

InDorse Image Assurance (InDIA)

Protect and Secure all Multimedia Files

Protecting classified data from leaking (intentionally or unintentionally) into the wrong hands has always been a challenge. Organizations deal with millions of multimedia files (digital animation, photos, x-Rays, video) that need to be secured and classified, but find it difficult to do.

Two security breaches underscore the difficulty organizations have in securing multimedia files:

1. May 2009 - The U.S. federal government mistakenly made public a 266-page report, its pages marked "highly confidential," that gives detailed information about hundreds of the nation's civilian nuclear sites and programs, **including maps showing the precise locations of stockpiles of fuel for nuclear weapons**. The report was intended for the International Atomic Energy Agency for purposes of nuclear transparency, but was not intended for consumption by the general public.
2. June 2009 - Leaks were plentiful ahead of the Sony keynote at E3. Before the show even kicked off, details and an image of the PSP GO showed up online and trailers for upcoming Sony games *Metal Gear Solid: Peace Walker* and *The Last Guardian* were leaked. Sony Computer Entertainment America head Jack Tretton was not happy about the leaks and feels that they stole some of the thunder from the Sony E3 announcements. Tretton told CNBC, "People don't respect confidentiality in this industry. It's tough enough to keep a secret within your own company, much less when you speak to third parties."

Introducing InDorse Image Assurance (InDIA)

InDIA automatically identifies, groups and embeds imperceptible corporate security policies onto any picture or video.

Via the customization of an invisible, or visible, Digimarc digital watermark (see Figure 1) placed on any image, InDIA is able view any multimedia file's metadata and search all file storage devices such as WebDAV, Windows File Share, SharePoint, NFS, Novell and Legacy devices, to locate and group images according to predetermined criteria.



Figure 1

Securing Digital Assets

While DLP/DRM and IRM products can have their use, they are not capable of being readily applied to anything other than what they were intended for. Whereas, InDorse can be applied as a product or a service to meet applications ranging from:

- Context-Based Security to Compliance
- Governance and Audit
- Configuration or Knowledge Management.



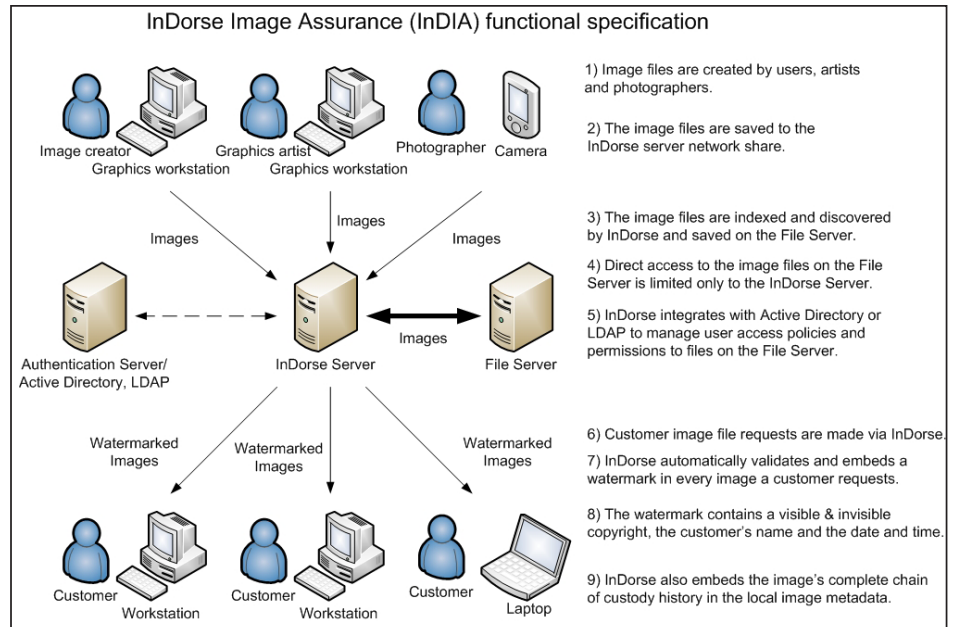
Support

InDIA Includes Support For The Following Image Files:

- BMP
- JPG
- PCT
- PCX
- PNG
- PSD
- TGA
- TIF

InDIA Image Data Formats Supported:

- Grayscale
- BGR
- RGB
- LAB
- CMYK
- CMYK Inverted
- ARGB, RGBA, BGRA



Once the images are logically grouped or clustered together, additional compliance or corporate policies may be seamlessly embedded into the metadata by InDorse Tag™. The tag follows the image where InDorse Protect™ takes over to automatically administer security policies prior to an end user opening the file. A complete audit trail can also be conducted showing who viewed, manipulated, forwarded or stored an image to a different server.

People often do not think twice before publicizing pictures. InDIA's foundation is predicated on this human behavior and counteracts it by embedding the images with corporate policies that dictate the image's use. The end user simply conducts "business as usual" and via the metadata, the image will inform the end user if they can view, download, file to another location or forward. All activity is tracked and reported back to the administrator.

