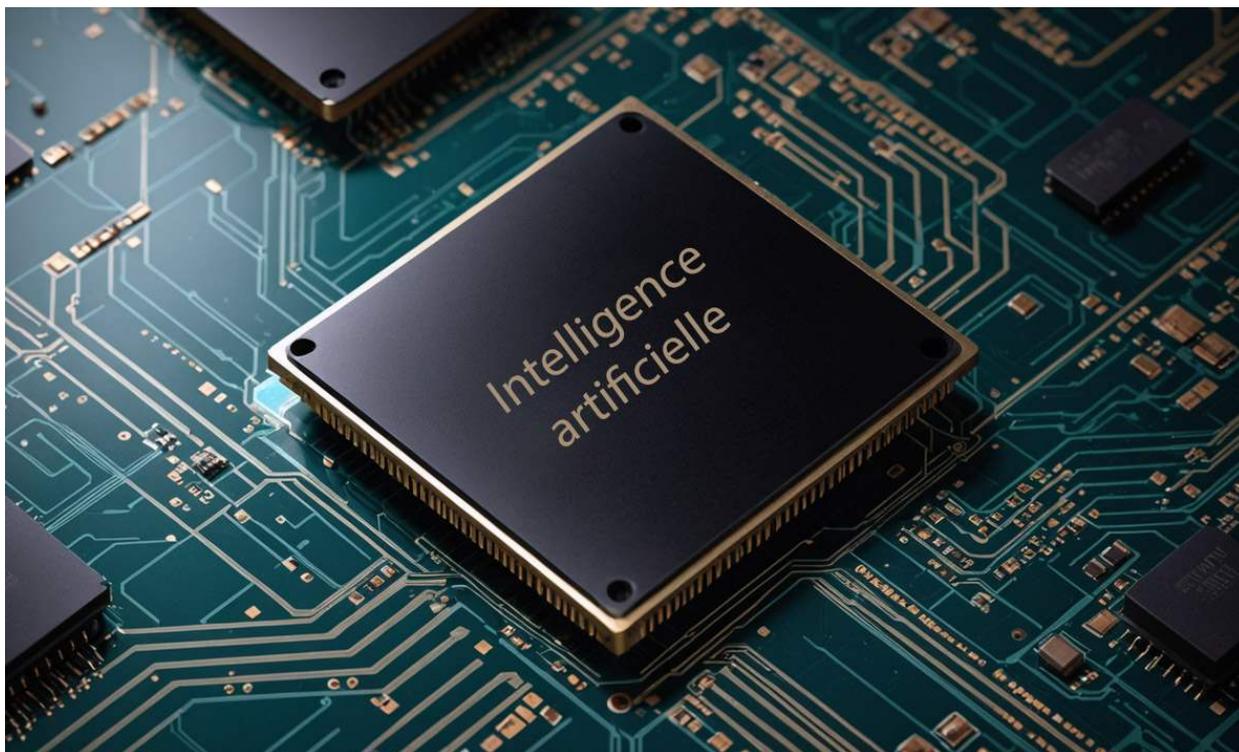


Concours photographiques de l'ACAP : Nouvelles normes d'authentification de l'IA



Résumé

L'Association canadienne de l'art photographique (l'ACAP) met en œuvre de nouvelles normes de vérification des images artificielles afin de relever les défis que posent les outils d'IA dans les concours de photographie.

À compter du 16 septembre 2025, nous introduirons de nouvelles normes d'authentification par IA, dont la mise en œuvre débutera le 1er janvier 2026. Ce délai de 108 jours donne aux photographes le temps d'examiner les détails fournis et d'apporter des ajustements à leurs flux de travail de traitement des photos.

Le défi : L'IA dans les concours de photographie

L'édition de photos par l'IA a révolutionné la photographie, mais elle a également créé une certaine confusion dans les concours de photographie. Alors que certains outils d'IA améliorent les éléments d'image existants de manière appropriée, d'autres outils d'IA sont interdits parce qu'ils génèrent un contenu synthétique qui n'a pas été capturé à l'origine par le photographe.

Distinction importante : Ces nouvelles normes s'appliquent spécifiquement aux photographies qui ont été modifiées à l'aide d'outils d'amélioration de l'IA, et non aux images entièrement générées par l'IA et créées à partir d'invites textuelles. Les images

entièrement générées par l'IA (celles créées entièrement à partir de textes sans photographie originale) sont interdites dans les concours l'ACAP.

Actuellement, la communauté des photographes est confrontée à plusieurs problèmes :

- Il n'existe pas de lignes directrices unifiées sur les outils d'IA acceptables pour les concours ;
- une application incohérente de ces directives d'un concours à l'autre ;
- Une technologie de détection de l'IA qui ne peut pas suivre l'évolution des capacités de l'IA ;
- une incertitude croissante parmi les photographes quant aux outils d'IA qui sont acceptables pour les concours.

Notre solution : Certificats de contenu (normes C2PA)

L'ACAP adopte les normes de la Coalition for Content Provenance and Authenticity (C2PA) pour assurer une vérification fiable des images de compétition. La C2PA est un consortium international qui élabore des normes techniques ouvertes et libres de droits pour le suivi de l'authenticité des contenus numériques.

À l'heure actuelle, 5 000 entreprises engagées soutiennent la norme C2PA, parmi lesquelles :

Adobe	AI Labs	Amazon
American Society of media Photographers		
Associated Press	Association of Photographers (UK)	
BBC	Canon	CBC
Getty Images	Globe and Mail	Google
Intel	Leica	LinedIn
Meta	Microsoft	Nikon
Open AI	Sony	Reuters
Stern		

Fonctionnement des Certificats de contenu

Certificats de contenu intègrent un manifeste de métadonnées signé, écrit dans le fichier de métadonnées au cours du processus d'exportation, et enregistrent les détails de provenance suivants :

- Le créateur original et les détails de la capture ;
- Appareil photo ou logiciel de création/édition utilisé ;
- Historique complet de l'édition avec horodatage ;
- Tous les outils d'intelligence artificielle utilisés pendant le post-traitement ;
- Chaîne de contrôle complète, de la création à la soumission.

Les métadonnées sécurisées sont intégrées au fichier image et peuvent être authentifiées à l'aide de l'outil de vérification disponible sur contentcredentials.org/verify. Certificats de contenu peut détecter toute modification non autorisée de ces métadonnées.

Lignes directrices pour la mise en œuvre par logiciel

Applications Adobe (Photoshop et Lightroom)

Nous avons créé sept (7) documents qui décrivent les outils d'IA acceptables et ceux qui ne sont pas autorisés. Ces documents précisent également les moyens spécifiques par lesquels les images doivent être enregistrées ou exportées afin de garantir la conservation des métadonnées de l'image.

Afin de soutenir la nouvelle norme d'authentification IA et les nouvelles exigences en matière de références de contenu, nous avons créé cinq pièges IA - Protéger votre éligibilité au concours, des directives destinées aux photographes qui participent à notre concours. Ces directives précisent quelles fonctionnalités IA sont acceptables dans les soumissions et lesquelles ne le sont pas :

- Adobe Photoshop – ([English](#)) ([French](#))
- Lightroom Desktop – ([English](#)) ([French](#))
- Lightroom Classic - ([English](#)) ([French](#))
- Lightroom Mobile - ([English](#)) ([French](#))
- Luminar Neo – ([English](#)) ([French](#))
- ON1 Photo RAW – ([English](#)) ([French](#))
- Topaz Labs – ([English](#)) ([French](#))

Processus de vérification

Tous les photographes et clubs photo peuvent évaluer leurs images afin de déterminer si elles ont été enregistrées en tant qu'images C2PA et si elles contiennent des caractéristiques générées par l'IA.

Les étapes suivantes décrivent comment vérifier une image à l'aide du site web contentcredential.org/verify.

Étape 1 : Visitez contentcredentials.org/verify

Étape 2 : Téléchargez ou glissez-déposez votre image

Étape 3 : Consultez le rapport d'authenticité complet

Le système de vérification accepte les formats de fichiers suivants : AVI, DNG, HEIC, HEIF, JPEG, PNG, SVG, TIFF, WebP

Badgé d'accréditation de contenu

AI-generative detected

Dernière personne ayant signé ou modifié le contenu avec de nouvelles informations d'identification

Résumé de l'édition

Ressources graphiques contribuant à l'image finale

Remarque : si une image de référence de contenu précédente a été utilisée pour créer la nouvelle image, l'image d'origine apparaîtra dans la case Ingrédients avec un CR dans le coin supérieur gauche .

Figure 1 - Capture d'écran de l'analyse par le site web Content Credential d'une image contenant au moins un élément généré par l'IA.

Ce que montre la vérification

- Source originale et date de création
- Logiciel et équipement utilisés
- Historique complet des modifications
- Utilisation d'outils d'intelligence artificielle (le cas échéant)
- Alertes de détection d'altération

Dans la fenêtre qui s'affiche sur contentcredentials.org/verify, une image C2PA enregistrée contiendra le code PIN Content Credential qui apparaîtra dans le coin supérieur gauche de l'image.

Voici un exemple de code PIN Content Credential.



Figure 2 - Exemple de l'épingle Content Credential.

Protocoles de détection et de vérification de l'IA

L'ACAP utilise le site web Hive AI Detection, qui est un outil de classification de l'IA, pour identifier les images susceptibles d'avoir été générées par l'IA.

Les représentants des clubs photo qui soupçonnent qu'une image peut être entièrement générée par l'IA peuvent la soumettre au directeur de la compétition pour analyse. L'image sera traitée par Hive AI Detection et les résultats seront renvoyés au représentant qui en a fait la demande.

Toutes les images susceptibles de gagner le concours sont soumises à un processus complet de vérification et d'authentification par le biais d'une analyse des références de contenu et d'une détection de l'intelligence artificielle. Toute image qui échoue à ces étapes de vérification sera disqualifiée du concours.

Avantages du C2PA pour la communauté des photographes

Pour les photographes individuels

- **Confiance et authentification** : Vérifie que vos images répondent aux normes du concours avant de les soumettre, évitant ainsi toute disqualification due à une utilisation inacceptable de l'IA.
- **Protection des droits d'auteur** : Les informations sur le créateur et les horodatages intégrés renforcent les revendications de droits d'auteur et garantissent une attribution correcte.
- **Reconnaissance professionnelle** : Des plateformes telles que LinkedIn reconnaissent les références de contenu, ce qui renforce la crédibilité professionnelle.

Pour les clubs de photographie

- **Vérification simplifiée** : Vérifiez l'authenticité des images sur le site Web Content Credentials avant de les soumettre à des concours externes (il n'est pas nécessaire de disposer d'une expertise spécialisée dans la détection de l'IA).

Remarque : pour l'instant, seules les images traitées dans Photoshop et Lightroom sont prises en compte.

Pour les organisateurs de concours

- **Vérification transparente** : Les organisateurs peuvent accéder à l'historique complet de l'image, y compris les détails de la capture, la chronologie de l'édition et l'utilisation des outils d'IA.
- **Traitement efficace** : La vérification automatisée de l'authenticité réduit le temps d'examen manuel tout en garantissant la conformité avec les règles de la compétition.
- **Détection des altérations** : Les fonctions de sécurité intégrées identifient les modifications non autorisées des métadonnées et les tentatives de manipulation du contenu.

Calendrier de mise en œuvre

Phase 1 : Annonce - 16 septembre 2025

- Publication de normes détaillées et de lignes directrices pour la mise en œuvre des certificats de contenu
- Fournir des guides de protection « Sept pièges » pour aider les photographes à éviter les problèmes d'éligibilité les plus courants.
- Encourager les membres à demander des éclaircissements au directeur des concours.
- Publication d'une mise à jour des critères d'édition des concours en vue de la mise en œuvre en 2026.

Phase 2 : Mise en œuvre complète - 1er janvier 2026

Exigence spécifique à Adobe (à compter du 1er janvier 2026) :

Les photographes qui retouchent leurs images dans Adobe Photoshop ou Lightroom sont invités à activer la fonction Certificats de contenu.

Pourquoi cette exigence est-elle nécessaire ? Les fonctionnalités Firefly AI d'Adobe n'enregistrent pas automatiquement l'utilisation d'outils de génération par IA dans les métadonnées standard, sauf si Certificats de contenu sont activées. Sans ces informations, il est impossible de vérifier si des outils de génération par IA interdits ont été utilisés, ce qui compromet l'intégrité du concours.

Toutes les autres applications de post-traitement :

Les images doivent être enregistrées ou exportées avec toutes les métadonnées contenant l'historique de l'appareil photo et des modifications, ce qui permet une vérification sans exigence supplémentaire en matière d'informations d'identification du contenu.

Pour commencer

1. **Examiner les lignes directrices** : Téléchargez le guide approprié pour votre logiciel d'édition à partir du site web de l'ACAP ;
2. **Mettre à jour le flux de travail** : Mettre en œuvre l'activation des certificats de contenu ou les protocoles de conservation des métadonnées ;
3. **Testez la vérification** : Utilisez contentcredentials.org/verify pour vérifier vos images traitées ;
4. **Pratiquer la soumission** : Assurez-vous que vos images répondent aux nouvelles normes avant la date limite du 1er janvier 2026.

Bêta-test" de la mise à jour des références de contenu

Le 2 septembre 2025, Adobe a annoncé de nouvelles fonctionnalités bêta pour ses normes Content Credential, visant à renforcer la confiance numérique, la transparence et le contrôle des créateurs dans l'IA générative et les flux de travail multimédias complexes.

Les principales nouveautés incluses dans le test bêta sont les suivantes :

- La fonction d'attribution aux créateurs vérifiés permet aux créateurs d'intégrer leurs références professionnelles authentifiées sur LinkedIn, Behance, Instagram et X dans leurs œuvres numériques, créant ainsi un lien direct entre leur identité vérifiée et leur production créative.
- La version bêta vous permet d'ajouter des références de contenu à un maximum de 50 images JPG ou PNG à la fois. Les prochaines mises à jour prendront en charge des fichiers plus volumineux et des formats supplémentaires comme la vidéo et l'audio.
- Les créateurs peuvent désormais définir des préférences quant à l'utilisation de leur contenu pour entraîner des modèles d'intelligence artificielle. Cette nouvelle

fonctionnalité permet de protéger leurs choix et pourrait s'aligner sur les réglementations internationales à venir concernant les options de refus d'entraînement à l'IA. (<https://contentauthenticity.adobe.com/>)

- Ces identifiants fonctionnent comme une empreinte numérique permanente qui reste associée à votre contenu quoi qu'il arrive - que quelqu'un le modifie, fasse des captures d'écran ou le partage. Cela permet de créer un historique complet montrant comment votre contenu a changé de mains et a été modifié au fil du temps.
- Des outils de navigation intégrés permettent à quiconque de vérifier comment le contenu a été modifié au fil du temps et de voir quelles informations d'identification ont été utilisées pour le créer.
- De nouveaux outils de filigrane et de cryptage sont en cours de développement pour mieux protéger les images numériques, en utilisant à la fois des marqueurs d'arrière-plan invisibles et des signaux d'authenticité visibles pour vérifier leur origine.
- Les dernières mises à jour techniques de la C2PA améliorent le formatage des manifestes, la gestion des flux de travail, les fonctions d'horodatage et les capacités étendues en matière de métadonnées.

Ces mises à jour visent à rendre la provenance des contenus plus robuste et plus conviviale pour les professionnels de la création, les organismes de presse et les communautés photographiques.

Commentaires de clôture

Les nouvelles normes d'authentification de l'IA de l'ACAP contribueront à préserver l'intégrité de nos concours en fournissant des directives claires sur l'utilisation acceptable des outils d'IA tout en maintenant la distinction entre la photographie capturée et le contenu synthétique.

Au fur et à mesure que les normes d'authentification du contenu et les applications de post-traitement seront mises à jour, nous communiquerons ces changements à nos membres en temps opportun. La mise en œuvre de ces nouveaux flux de travail standard aura un impact significatif sur de nombreux photographes, et nous vous demandons d'accepter ces normes dans votre intérêt et dans celui de l'ACAP.

Si vous avez des questions ou des préoccupations à ce sujet, n'hésitez pas à envoyer un courriel au rédacteur à l'adresse suivante competitions@capacanada.ca

Sheldon Boles – FACAP
Directeur des concours de l'ACAP