Go flag on the media. The advantage of using a HCRC check is that it not only provides Go/No Go validation, but also provides the sector location where the problem occurs.

Checksum or Signature over the entire image

Using a checksum or signature over the entire image takes a snapshot of the entire image; the snapshot value is then used to ensure the image integrity. This method has the advantage of being straightforward to calculate, and since the checksum represents the entire image, the value can be easily noted in paperwork and on the media. Since the method of taking the snapshot can be modified to allow for normal changes caused to the media during mastering (padding of sector lengths for DVD, postgap for CD), the snapshot allows for reasonable assurance of catching a bad piece of media.

There are three disadvantages to this method:

1) Errors in Calculation: As the size of the next generation images reaches 30 GB and higher, the greater the size of the image being calculated over, and the higher the risk of unintended error.
2) Entire Image must be Checked: Since the checksum is calculated over the entire image, you have to read the entire image to validate it. There is no method of checking part of the image, or only reviewing one piece of the media (in conjunction with a physical tester, for example).
3) No Insight into Error Location: The use of a checksum provides no insight into where in the image an error occurs.

Bit-for-Bit Verification

Bit-for-bit verification compares each bit of two images. This ensures there is no difference in the content between two images. The disadvantages of bit-for-bit verification are:

1) Requires Access to Both Images at Testing Site: Bit-for-bit verification requires access to both images at the workstation performing the testing. If one image is located on another system or a network server, bit-for-bit requires networking resources to access the content. If the content is located in another facility or another part of the facility not connected to the workstation running the verification, then there is no means to perform the bit-for-bit without carrying the physical media to the workstation.
2) Network bandwidth requirements: Bit-for-bit places high requirements on the network. For example, DVD bit-to-bit comparison requires handling two 5GB image files. Using bit-for-bit results in an increased network server investment that must be made for network mastering or face the inevitable shortening of the life of network systems already in place.
3) Content testing time limited over network: When comparing files on a network drive, the larger files (that is, the image itself) required by bit-for-bit will be limited by your network speed.
4) Security of customer IP: Bit-for-bit requires a copy of the customer's content to be made available for testing in replication. In the case of CSS jobs, un-encrypted content has to be made available for comparison against the replica. That means customer content will be 'open and unprotected' on the facility floor. Many organizations do not allow this for IP protection; replicas have to be taken back to the premastering area for testing.

The HCRC Resolution

DCA's HCRC or Hierarchical CRC moves beyond current verification methods, taking advantage of the positive aspects of both, while avoiding the disadvantages inherent in each method.

Taking advantage of the checksum or signature method, DCA's HCRC takes a snapshot not only of the entire image, but of each sector of the image. The individual sector snapshots are then collected and saved into a single HCRC file saved with the image. A second copy of the image is not required for verification, since the saved HCRC file is used to represent the second copy of the image.

Taking advantage of the bit-for-bit method when the image is compared against the HCRC, DCA products will check each sector's CRC and if a problem is found, it will report the specific sector where that problem occurred.

Hierarchical		1	2	3	4
CRC	1	2	3	4	5
	2	6	7	8	9
	3	1	2	3	4
	4	5	6	7	8

Cell	Original Value
1x1	2
1x2	3
1x3	4
1x4	5
2x1	6
2x2	7
2x3	8
2x4	9
3x1	1
3x2	2
3x3	3
3x4	4
4x1	5
4x2	6
4x3	7
4x4	8

Hierarchical		1	2	3	4
CRC	1	2	3	4	5
	2	6	6	9	9
	3	1	2	3	4
	4	5	7	6	8

Cell	Original Value	Recalculated or Compare Value
1x1	2	2
1x2	3	3
1x3	4	4
1x4	5	5
2x1	6	6
2x2	7	6
2x3	8	9
2x4	9	9
3x1	1	1
3x2	2	2
3x3	3	3
3x4	4	4
4x1	5	5
4x2	6	7
4x3	7	6
4x4	8	8

In the above example, a specific value has been obtained for each cell or position. Instead of calculating a total from those values, the entire table is kept. Then when the errors are entered into the array, they are easily caught by the HCRC – and the position of the error noted, as well.

The HCRC thereby fulfills the roles of both methods. As a type of CRC, the HCRC provides self-referential validation. That is, it is a simple means to tell if an image is the same as the one that came into the facility. It also fulfills the role of bit-for-bit comparison by distinguishing between two images or two versions of the same image and notes or specifies which sector(s) have the error.

Overcoming the Disadvantages of the Other Methods

Issue	Method	HCRC Resolution
Errors in Calculation	Checksum or Signature	Each sector is calculated against the HCRC value, thereby limiting errors in the calculation only to the specific sector, not the entire image.
Entire Image Must Be Checked	Checksum or Signature	Since the sectors are each individually represented by the HCRC, a range of sectors or a location on the disc can be verified without needing to check the entire image.
No Insight Into Error Location	Checksum or Signature	HCRC pinpoints mis-compares by both sector address and radius points, allowing for more detailed analysis of your loading, LBR output, stampers and replicas.
Network Bandwidth Requirements	Bit-for-bit	Using an HCRC allows for self-validating data transfers from point to point with minimal overhead, as opposed to requiring double bandwidth for transferring back, then performing a read back after transfer to ensure it is OK.
Content Testing Time Limited Over Network	Bit-for-bit	Since an HCRC is only a fraction of the size of the original customer content, as the density or volume of media increases, you will not have to expand your mastering network to perform analysis.
Security of Customer IP	Bit-for-bit	Since there is no way to change an HCRC back into the original content, it is completely risk free to use the HCRC on the facility floor to compare replicas - without allowing content outside of the mastering Network.

Case Study – Data Corruption Caught Just Prior to Mastering

Since DiscTag Enabled formatters can automatically verify HCRC on images as they are being streamed to the encoder, the following scenario has become something that DiscTag replication facilities can rely on being caught.

A DiscTag plant received a large volume order from a customer with a request that they keep the source image, in the event of any additional volume being necessary. As it happens, in this case, the customer called back 30 days after the first run with a request for additional production. The current set of stampers was insufficient to fulfill the re-order volume, so new mastering was ordered.

The plant pulled the original source image, along with their original HCRC value, which was stored on their metadata server. During mastering, the HCRC verification reported a mismatch at sector 41EF6h. The plant informed the customer of the corruption, who sent another copy of the source image. A comparison of the new source image with the existing image at the plant revealed that HCRC had, in fact, correctly located the problem at 41EF6h.

Had the plant used bit-to-bit against the source image or generated a new checksum on the second order, there would have been no errors identified on all mastering and discs when, in fact, the discs would have been incorrect. **In this case, the use of the original HCRC value (from the original, uncorrupted source), prevented the plant from shipping an incorrect re-order run.**

> The HCRC archive is not only failsafe, since its' self-validating mechanism ensures that it is the most accurate reference for a facility, but it also, with the DiscTag, is automatically tied to the image, so a plant is always assured that the image is always verified with the correct reference.

Case Study – Physical Problem 'Located' By HCRC

In April 2006, a DiscTag replication facility was starting to bring their new HD DVD process up from scratch, using a new LBR and existing replication lines.

During the first few test cuts, HCRC verification consistently pointed out mismatches at radius 31.25mm. The radius location provided was an approximate calculation done by the DCA software, using the sector addresses that mismatched. After investigation with the microscope and DOM, it was found that **the HCRC was correctly pointing out a specific radius on the disc that was failing due to a physical defect on the replication line**.

> HCRC is a quick and reliable way to tune in physical processes and can be a key driver in helping to bring up new formats and processes quickly.

Case Study – False Mismatch Reported By Bit-to-Bit

In February 2007, a DiscTag replication facility found a scenario wherein the HCRC ended up catching an error that the standard bit-to-bit compare missed.

1) The plant received an image via WAM!Net
2) The image was collected to the M:\ drive
3) An operator used DCA's pre-mastering tools to transfer and analyze the incoming image, at which time an HCRC was created against the M:\ drive source. The source image sector 327D7h contained a starting value of 0002 and the HCRC reflected the value correctly.
4) After the transfer and analysis, a copy of the image was placed on the S:\ drive for mastering.
5) After replica creation, an HCRC comparison was made with no errors.
6) As a precaution, the operator compared the replica against the M:\ drive source, and found a bit-to-bit comparison error at sector 327D7h.

After all investigation, it was determined that between the time of the original transfer from M:\ to S:\ and the time of replica verification, a bit had been flipped from 2 to 0 in the original image at sector 327D7h.

In this case, **the bit-to-bit comparison actually yielded a false mismatch**, since it flagged a mis-compare against a 'bad' source (post bit-flip). **The HCRC verification, however, was proven to be valid** in verifying the replica as a correct representation of the 'good' source (pre-bit flip), **as the HCRC self-validated its' collection of CRCs using the internal checksum**. Simply, the replica and the original (pre-bit flip) source matched fine, but **the source after the bit flip ceased to be a valid comparison reference.**

> HCRC can be a tremendous help for plants faced with a false mismatch, as it can save the costs of re-cutting a run of discs that are flagged incorrectly due to a corrupted source image.

Ready for 3G Optical Discs

HCRC is ready for the next generation of optical discs, whether HD DVD or Blu-ray. Its size requirements are ready regardless of how large the density becomes – 30GB, 50GB or even higher. HCRC offers an elegant solution for AACS copy protected images now. Since the pre-AACS HCRC is used to validate your data during the AACS encryption process, and then, immediately, a new HCRC on the post-encrypted content is generated, you have the best assurance that your encrypted data matches the pre-encrypted data. And, when AACS provides for complete decryption, including all segments, for verification, HCRC allows you to use the pre-AACS HCRC value to be used to validate the replica, providing complete assurance.

Conclusion

When you utilize HCRC throughout your organization, it serves as a ready reference throughout your replication facility, ensuring that nothing goes wrong during the entire process. Bottom line: while Checksum or signatures are good, the HCRC is outstanding. And with DCA's unique DiscTag providing a link to the HCRC and associated metadata for each title, HCRC verification is automatic for your operators (no more guessing the correct Title/Customer Name for the replica you're holding, no more

looking for where the original image data exists, no more data entry problems, no more version comparison issues). HCRC is a vital link in the DiscTag Enabled workflow chain.

Finally, the HCRC is better because it allows the verification process to move up stream, even into content creation. Authoring can generate a HCRC prior to sending the content to the replication facility. During the processing of the content, that HCRC remains with it, automatically tied to the image with the DiscTag, and always serving as the reference validation check on the content.

Only DiscTag Enabled products allow you to take advantage of HCRC during loading and pre-mastering. In addition, only DiscTag Enabled mastering products (such as DCA MIS V8, 8.5 and Pro) allow you to take advantage of HCRC during mastering.

For more information contact your Regional Sales Manager

Americas & Asia	*Europe*	*Japan*
Fred Perez	Chris Vangramberen	Nozomu Hayatsu
Fredp@dcainc.com	chrisv@dcainc.com	nozomu@dcainc.com
Telephone:	Telephone:	Telephone:
925-426-9948	+49-6021-45900-0	+81-3-3402-5631
Fax:	Fax:	Fax:
240-248-1105	+49-6021-45900-29	+81-3-3402-5615