Names of testers:

Ying Fei Zang (261054638) ying.zang@mail.mcgill.ca

YunShan Nong (261055472) yunshan.nong@mail.mcgill.ca

Yu Tong Hu (261051311) yu.tong.hu@mail.mcgill.ca

Date: 09-Apr-2024

Title: Software Validation of “The GENERAL”

Overview:

This report presents some potential test objectives for The GENERAL as described in The GENERAL software requirement specification. Guiding Principles - C2PA

The type of potential test objectives presented include Capabilities, Failure Modes, Usage Scenarios and Quality Factors related to performance.

A short summary of each potential test objective is included. Each summary will identify risks being studied, variables being manipulated, variables being observed and the test design technique which is proposed to implement the test objectives.

The paper will also describe how regression testing could be implemented as part of the development process to help determine if changes to The GENERAL code base accidentally inject regression bugs.

Capability Test Objectives

1) Test Objective (Capability)	Confirm The GENERAL can support *all* common asset and content file formats.
Risk being studied	Build confidence for existing customers to confirm that they can perform typical transactions with The GENERAL
Variables which will be manipulated	All entries of common asset and file formats Number of trials
Variables which will be observed	Generated files The GENERAL production log files.
Test design approach	Pareto analysis will be used to identify the most common format

2) Test Objective (Capability)	Confirm The GENERAL allows for flexibility in whether C2PA data is stored directly in asset files or hosted in cloud-accessible storage.
Risk being studied	Confirms that The GENERAL is not storing data in other platforms for privacy purposes and to build trust with current customers
Variables which will be manipulated	Type of files Generated files
Variables which will be observed	The GENERAL production log files Cloud storage or Asset files
Test design approach	Boundary value analysis helps to ensure the system's reliability, compatibility, and

	usability across a range of scenarios and configurations

3) Test Objective (Capability)	Confirm The GENERAL manifest can be defined with a pairwise complete set of all input parameter options.
Risk being studied	Confirm that all values of all variables can be successfully entered in a manifest in combination with all values of each other variable at least once.
Variables which will be manipulated	Type of files: Size: Type of editings: Data storage:
Variables which will be observed	Saved state of manifest
Test design approach	Pairwise combinations testing using constraints to ensure no violation of guiding rules

4) Test Objective (Capability)	Confirm The GENERAL implement C2PA specifications on the computing platforms in widespread use in both developed and developing regions, specifically including lower-cost and older mobile devices.
Risk being studied	Confirms the operation of The GENERAL in different programs and devices ensuring its compatibility and acquire its different specifications to allow future upgrades
Variables which will be manipulated	Type of files Size

	Type of editings Data storage Type of platforms/programs Type of devices
Variables which will be observed	The GENERAL production log files
Test design approach	Decision table to ensure the identifications of the factors that influence the implementation of The GENERAL

5) Test Objective (Capability)	Confirms that The GENERAL allows manual and automatic filtering to remove sensitive information before sharing with others.
Risk being studied	Ensures that The GENERAL effectively protects sensitive information without being manipulated for malicious purposes
Variables which will be manipulated	Type of files File content
Variables which will be observed	The GENERAL production log files
Test design approach	Pareto analysis will be used to identify and address the vital few types of sensitive information that contribute to the majority of risks before sharing with others.

6) Test Objective (Capability)	Confirms that The GENERAL discloses the nature of information that will be captured, recorded, and/or stored on users' behalf and obtains informed consent from their users before doing so

Risk being studied	Confirms the trust between the program and its users, ensuring that users perceive their data privacy and informed consent as valued and respected
Variables which will be manipulated	Type of files File content
Variables which will be observed	Source of files
Test design approach	Scenario-based testing will allow the representation of typical user interactions with The GENERAL, ensuring that each scenario includes the disclosure of information and consent process

Failure Mode Test Objectives

1) Test Objective (Failure Mode)	What if the signing credentials of the given data set is not listed on any of the validator’s trust list.
Risk being studied	Whether credentials from random organizations which are not in the validators’ trust lists can pass The GENERAL’s validation.
Variables which will be manipulated	C2PA content credentials Claim inside the manifest of the assets
Variables which will be observed	Validator’s trust list Error message of The GENERAL console Failure code The GENERAL log file
Test design approach	State modeling of The GENERAL. Decision tables

2) Test Objective (Failure Mode)	What if the framework had an update and has deprecated some functions?
Risk being studied	See if dataset with old credentials from previous version can be accepted with updated C2PA framework.

Variables which will be manipulated	The given Assets Content credentials of the Assets Deprecated functions names
Variables which will be observed	Failure code Error messages on The GENERAL console. The GENERAL log files.
Test design approach	Random selection of values for variables.

3) Test Objective (Failure Mode)	What if a tampered data set with credentials were given to The GENERAL?
Risk being studied	The GENERAL's capabilities of recognizing tampered assets even if the correct credentials were given.
Variables which will be manipulated	The given data set. The GENERAL's tampered data recognition model
Variables which will be observed	Failure code Error message on The GENERAL console The GENERAL log files.
Test design approach	State modeling of The GENERAL Process block diagram

4) Test Objective (Failure Mode)	What if normal softwares with incomplete credentials were given?
Risk being studied	Confirm that The GENERAL prevents the validation of software with inappropriate credentials.
Variables which will be manipulated	The given software Content credentials of that software
Variables which will be observed	Failure code Warning messages about the incompleteness of credentials on The GENERAL console. The GENERAL log files.
Test design approach	Random selection of values for variables.

5) Test Objective (Failure Mode)	What if a valid software with a timestamp that is not in the validator's trust list is given?
Risk being studied	Confirm The GENERAL does not allow the validation of software with a suspicious timestamp that does not match with what was indicated in the validator's trust list.
Variables which will be manipulated	The given software
Variables which will be observed	The given software's timestamp in the manifest Validator's trust list Failure code

	Error messages on The GENERAL console. The GENERAL log files.
Test design approach	Process block diagram

6) Test Objective (Failure Mode)	What if a software with missing claim signature is given?
Risk being studied	Confirm The GENERAL does not allow the validation of software with missing claim in its manifest.
Variables which will be manipulated	The given software’s manifest
Variables which will be observed	Failure code Error messages on The GENERAL console. The GENERAL log files.
Test design approach	Process block diagram

Usage Scenario Test Objectives

1) Test Objective (Usage Scenario)	Can The General only select unmodified/original photos from social media during dataset selection stage of training involving computer vision?
Risk being studied	Make sure The General can filter out modified photos from social media.
Variables which will be manipulated	Content credentials on social media Photo provenance information Digital signature
Variables which will be observed	Acceptance (detection flag) state of The General The General’s dataset size State of training session
Test design approach	Story boarding of usage scenarios. State Models.

2) Test Objective (Usage Scenario)	If random noise is introduced into the dataset by altering pixel values, can The General detect the presence of noise in the dataset and identify it as tampering?
Risk being studied	Make sure The General can detect noise injection to avoid the impact of noise on the integrity and accuracy of the dataset
Variables which will be manipulated	Level of noise type of noise

Variables which will be observed	response time of The General Detection accuracy (detection flag state)
Test design approach	Story boarding of usage scenarios Agile Story Acceptance Tests

3) Test Objective (Usage Scenario)	If dependencies of the software used for training are modified, can The General detect unauthorized changes and prevent the execution of tempered code?
Risk being studied	Make sure unauthorized changes to software are detected by The General and the training is paused.
Variables which will be manipulated	dependencies of software extent of tampering
Variables which will be observed	response time of The General Detection accuracy (detection flag state)
Test design approach	Story boarding of usage scenarios Agile Story Acceptance Tests

4) Test Objective (Usage Scenario)	If labels associated with a subset of data samples are modified, can The General recognize discrepancies between the expected labels and the manipulated ones?

Risk being studied	Make sure The General can detect discrepancies between expected labels and manipulated ones and pause the training or inference in order to avoid incorrect model training and biased predictions.
Variables which will be manipulated	Type of label manipulation extent of label manipulation
Variables which will be observed	response time of The General Detection accuracy (detection flag state) Error rate in detecting label manipulation
Test design approach	Story boarding of usage scenarios Control flow Agile Story Acceptance Tests

5) Test Objective (Usage Scenario)	Can The General trace back the original file or an interested data based on a modified version?
Risk being studied	Make sure The General can use provenance information of C2PA framework to trace back specific data of interest to ensure the accuracy of data.
Variables which will be manipulated	provenance information extent of concealment attempts (ex: encryption, watermark, data masking)
Variables which will be observed	provenance information C2PA manifest

	C2PA Authencity Detection speed accuracy of tracing
Test design approach	Story boarding of usage scenarios control flow Agile Story Acceptance Tests

6) Test Objective (Usage Scenario)	Can The General be used with screen reader by users with visual impairments ?
Risk being studied	Make sure that all user interface elements are properly labeled, interactive components are accessible via keyboard navigation and content is presented in a logical and understandable manner when accessed through a screen reader
Variables which will be manipulated	Screen reader software The General compatibility user interface elements
Variables which will be observed	compatibility with screen reader software accessibility of user interface elements content presentation and understandability
Test design approach	Story boarding of usage scenarios.

Quality Factors Test Objectives

1) Test Objective (Quality Factors Related to Performance)	Study the data poisoning success rate before and after the C2PA credential was applied.
Risk being studied	How well The GENERAL with C2PA framework can prevent data poisoning attack.
Variables which will be manipulated	Numerous data set with and without C2PA content credentials
Variables which will be observed	Number of successful attacks with C2PA Number of attack failures with C2PA Number of successful attacks without C2PA Number of attack failures without C2PA
Test design approach	Pareto analysis.

2) Test Objective (Quality Factors Related to Performance)	Study the ratio of acceptance of tampered data between 2 models: one with credential and one without.
Risk being studied	How well does the application of C2PA framework can prevent data tampering
Variables which will be manipulated	Numerous data set with and without C2PA content credentials
Variables which will be observed	Number of accepted tampered data with C2PA Number of accepted tampered data without C2PA
Test design approach	Pareto analysis.

3) Test Objective (Quality Factors Related to Performance)	Study the ratio of data size and software usage (CPU, memory, time)
Risk being studied	Concern that the software may be too resource consuming
Variables which will be manipulated	Size characteristics
Variables which will be observed	CPU usage Memory usage Time usage
Test design approach	Dynamic analysis

4) Test Objective (Quality Factors Related to Performance)	Study the ratio between the data marked as removable and nonremovable by C2PA-compliant tools
Risk being studied	Concern about the correctness of detection of the data
Variables which will be manipulated	File content Type of files
Variables which will be observed	The GENERAL log files
Test design approach	Pareto analysis

5) Test Objective (Quality Factors Related to Performance)	Study the amount of time it takes to trace back the original data of interested based on modified version

Risk being studied	Concern that tracing time being slow for most cases
Variables which will be manipulated	Number of modified sets of data
Variables which will be observed	time to trace back original data variation in time
Test design approach	pareto analysis

6) Test Objective (Quality Factors Related to Performance)	Study the response time of The General for model inference tasks, specifically classifying unmodified images during pre-training.
Risk being studied	Make sure the average response time of The General is under a threshold, not too slow
Variables which will be manipulated	number of requests (load) ratio of modified images
Variables which will be observed	response time throughput (number of requests processed per unit of time) resource utilization
Test design approach	pareto analysis

Regression Testing of The GENERAL

The objective of regression testing for "The General" is to ensure that software updates or modifications do not introduce new bugs or regressions that could affect the system's functionality, performance, or reliability.

A lab is set up near the development team in which three different production runs can take place.

1. A typical case

2. A harsh case

3. A very fast case

Periodically, at least once per week, a production run of each type is done on software under development using the lab set up.

Review of log files and produced products is done to identify any unexpected variations.

A unit test framework is part of the Continuous Integration server. The unit test framework mocks any access to the physical The GENERAL and is run against every build done as code is checked into the source code repository.