ImageSignature

ImageSignature v2.0 is a self-contained, highly-reliable method for tracking and verifying BD and HD images as they move through the disc manufacturing process – from authoring to final QC.

Enhanced Capability

ImageSignature Version 2.0 incorporates a new structure to better handle BD and HD processes. It provides fast layer checking capability, self-verification, and a simpler manual signature input and display. Newer versions of EclipseSuite BD and EclipseSuite HD will automatically incorporate this new signature structure.

One Signature – Authoring to Replication

A key characteristic of ImageSignature is that the same signature can be derived from an image at any point in the process. Any time an image is tested with any of the EclipseSuite programs, the signature is validated and reported. The image signature validation is always performed on unencrypted or decrypted data. When decryption is required, the process is fast and automatic.

Simpler User Interface

EclipseSuite BD and HD present the last 6 bytes (12 characters) of the 20-byte signature value to the user. This easily recognizable short form of the signature can be entered into ImageVerify when manual signature entry is necessary.
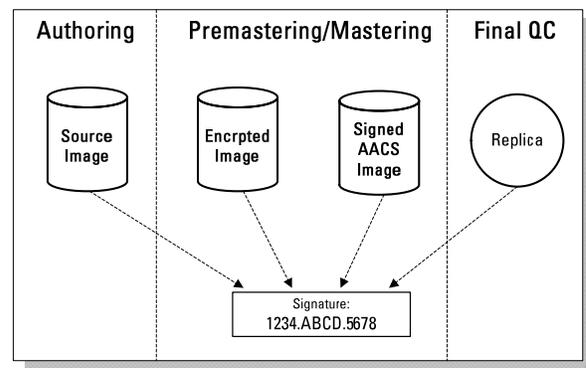
Quick Layer Check

The primary signature can be used to detect layer mismatches, but only after the entire image is read. However, the new Layer Match Hash can report a layer mismatch almost instantly. The Layer Match Hash is created from specific, limited data from each layer that is easily and quickly accessed.

Self-verification

Since every ImageSignature 2.0 disc has its signature stored on it, ImageVerify can use that signature to validate the image integrity. This self-verification process is limited and should be used cautiously since it is somewhat self-fulfilling. As the signature and data always stay together in the CMF, if the data is correct, the signature should always match. The self-verify should trigger a failure only in cases where the data is not correctly transferred to the glass master (e.g. corrupted by the formatter, laser dropout, etc.) or if the replica cannot be read accurately by the drive. It will not detect image mixing problems (e.g. the mastering operator chose the wrong image) and should only be used if replicas are checked for mixing elsewhere in the process.

SPECIFICATION – VERSION 2.0 SIGNATURE FOR BD AND HD

Signature Values

In order to create a signature that remains constant through the entire manufacturing process, it is necessary to exclude certain data from the signature calculation that is known to change as the image moves through encryption and mastering. It is important to note that the excluded data does not include user data and is checked by other means during the image analysis, so image integrity is guaranteed.

ImageSignature 2.0 utilizes up to three internal 20-byte hash values in addition to the primary signature:

- **Signature**– a digest of the disc information and the layer 0 and layer 1 (in case of dual layer images)
- **Layer 0 hash**– includes sector addresses (using PSN) and 2048 bytes of every user data sector
- **Layer 1 hash**– includes sector addresses (using PSN) and 2048 bytes of every user data sector
- **Layer Match hash**– includes specific data from 32 sectors of each layer in case of dual layer images for quick layer bonding check.

  Note: L1 Hash and the Layer Match Hash are not created for a single-layer image

```
[Signature]
Version=2.0
SignatureInfo=3C,2,0,2,2,1,1,30000,5705C0,A5FA40,52F8A0,1,
56FF73,2B95795CC,52F43C,298EDB0F0
Signature=DA193FA02296901F3957CB99482299A6F114486D
HashL0=5103BC4881C068549EB780CA8CD526AF275DB5CE
HashLM=2D02E8F9724C2F7D395BDD6F69E661423E629AFD
HashL1=E3C2CD0F218779A202B55FBEC0A936C80E0D72B2

[LogfileName]
*ActualFileName.esg*

[SignatureDisplay]
*99A6.F114.486D*
```

ImageSignature File Example

ImageVerify Methods Using Signature:

- **Verify-after-Copy**
  - ImageCopy calculates signature, encrypts image, and copies to an output folder
  - ImageVerify (running inside ImageCopy) decrypts and compares output image to source signature file (same as *Verification to a signature file* below)
- **Verification to a Signature File**
  - Signature information is read from signature file.
  - If present, signature information is compared to disc information. A mismatch is shown immediately.
  - Quick layer check is performed for dual layer images. A mismatch is shown immediately in most cases.
  - The replica is decrypted to calculate layer 0 and layer 1 (if dual layer) hashes. A mismatch is shown as soon as each layer finishes processing.
  - The signature value gets calculated from the previous information. A mismatch is shown at the end of the process.
- **Verification to a Signature Value**
  - User enters the display formatted signature value (12 characters)
  - The replica is decrypted to calculate layer 0 and layer 1 (if dual layer) hashes.
  - The signature value gets calculated from the previous information. A mismatch is shown at the end of the process.
- **Self-Verification**
  - Signature information is read from disc control data (HD) or PIC data (BD).
  - Signature information is compared to disc information. A mismatch is shown right away.
  - Quick layer check is performed if dual layer. A mismatch is shown immediately in most cases.
  - The replica is decrypted to calculate layer 0 and layer 1 (if dual layer) hashes. A mismatch is shown as soon as each layer finishes processing.
  - The signature value gets calculated from the previous information. A mismatch is shown at the end of the process.

  Caution: This will test the integrity of the data, but will not detect if the image is correct.