EXAMINATION OF METADATA OF DRONE IMAGES TO PRESERVE THE CONFIDENTIALITY, INTEGRITY, AND ORIGINALITY OF THEM

Gergely Lapis [1,2*], Veronika Kozma-Bognár[2]

[1] Thyssenkrupp Components Technology Hungary Kft., Hungary
[2] Drone Technology and Image Processing Scientific Lab, Dennis Gabor University, Hungary
[*] Correspondence: gergelypeter.lapis@gmail.com

DOI: 10.66538/DH.2025.1.1.14

Abstract

The usage of drones is spreading these days not just for industrial use, but also in everyday life. To keep secure the metadata of created drone images is crucial, because against the images that are made by mobile phones, they are usually used for post-processing, like creating orthophoto, and taking different measures. For ordinary people the personal information that is stored in the metadata could be important, and they usually do not care about this information. In the following article we will present two of our own solutions for these problems, which could be implemented for every type of metadata, but especially for drone image metadata. The first solution will show a process to create a single number to measure the criticality of included metadata against protected information and provide a mitigation operation to lower the risk. The second solution outlines a possible process to keep the integrity of metadata and image data without preventing the possibility of post-processing the image and/or metadata attached to it.

Keywords: metadata, drone images, information security

1. Introduction

Assigning extra information to images is much older than we think. In ancient times there were card indexes in the libraries for the stored papyrus rolls. With the appearance of photography, the attached information also existed. Just not in digital format, but rather than in written form usually on the back of the photos: who made it, when, where, and who or what could be seen in the photo. With the advance of digital photography, the demand to store the extra content in digital format together with the image is raised. To solve this problem, different standards have been made. The IPTC, which was created for storing press related information with the images, the Exif, which was focused on the technical parameters of the creation of images, and the XMP which was invented for storing post-processing information about digital images [1] [2] [3].
Today all these three standards are working together and supplement each other. The XMP format became an ISO standard (ISO 16684-1), and this is the format that could be used for most image types. The Exif and IPTC are mostly used for TIFF and JPEG images, but XMP could be used for SVG or DNG images also.

These standards were invented during the beginning of the 90's, today they are industrial standards, which are used by every digital camera manufacturer [4]. Therefore, the data, which are stored in the metadata, are now well-known format what is great if you want to process the information, but not too good if you want to keep the originality of the information. The metadata attached to the images are not protected in any way. So, everyone with a metadata reader and writer application could modify or access or modify the information that is stored in it [5].
The specialty of XMP format is that it could keep containing both the IPTC and Exif fields, for what the other two could not do [6] [7]. The XMP is an XML-based scripting language therefore very flexible and could be extended. Also, it could contain user-created

fields and namespaces, which very often are used by the manufacturers to create manufacturer-, device- or model-specific metadata [8] [9] [10].

There are different processes that are usually used for keeping the originality of information in images. Usually, they use some kind of cryptographic process to secure the whole image or just the metadata. Like the process that extracts the EXIF data from a JPEG image and encrypts it with a symmetric key [11]. The advantage of the process is that it is very simple and therefore fast, the image itself takes no changes, and the security level of the solution is relatively good. The disadvantage is that it could be used right now just for jpeg images and just for Exif metadata. Besides, the metadata is not readable anymore, just in case you own the encryption key. Another solution is to secure image information itself. The solution is called Fully Homomorphic Encryption using Magic Number Fragmentation and El-Gamal Encryption [12] [13]. It changes the image content of a picture, which remains an image but does not contain any recognizable visual information, and changes the histogram of the image by creating a relatively uniform distribution. In this case the metadata remains as it is, but the image content is changing. Which means you could process the metadata but could not process the image content. More research shows that the encryption of image data is more different than the usual file information [14] [15].

Of course, there is always a way to secure any image file by encrypting the whole file with symmetric or asymmetric keys. This process secures the image and the metadata content also but prevents us from using the image file for any further process. So, these operations are good from a security perspective but not so usable from post-processing and free usage perspectives [16].

The encryption of an image file could keep the integrity of the source, but after decrypting the file, the metadata still could contain GDPR or any other relevant information [17]. So, when someone uploads an image to the cloud, they usually do not care about the included metadata. The social media platform usually could clear personal or confidential information from the metadata during the upload of an image, but these processes just clear the data without any examination or checking. They just delete everything, even if half of the deleted information is not relevant [18] [19] [20].

From a practical point of view, the classification or integrity of metadata has already been addressed in many cases. Social media, medicine, forensics, or agricultural side these questions were mentioned [21] [22] [23] [24].

2. Review metadata information and mitigate the risk

To solve the previously described problems, we have defined a process that categorizes the metadata along with the protected information, which could be GDPR or any other information, like the geographic location where the image was taken or the exact date and time when it was created, and after the categorization, it calculates a criticality number from the data, which defines how close the data together to the protected information [25]. After it we have shown a mitigation operation, what can lower the risk. It could be used to avoid publishing confidential or non-public information.

2.1. Categorizing the metadata

First, we must clarify what kind of metadata fields are available. As was mentioned earlier, the IPTC contains press related information like author, location, and other legal information about the circumstances of making the image. The Exif contains the most information about where, when, and how the image was made. With what kind of equipment and settings, like ISO value, shutter speed, model, and serial number of the camera? The XMP contains the processes that were done on the image (modifying brightness, changing the color palette or applying a filter) [25].

As we can see, there are various fields which could be presented in the metadata. So first we have to group them through something. The major groups are the following:

- Personal data
- Data connected to the making of the image
- Technical parameters
- Audit-like data

1. **Personal data**

These metadata fields contain data about the person who created the image or made modifications to it. These data are GDPR relevant, so they are very sensitive, and only with the explicit approval of the person could they appear during publishing the image on any interface [26]. The personal data is divided into three different subgroups:

- ***Identification data:*** which could identify the person itself, like social security number or identification card number. These types of data appear very rarely in the metadata and usually attach them to images that could be possible by official organizations. The common nature of these data is that though it appears in metadata, they are usually not public searchable information.
- ***Specific data****:* These data could identify a person together with other data. The data could not exactly identify the person; there could be thousands of people with the same name but supplementing it with other data could do it (name plus date of birth plus place of birth). The email address belongs here, because it could not refer to the person itself. like smallfox@anything.com. Data like this is the most relevant information, because it could appear more often in metadata, and there are several possibilities to search on the net to identify a given person, based on this data.
- ***Supplementary data***: Which is not exactly connected to a person but could be suitable to identify a person. Like the serial number of a device, which is connected to a given person or company. The identification number of the application is used to modify images, or other person-specific information.

2. **Data connected to the creation of Image**

All the data that describes the location or date and time of creation of the image belongs here. But also, it could be any field which describes any circumstances of image creation, like description about the content of the picture like the IPTC Headline field, which could contain any description about the image. These fields are usually freely editable, so anything could be put into them; therefore, it is very hard to analyze their contents against the protected information.

3. **Technical data connected to creating Image**

These are the technical details about which was set during the making of Image. The brand and model of the device was used, technical specifications about the composition, timing, sensitivity, and image or filter settings. These settings could be different for different devices, but there are several which are common for everyone. It is interesting that these settings are technical ones but could refer to a significant author.

4. **Traceability data**

These are usually the least relevant data, because the refer where the image was processed or modified earlier. It could be interesting but mostly used by image processing applications. The Media management namespace of the XMP contains these fields and tags.

2.2 Examining and defining the confidentiality level of metadata

During the examination of data, we have focused on how the metadata is connected to a given person, whether it is permanent or could be changed during the time (for example, a date of birth is permanent, an address could be changed but both are connected to a person). This could be applicable to any other information to be protected. The most important aspect is how strictly the data could be connected to the information. The other aspect is how close the data is to knowing the information. Like place of birth is strictly connected to a person, but incase that it is a bigger city, it does not drive us too close to identify the person. It is the same as the date of birth. But if we combine the two data, we are much closer.

The two aspects are as coordinates of a two-dimensional searching vector. The length of the vector gives us the **search distance**. As small as the search distance is, we are as close to identifying the information (Table 1).

Table 1. Defining of Binding and Identification levels

Levels	Binding	Identification
1	Data which could be bonded directly to the protected information and permanent in time (is case of personal	Highly narrows down the area of searching, capable of identifying the information with a few other data
2	Medium level data which is bonded directly to the information but could be changing in time (like address)	Moderately narrows down the searching area, pointing to a direction but not enough to identify the information
3	Distant data which could not be bonded directly to the information and could be permanent or changing in time (in case of personal data like the date of making the	Poorly narrows down the searching area

Let's see an example for each cell of table, connected to the protected information of creator of Image. Binding / Identification level): 1/1 – name, date of birth; 1/2 - place of birth; 1/3 – color of eye; 2/1 – address; 2/2 – email address; 2/3 – weight; 3/1 – location of creating of image; 3/2 – Serial number of used cameras; 3/3 model of used camera.

Above these there are two technical categories also, which do not appear in the table. Level 0, what is the immediately identification data, what means this data identifies the protected information immediately (in case of personal data like social security number). The other one is the custom field, which is not part of the basic standards, or a complex field or tag, what is difficult to analyze. In these cases, the field must be examined and categorized individually or just could be cleared (Table 2).

Table 2. Binding and Identification level matrix

Binding level	Identification level		
	1	2	3
1			
2			
3			

The table defines the **Identification distance categories**, what could be four different: Red: Critical; Orange: High; Yellow: Medium; Green: Low. This category defines how important the field or tag is during the mitigation process. Every cell in the matrix has another value, the **Identification distance value**. It is created like the normal Euclidean vector length:

$$D_a = \sqrt{S_k^2 + S_a^2}$$

Where,

D_a: Identification distance value

S_k: Biding level

S_a: Identification level.

The calculated value itself is not applicable to define a common value, because in the metadata these fields or tags are placed in various ways, and the information is not just a summary of the data. Therefore, we calculate some kind of average value that represents how close the summary of data is to the identification of information. For a better understanding of value, we calculate the average value in that way, so that zero (0) means the total unidentifiability of information, and the one (1) is the trustable

identification. To reach that, we have used the combination of square root average and harmonic meaning. We have chosen the harmonic meaning because the higher Identification distance value means less in the formula. We also wanted the value of the formula should not be linear growing, because in these kinds of data, the information of summarized data does not equal the summary information of data. We have wanted a lying-down parabola, because going forward on the x-axis the value on the y-axis does not grow linearly, and against the function, it is not limited, but growing rate slows down.

$$F_m = \sqrt[2]{\frac{\sum_{i=1}^{n}\left(\frac{1}{D_{ai}}\right)^2}{d_{ak}}}$$

Where,

F_m: Identification value,

1-n: used number of Identification distance values,

D_{ai}: Identification distance value of item i,

d_{ak}: used number of Identification distance categories

The calculated value meets with the following predefined rules:

- If we add new data to the formula, we step closer to the threshold.
- If we remove data from the formula, we step farther from the threshold.
- If we replace data with another one with lower D_a the calculated value moves closer to the threshold.
- If we replace data with another one with higher D_a the calculated value moves farther from the threshold.
- The threshold could be reached and exceed able (the function is not limited from above).
- The function does not grow linearly.

Let's see an example with different data values.

First, we take the identification distance vectors, and calculate the number of Identification distance categories:

$$v_1 = [1,2], v_2 = [2,1], v_3 = [3,2], v_4 = [3,3] => d_{ak} = 2$$

The Identification distance values that belong to these vectors are:

$$D_{v1} = \sqrt[2]{5}, D_{v2} = \sqrt[2]{5}, D_{v3} = \sqrt[2]{13}, D_{v4} = \sqrt[2]{18}$$

The Identification value from these is:

$$F_m = \sqrt{\frac{\left(\frac{1}{\sqrt[2]{5}}\right)^2 + \left(\frac{1}{\sqrt[2]{5}}\right)^2 + \left(\frac{1}{\sqrt[2]{13}}\right)^2 + \left(\frac{1}{\sqrt[2]{18}}\right)^2}{2}} = \sqrt{\frac{\frac{1}{5} + \frac{1}{5} + \frac{1}{13} + \frac{1}{18}}{2}} \approx 0{,}5160$$

If we replace one of the vectors with a critical one (red matrix cell in Table 2), the value of F_m rises to 0,6989.

The identification threshold does not require to be at one. It could be anywhere based on the usage and the nature of the information. We could also set a range of thresholds where we define the information as identifiable. In our case we have created four ranges (Table 3).

Table 3. Example for identification levels by range

Identification level	Range
low	0,0000 -0,4000
medium	0,4000-0,7000
high	0,7000-0,9200
critical	above 0,9200

With the set ranges we could move the value not just below or above the threshold, but between the ranges.

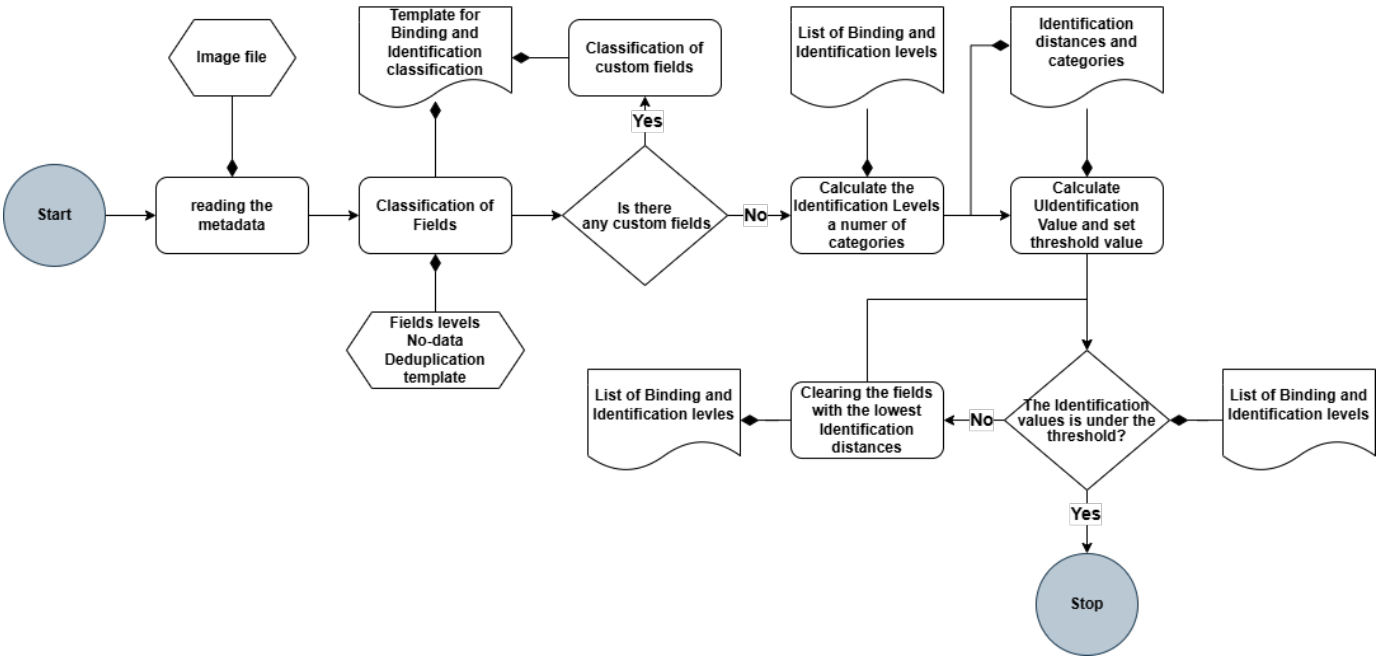
Of course, the preparation of fields for doing the calculation and assigning them into Binding and Identification levels is very crucial. The fields with level zero must be cleared immediately, and the custom fields must be analyzed. The preparation must be suited to the information which must be protected. If a classification template is ready, it could be used for any metadata.

2.3. Mitigation process

Because now we have an exact Identification value, we can make a process to mitigate the risk. The mitigation process is much easier now, as we put every field and tag into a given Identification matrix cell, because we just have to remove or clear the data with the smallest Identification distance values, to lower the Identification value. The goal of the process could be to lower the value but could be to reach a previously set range. We also could have some constraints on which field could be cleared, and which is mandatory.

The process requires putting the metadata fields into the appropriate Binding and Identification levels. The classification is not a static process, because it depends on the information that must be secured (we would like to protect personal data, the location of the image creation, etc.). The template which will be created is the base of processing the metadata of images. All templates are connected to specific information. The Figure 1 below shows the process of template creation for our test images.

Figure 1. Process of data classification and risk mitigation



It is important that during the mitigation process the d_{ak} value must remain the same as it was for the first calculation. So, if we remove fields the summary number of Identification distance groups will remain.

The next example shows the mitigation process of a drone image, on which we have made the data classification. The result is in the Table 4.

Table 4. Data classification of a test drone image (Red: Critical, Orange: High, Yellow: Moderate, Green: Low)

Metadata label	Level		Identification distance
	Binding	Identif.	
"ExifToolVersion": 12.85	3	3	Low
"FileName": "DJI_20241005121151_0001_MS_G.TIF"	3	2	Low
"FileModifyDate": "2025:04:25 17:16:06+02:00"	3	2	Low
"FileAccessDate": "2025:04:28 06:51:07+02:00"	3	2	Low
"FileCreateDate": "2024:10:19 07:24:30+02:00"	3	1	Moderate
"Make": "DJI"	3	3	Low
"Model": "M3M"	3	3	Low
"ModifyDate": "2024:10:05 12:11:51"	3	1	Low
"About": "DJI Meta Data"	3	3	Low
"ImageSource": "MS_G_CAMERA"	3	3	Low
"GpsStatus": "Normal"	3	3	Low
"AltitudeType": "GpsFusionAlt"	3	3	Low
"AbsoluteAltitude": "+230.642"	3	1	Moderate
"RelativeAltitude": "+60.002"	3	1	Moderate
"CameraSerialNumber": "5HZO3AGGC270PM"	3	2	Low
"DroneModel": "M3M"	3	3	Low
"DroneSerialNumber": "1581F5FKD232T00D199S"	3	2	Low
"CaptureUUID": "39ce4e7ac466418a8cc13a25d70ff9ce"	3	2	Low
"DroneID": "1581F5FKD232T00D199S"	3	2	Low
"Version": 7.0	3	3	Low
"RigName": "M3M"	3	3	Low
"City": "Kis-Balaton"	3	1	Moderate
"Headline": "Kis-Balaton terepi mérés"	3	1	
"Source": "Lapis Gergely"	1	1	Critical
"ApplicationRecordVersion": 4	3	3	Low
"DateTimeOriginal": "2024:10:05 12:11:51"	3	1	Moderate
"CreateDate": "2024:10:05 12:11:51"	3	1	Moderate
"SerialNumber": "1581F5FKD232T00D199S"	3	2	Low
"GPSAltitudeRef": "Above Sea Level"	3	3	Low
"GPSStatus": "Measurement Active"	3	3	Low
"GPSMapDatum": "WGS-84"	3	3	Low
"GPSAltitude": "230.6 m Above Sea Level"	3	1	Moderate
"GPSLatitude": "46 deg 37' 36.61\" N"	3	1	Moderate
"GPSLongitude": "17 deg 12' 44.54\" E"	3	1	Moderate
"FOV": "63.7 deg"	3	3	Low
"GPSPosition": "46 deg 37' 36.61\" N 17 deg 12' 44.54\" E"	3	1	Moderate

As it can be seen, we have 3 different Identification categories, which means the value of d_{ak} will be 3. The calculated Identification value based on data above is:

$$F_{me} = \sqrt{\frac{\left(\frac{1}{\sqrt[2]{2}}\right)^2 + 12 * \left(\frac{1}{\sqrt[2]{10}}\right)^2 + 8 * \left(\frac{1}{\sqrt[2]{13}}\right)^2 + 15 * \left(\frac{1}{\sqrt[2]{18}}\right)^2}{3}} =$$

$$\sqrt{\frac{\frac{1}{2} + 12 * \frac{1}{10} + 8 * \frac{1}{13} + 15 * \frac{1}{18}}{3}} \approx 1{,}0245$$

The calculated Identification value (F_{me}) is above the set threshold (0,92) which means we could receive protected information from the content of fields (the person who made the image). We could start to mitigate the risk by clearing the critical fields (red ones), and the modified Identification value will be then:

$$F_{m1} = \sqrt{\frac{12 * \left(\frac{1}{\sqrt[2]{10}}\right)^2 + 8 * \left(\frac{1}{\sqrt[2]{13}}\right)^2 + 15 * \left(\frac{1}{\sqrt[2]{18}}\right)^2}{3}} =$$

$$\sqrt{\frac{12 * \frac{1}{10} + 8 * \frac{1}{13} + 15 * \frac{1}{18}}{3}} \approx 0{,}9396$$

The modified Identification value is much lower than the original one was, but it is still above the threshold. But because the fields are in the lower part of Identification distances, extracting the protected information from the fields is much harder than it was at the beginning.

Below we show some sample images from a test bundle of 37 images. The samples were created with different types of cameras, to make the sample more general. The used cameras were Mapir Survey 3w rgn, Hasselblad L1D-20c, DJI FC-6510, DJI M3M. Therefor the images were made both with visible spectrum, NIR and with multispectral cameras. The resolution of the images were also different, and because of the usage of different cameras, the registered metadata also differs in the images [21].

Figure 2. Sample images from the test bundle

We measured the metadata information for all images against the creation date of the images. Table 4 shows the occurrence percentage of date data in each kind of metadata type.

Table 5. *Occurrence percentage of data data in metadata types for test images*

Number of Images	Exif	Xmp	Iptc
37	100%	64,86%	2,70%

We have made data clearing and filtering on the sources, and removed duplicates, and calculated the Identification value. The table shows the average Identification value before data filtering, before deduplication, the final value, and the value after mitigation. The last 3 columns show the number of occurrences of date fields in each metadata format.

Table 6. *– Test results for bundle of test images*

Number of images : 37	Identification value				Exif pcs	Xmp pcs	Iptc pcs
	Before data filtering	Before deduplication	Final values	After mitigation			
Averages:	1,4430	1,0992	1,0992	0,3479	100%	64,9%	2,7%

3. Keeping the integrity and originality of metadata

Another common problem with the metadata is that they could be modified. If we want to keep the image and metadata in a usable format, we cannot encrypt them. How could we ensure in this case the integrity of metadata? A solution could be to replicate our metadata into different parts of metadata and use different metadata formats. It is a possible solution because there are many overlaps between the fields of different metadata standards. Also, a solution to only encrypt some fields, not the whole metadata section. In this case we could keep the availability of the other fields, but we still need the key to read the data from the encrypted fields. If we are using asymmetric encryption keys, we could pass the public key with the image in a custom XMP field, but it does not prevent the modification of the metadata. Because anyone could modify the information and encrypt it with a new key [27] [28].

What could be the solution then? Creating checksums from the data with different formulas could help us. Of course, in this case the metadata is still modifiable, but if we are using individual formulas, we could check if the metadata is the original one or not. And this process gives us the free usability of image- and metadata. If we are creating different hash codes from different fields that overlapped with each other we could tell, if there was a modification in the data, where it was. A hash also could be made from the image data also, and in this case, we could check if the image is corrupted or not [29] [30].

To do that, we created a new namespace in XMP and added different sections to it, which contain the hash code and other relevant information from the image.

Namespace: secuirtycheck

Property groups: sourcelink, checksum(1)…checksum(n), generalcheck

Sourcelink: sourceid, sourceblock

Checksum(n): checktype(n), checkcode(n)

Generalcheck: gentype, summarycheck, imagecheck, timestemp

The Sourcelink property group includes the ID of the previous transaction, and the checksum of it. The Cheksum section contains the different hash codes created from different parts of the image and metadata contents. A general check includes the types of hash code generation and the summarized metadata and image data hashes, and a timestamp.
During the research a Python code was developed for creating a namespace and some custom properties in XMP format. This adds custom fields to the end of the XMP metadata section. The code uses a pyexiv2 library to manipulate XMP metadata.
Of course, recalculating these hash codes today with the current calculation capacities is not a big challenge. Storing hash code in custom XMP fields is a good start but does not solve all the problems [31] [32].

Our solution is to use different hash codes and store them into custom XMP fields and create a blockchain system based on these hash codes. In this solution a blockchain transaction is not a payment or financial statement, rather than a hash code creation for a given image.

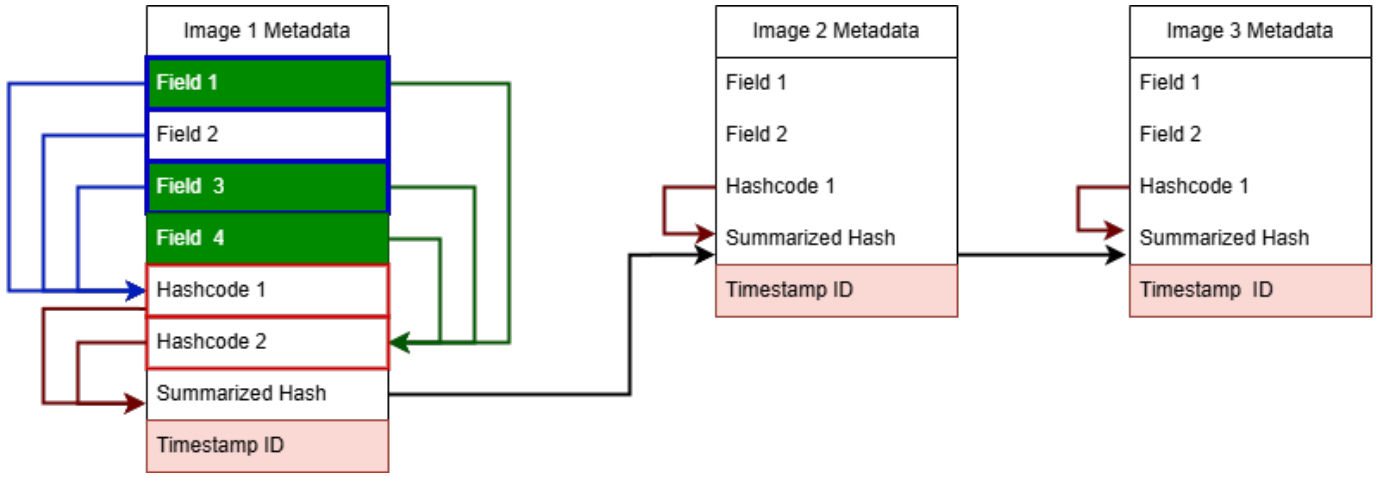
The system, like cryptocurrencies, has three major elements. The first one is a chain of the hash codes. Every transaction receives its own hash code, but it includes the hash code of the previous transaction. The first block does not point anywhere; this is called the Genesys block. The structure of these blocks is very similar to the building of database index files or to the folder information contained on hard drives but pointing backward and not forward. Every block receives a timestamp, which is an individual identification number. The block could be searched easily by this number. The blocks are connected continuously to each other, so there is no possibility to put a block between the chain, just to add a new one. If you want to put a block in the middle of the chain or change data in it, you have to recalculate all the hash codes from that point till the end of the chain [33] [34].

The second element is the Proof-of-Work (PoW), which has the exact function of slowing the recalculation of chain blocks. It also approves the creation of a new block. PoW is usually a complex mathematical problem that must be solved. The result of it is the "proof of work". These algorithms could be different ones, the commonality is that calculating the result is very resourceful, but to check the result is very easy. One algorithm is the "Hashcash", when the PoW is a number whose hash code starts with a given pattern. This could be solved by guessing, because creating the source number from a hash is very hard. So, you must put much processor time into it, but to check the result is simpler. This element ensures that nobody could change something in the middle of the chain, because recalculating and doing PoW for each block after it in a reasonable time, would require such a huge amount of processor resources, which we could not have till now [35] [36].

The third element is the peer-to-peer distributed network. This means that the content of the blocks is replicated to each participant's computer, and an election routine decides what is the approved content for a block. If someone wants to control the "election" must take over more than fifty percent of the network. As larger the network is, the more secure it is [37] [38] [39].

Our process for keeping or at least checking the integrity of image metadata is a blockchain network for image metadata checksums. It could be called Image Metadata Blockchain Network (IMBN). Every participant could register and upload images into the system, what will create different checksums from the metadata and from the image content, and put it into a transaction, which will receive an identification timestamp, and a calculated summarized checksum form the checksums and from the checksum of the previous block. The content of a transaction in this case is a couple of checksums. To make the registration not just for a single picture, but rather a series of images, what is very common in the world of drones, in case of that, the system will calculate hash code for the whole series, and the transaction will contain the summarized checksums. It means if an image is changed or modified in the series, the summarized hash code will not be equals. With this process we could provide the integrity check of hundreds of images just in one transaction.

Figure 3. Connection and inheritance of Blocks and Hashes



In the system there will be three main processes which must be defined and implemented. The processes are registration, uploading original image or images, checking image or images.

- **Registration**: A user/participant could register in the system. Receives an identification number, and the registration must be done with backcheck.
- **Uploading original image or images**: A registered user uploads an image or a series of images. The system calculates the checksums from the image(s) and creates a transaction in the system. The system creates a timestamp for the transaction, and it is included in all uploaded image metadata with the calculated checksums also. The approval of the transaction will be done with PoW, and when it is done, the user could download the images with the checksums included in their metadata.
- **Checking Image or Images**: This function could be started by anyone registered or not. The user uploads an image or series of images into the system, and based on transaction metadata, the system checks that the hash code of the uploaded image(s) is the same as it is in the transaction. To do that calculates the hash codes for the uploaded images. If the hash code does not match, the system returns three different outcomes.
    - If the timestamp is matching but the hash code of metadata is not, then the metadata was changed.
    - If the metadata hash codes matched, but the image-based does not, then the image content has changed
    - If neither the metadata nor the image hash code is matching, then the timestamp does not belong to the uploaded image(s), or both metadata and image contents have been modified.

Of course, the implementation of a system like this is not so simple, but the described process represents well the theoretical operation of it.

Why is it so crucial to provide the integrity of metadata or image content of drone images? Drone-made images usually are the basis of some further investigations, like do we have to spray the crops or not. In the future, more decisions will be made based on drone images. If someone hacks the creation date of images, and the decision maker thinks that the taken images were made at a particular time, we could make the spray at the wrong time, and we could lose the whole crop. From practical point of view, there are already [22] [23] [24].

4. Conclusions

The process for image metadata classification and mitigation was tested on different images, and it is capable of representing the confidentiality of image metadata with one value. This value could be easily mitigated and used for making comparisons between different images. The most complicated part of the process is the creation of templates for the metadata fields, but because the metadata standards do not change frequently, the templates could be used for longer periods. The process precision decreases

with the significant rise in the number of classified fields or could lose its relevance. But the process itself could be used for any information that must be protected and could be applied not just for drone images rather than any kind of information [40] [41] [42] [43].

Parts of the process could be automatized, but because of custom fields, there always will be a manual check in the templates.

The process for keeping the integrity of drone image metadata without limiting the usability of the data is usable. The process has two different stages, the first one is to store hash codes into custom XMP fields, and the second one is how to preserve that anyone could modify these hash codes. To ensure that we have outlined an Image Metadata Blockchain Network (IMBN), which works similarly as other blockchain networks, using the has codes and timestamps, the Proof-of-Work, and the distributed peer-to-peer networks. But the transaction in it is not a financial payment rather than a creation of image hash codes.

The system could be implemented into manufacturers' devices (drones) and could be made automatically during the making of the images. with the settings that every image on-by-one will be registered, or the whole series of images taken during the flight [35] [44].

5. Acknowledgments

Project no. TKP2021-NVA-05 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP 2021 funding scheme.

References

1. Foote, K. D. "Dataversity," Dataversity, 2 February 2021. [Online]. Available: https://www.dataversity.net/a-brief-history-of-metadata/. [Accessed 03 2025].
2. PhotoMetaData.org, "Metadata: History Timeline," PhotoMetaData.org, 2025. [Online]. Available: https://photometadata.org/META-Resources-Metadata-History-Timeline. [Accessed 3 2025].
3. Mills, R. "Image Metadata and Exiv2 Architecture," 27 08 2021. [Online]. Available: https://exiv2.org/book/index.html#2. [Accessed 25 01 2025].
4. MetaData.org, "Metadata History," 2025. [Online]. Available: https://photometadata.org/META-Resources-Metadata-History. [Accessed 03 2025].
5. ElQuadi, M. M., Lesiv, M., Dyer A. D., Dorin, A. "Computer vision-enhanced selection of geo-tagged photos on social network sites for land cover classification," ENVIRONMENTAL MODELLING & SOFTWARE, vol. 128, p. 104696, June 2020.
6. Adobe, "XMP-Toolkit-SDK: Data model serialization, and core properties," April 2012. [Online]. Available: https://github.com/adobe/XMP-Toolkit-SDK/blob/main/docs/XMPSpecificationPart1.pdf. [Accessed 25 01 2025].
7. Adobe, "XMP-Toolkit-SDK: Storage in files," January 2020. [Online]. Available: https://github.com/adobe/XMP-Toolkit-SDK/blob/main/docs/XMPSpecificationPart3.pdf. [Accessed 25 01 2025].
8. International Press Telecommunications Council, "IPTC," 2025. [Online]. Available: https://iptc.org/std/photometadata/specification/IPTC-PhotoMetadata. [Accessed 24 04 2025].
9. Camera & Imaging Products Association, "CIPA Standards," 02 2024. [Online]. Available: https://www.cipa.jp/e/std/std-sec.html#. [Accessed 25 11 2024].
10. Adobe, "XMP-Toolkit-SDK: Additional properties," 2022. [Online]. Available: https://github.com/adobe/XMP-Toolkit-SDK/blob/main/docs/XMPSpecificationPart2.pdf. [Accessed 25 01 2025].
11. Wijayanto, H. , Riadi I., Prayudi, Y. "Encription EXIF Metadat for Protection Photographic Image of Copyright Piracy," IJRCCT - INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER AND COMMUNICATION TECHNOLOGY, vol. 5, p. 237, May 2016.
12. Mostefa, K., Laouid, A., Yagoub, M. A., Euler, R., Medileh, S., Hammoudeh, M., Eleyan A., Bounceur, A. "A fully homomorphic encryption based on magic number fragmentation and El-Gamal encryption: Smart healthcare use case," 12 07 2021. [Online]. Available: https://onlinelibrary.wiley.com/doi/10.1111/exsy.12767. [Accessed 25 11 2024].
13. Kahla, M. E., Beggas, M., Laouid, A., Kara M., AlShaikh, M. "Asymmetric Image Encryption Based on Twin," in 2021 International Conference on Artificial Intelligence for Cyber Security Systems and Privacy (AI-CSP), El Oued, Algeria, 2021.

14. Kaur, M., Singh, S., Kaur, M. "Computational Image Encryption Techniques: A Comprehensive Review," MATHEMATICAL PROBLEMS IN ENGINEERING, Vols. Meta-Heuristic Techniques for Solving Computational Engineering Problems, 19 July 2021.
15. ECMA International, "Technical reports - JPEG File Interchange Format (JFIF)," June 2009. [Online]. Available: https://www.ecma-international.org/wp-content/uploads/ECMA_TR-98_1st_edition_june_2009.pdf. [Accessed 07 05 2025].
16. Hoffmann, E. J., Abdulahhad K., Zhu, X. X. "Using social media images for building function classification," CITIES, vol. 123, p. 104107, February 2023.
17. Hazer A., Yildirim, R. "A review of single and multiple optical image encryption techniques," JOURNAL OF OPTICS, vol. 23, no. 11, 13 October 2021.
18. Kaur M., Kumar, V. "A Comprehensive Review on Image Encryption Techniques," ARCHIVES OF COMPUTATIONAL METHODS IN ENGINEERING, vol. 27, pp. 15-43, 2020.
19. Chhetri, T. R., Fensel A., DeLong, R. J. "GDPR consent management and automated compliance verification tool," SOFTWAREX, vol. Volume 27, no. 101821, September 2024.
20. Choompookham, T., Okafor E., Surinta, O. "Mulberry leaf dataset for image classification," DATA IN BRIEF, vol. 54, p. 110281, June 2024.
21. Berke, J. "Application possibilities of orthophoto data based on spectral fractal structure containing boundary conditions," REMOTE SENSING, vol. 17, no. 7, p. 1249, 2025.
22. Berke, J., Győrffy, K., Fischl, G., Kárpáti L., Bakonyi, J. "The application of digital image processing in the evaluation of agricultural experiments," Computer Analysis of Images and Patterns, vol. 719, pp. 780-787, 1993.
23. Biró, L., Kozma-Bognár V., Berke, J. "Comparison of RGB Indices used for Vegetation Studies based on Structured Similarity Index (SSIM)," JOURNAL OF PLANT SCIENCE AND PHYTOPATHOLOGY, vol. 8, no. 1, pp. 7-12, 2024.
24. Csákvári, E., Halassy, M., Enyedi, A., Gyulai F., Berke, J. "Is Einkorn Wheat (Triticum monococcum L.) a Better Choice than Winter Wheat (Triticum aestivum L.)? Wheat Quality Estimation for Sustainable Agriculture Using Vision-Based Digital Image Analysis," Sustainability, 2021, 13, 12005.
25. Boutell M., Luo, J. "Beyond pixels: Exploiting camera metadata for photo classification," PATTERN RECOGNITION, vol. 38, no. 6, pp. 935-946, June 2005.
26. Rupp V., Grafenstein, M. "Clarifying “personal data” and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection," COMPUTER LAW & SECURITY REVIEW, vol. 52, April 2024.
27. Spyrou E., Mylonas, P. "Analyzing Flickr metadata to extract location-based information and semantically organize its photo content," NEUROCOMPUTING, vol. 172, pp. 114-133, January 2016.
28. Darwish, M. M., Kamal, S. T., Hosny, K. M. "A color image encryption technique using block scrambling and chaos," MULTIMEDAI TOOLS AND APPLICATIONS, vol. 81, pp. 505-525, 13 September 2021.
29. Berke, J. "Spectral fractal dimension.," in Proceedings of the 4th WSEAS Telecommunications and Informatics (TELE-INFO ’05), Prague, Czech Republic, 12-14 March 2005.
30. Korus, P. "Digital image integrity – a survey of protection and verification techniques," DIGITAL SIGNAL PROCESSING, vol. 71, pp. 1-26, December 2017.
31. Neil, B. “The XML handbook”, Great-Britain: Person Education Limited, 2000.
32. Stvilia B., Jörgensen, C. "User-generated collection-level metadata in an online photo-sharing system," LIBRARY & INFORMATION SCIENCE RESEARCH, pp. 54-65, 2009.
33. Di Pierro, M. "What Is the Blockchain?," COMPUTING IN SCIENCE & ENGINEERING, vol. 19, pp. 92-95, 2017.
34. Maesa D. D. F., Ricci, L. "Blockchain protocols, data analysis, and applications," BLOCKCHAIN RESEARCH AND APPLICATION, vol. 4, no. 4, p. 100164, December 2023.
35. Shen, M., Gou G., Xuan, Q. "Security and privacy of blockchain," BLOCKCHAIN: RESEARCH AND APPLICATIONS, vol. 4, no. 1, p. 100130, March 2023.
36. Paphitis, A., Kourtellis N., Sirivianos, M. "Resilience of Blockchain Overlay Networks," in Network and System Security - 17th International Conference, Canterbury, UK, 2023.
37. Cheng, L., Tan, H., Li, X., Pan, W., Zhao, H., Yuan M., X. Li "A hierarchical overlay network optimisation model for enhancing data transmission performance in blockchain systems," SCIENTIFIC REPORTS, vol. 14, p. 31900, 2024.

38. Howell, A., Saber T., Bendechache, M. "Measuring node decentralisation in blockchain peer to peer networks," BLOCKCHAIN: RESEARCH AND APPLICATION, vol. 4, no. 1, p. 100109, March 2023.
39. Qju, H., Ji, T, Zhao, S., Chen, X., Ji, Q., Cui, H. "A Geography-Based P2P Overlay Network for Fast and Robust Blockchain Systems," IEEE TRANSACTIONS ON SERVICES COMPUTING, vol. 16, no. 3, pp. 1572 - 1588, May-June 2023.
40. Egerson, J. I., Mosopefoluwa, W., Okafor, M., Olaleye A., Aribigbola, A. "Cybersecurity strategies for protecting big data in business intelligence systems: Implication for operational efficiency and profitability," WORLD JOURNAL OF ADVANCED RESEARCH AND REVIEWS, vol. 23, no. 2, pp. 916-624, 2024.
41. Sandra, P., Zhe, W., Panagiotis, D. C. "Cybersecurity in process control, operations, and supply chain," COMPUTERS & CHEMICAL ENGINEERING, vol. 171, p. 108169, March 2023.
42. Sramkó, P. “Cybersecurity, cyber defense”, Budapest: Globeedit, 2021.
43. Syed Wasif, A. H., Haider, A., Waleed, B. S., Muhammad, F., Abdul, R. J., Malik, J., Malik, H. M.,. Khan A. W., Atiquzzaman, M. "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons," ASSOCIATION FOR COMPUTING MACHINERY, vol. 54, no. 3, pp. 1-36, 2021.
44. Li, K. "Digital media system design and visual art analysis based on Information Security," MEASUREMENT: SENSORS, vol. 11, p. 100978, February 2024.