International Journal of Grid and Distributed Computing
Vol. 10, No. 10 (2017), pp.89-98
http://dx.doi.org/10.14257/ijgdc.2017.10.10.08

A Study on the Guarantee of Authenticity and Permanent Preservation of Digital Image Evidence

Yong Jin Kim[1] and Gyu An Lee[2]

[1]Department of Science Criminal Investigation, General graduate school, Chungnam National University,
(34134) 99, Daehak-ro, Gung-Dong, Yuseong-Gu, Daejeon, South Korea,
guidoloveson@hanmail.net (Yong Jin Kim: First author)
[2]Department ofConvergence Education, Hoseo Graduate School of venture,(06724) 2497, Nambu-Sunhwan-ro, Seoul, South Korea,
leegyuan@hotmail.com (Gyu An Lee : Corresponding author)

Abstract

Investigators acquire and analyze various forms of evidence at the scene of the incident and identify the substantive truths associated with the incident. In particular, investigators in charge of primary investigations shoot various digital photographs and videos and analyze them to find clues to investigations.With the advancement of science and technology, digital photographs and moving pictures have been generalized in the event scene recording method through sketching or analog photography, and it is now possible to reproduce the scene using a 3D stereoscopic scanner.

Records of investigations by the first investigating agency are sent to the prosecutors along with various evidence. Currently, only a few photographs or images necessary for investigation are recorded in the digital image recordings taken by the investigator, and the management system of the remaining data is insufficient.The rapid development of science and technology, and the fact that decades after its occurrence, are being resolved through scientific investigations, if the video recordings taken by investigators are well managed and preserved, it will be an important key to resolving the unsolved incidents.

Through this study, it will be helpful to develop the scientific investigation by suggesting the authenticity guarantee system and the systematic preservation and management plan for the digital image evidence taken by the investigator.

Keywords*: Digital Evidence, Authenticity, Permanent preservation, Photograph*

1. Introduction

We are now living in the digital age. The development of digital technology is changing the paradigm of our lives. For example, art photographs or recorded photographs, which have been recognized only as areas of professional photographers in the past, are no longer the work of a specific expert, but a hobby of the general public. Almost everyone uses cell phones and mobile phones have built-in camera functions so anyone can easily take pictures or videos from anywhere.

Digital imaging equipment, including mobile phones, became a necessity for investigators who were sent to the crime scene to record the scene and collect evidence. In addition, our daily lives are being recorded through black boxes installed in cars and CCTVs installed all over the country, and these video recordings are increasingly being presented as evidence for resolving crimes and conflicts in everyday life. Accordingly, cases related to digital image evidence are increasing. The problem is that the

Received (June 19, 2017), Review Result (September 13, 2017), Accepted (September 15, 2017)

ISSN: 2005-4262 IJGDC

understanding of the characteristics of digital evidence, which is different from the analogue evidence, does not follow the development of technology.

In the case of a Supreme Court case, a photograph on the screen taken with the text information shows the exception of Hearsay rules as independent evidence presented separately from the character information stored in the mobile phone. In order to have theevidence ability, it must be recognized that the original had existed, that it was correctly transferred, and that the submission of the original was incompetent or difficult. [1]

However, this case also mentions only authenticity as one of the requirements of evidence ability, but there is no mention of specific details or proof of authenticity. As the number of digital video recordings submitted to court is increasing exponentially, the debate on the authenticity of digital video evidence is still lacking. Therefore, the necessity of presenting guideline to guarantee the authenticity of digital image evidence is reduced for investigators and business people who collect and analyze digital image evidence most frequently and often at the scene of the incident.

A record documents that are recorded by a team of investigators when they begin to investigate an incident are the beginning and the end of the investigation. Normally, investigations are proceded from the stage of various steps such as situation reports, records, seizures and lists, warrants, result reports by request of the warrants, analysis requests and results.

During that steps thausands of digital evidence photographs will be taken by the investigator or site verification investigator and that will be stored on the server and the computer of the investigation agency. However, very minimum photographs of crime scenes could be used and the rest could be deleted, damaged, lost, or classified due to personnel movements.

In this study, digital photographs collected and analyzed by investigators are categorized as digital evidence, the procedures and problems of collection and storage will be examined. As a result of this study, I propose a storage method of digital evidence and suggest a means to preserve it semi -permanently so that it can be closer to the real truth pursued in the criminal procedure law. To do this, we study the features of digital evidence and the authenticity of digital photographs, and propose a way to preserve them permanently.

2. Features of Digital Evidence and the Way Of Giving Authenticity

The digital image recordings taken by the investigator on the scene of the incident are called digital evidence, and the digital evidence is defined as a code system consisting of 0 and 1 that is transmitted as evidence and worthy.Digital evidence is different from existing analog evidence, and certain conditions must be met to use it as evidence in court. First of all, I would like to suggest some ways to give authenticity to the digital image recordings taken by the investigators after considering the features of digital evidence.

2.1. Features of Digital Evidence

Digital evidence consists of a series of codes, 0 and 1, that are stored or transmitted on digital media. Therefore, digital information can not recognize its existence and contents by human perception ability. In order to investigate digital evidence in court, the digital media must be restored to analog information so that it can be applied to the monitor and printed on paper or other media.And since all methods give visibility to invisibility, no transformation of information should occur in the process of changing.Because digital evidence is a set of binary numbers, it is possible to forge or modulate by simply inputting a simple command, and it is easy to delete. Therefore, in the process of collecting and analyzing digital evidence, the inherent value should not be changed and it must be proven that it has not changed.

Digital evidence can be distributed or hidden throughout the world through networks such as the Internet. In the case of cybercrime requiring digital coin, bit coin, in exchange for providing a decryption key for decrypting encrypted contents through the Ransom way, the flow of funds is made internationally and it is difficult to trace.

Digital evidence is information that is stored on or transmitted through digital media and does not depend on the form of digital media. Digital evidence is evidence of information independent of the media, and if the values are the same, they will have the same value regardless of the media they are stored in. [2]

To summarize the characteristics of these digital evidence, they include invisibility, ease of duplication, vulnerability, large capacity, and globalization.

2.2. Features and Usability of Digital Image Evidence

In the United States, there is a non-profit human rights organization called INNOCENCE PROJECT, which helps people who have been convicted of a misdemeanor by proving their innocence through re-examination of DNA tests. It started in 1992 at the Benjamin Law School in New York, and as of January 2011, the number of people who was helped by that group is about 260. Through the activities of such nonprofit organizations, we have recognized the truth that the development of science and technology has played a role in correcting the unfair trial and the importance of managing proof. [3]

The development of imaging technology can provide a very important clue to reconstruct the scene of the incident and reveal the real truth. If the incident scene photographed in a two-dimensional manner can be reconstructed in 3D using a 3D image program and printed with a 3D printer, the scene of the incident can be reproduced as it is, and the investigator will be able to find the clues of incidents through the reconstructed crime scene.

Modern people living in the digital age are very skilled at changing digital video recordings using programs such as Adobe Photoshop, so they can easily change digital video recordings, submit distorted video evidence to court, this can have a significant impact on the freedom of the judge. On the other hand, even if true video evidence is submitted to the court, strict criteria must be met to recognize it as evidence, if the power of evidence is denied based on the nature of digital evidence.

Considering the impact of video evidence on judges and jury freedom, the importance of digital video evidence in litigation is likely to increase.Generally, jurors are bored, confused, and difficult to judge when a lawyer or witness is trying to explain a technical and complex issue. However, if the same thing is explained through a visual device that simplifies complex problems, the judgments can be turned in a totally different direction. Jurors generally try to remember 85% of what they know visually, compared to trying to keep 10% of what they hear. [4]

The Supreme Court believes that in order for documents output from digital storage media, which are seized, to be used as evidence, the identity of the contents stored in the original digital storage media and the printed documents should be recognized. In most cases, it is sufficient for the court to testify that the witness is simply and accurately portraying the scene in order to prove the authenticity of the photograph.

On the other hand, in the case of the United States, even if there is no witness testimony, if the process of forming a photograph or the reliability of the system is recognized, the photograph may be accepted as proof by the Silent witness theory which recognizes the authenticity of the photograph. Factors to determine the authenticity of the photographs include: ① evidence to form the time and date of the photo shoot ② whether there is evidence that it has been edited or manipulated ③ the capabilities and operating conditions of the photo in relation to the authenticity and accuracy of the photo ④ The stability of the equipment used to photograph, including its safety, the expertise of the

person employed for the operation and testing of the equipment, and the statement of the identity of the relevant participant depicted in the photograph [00]In view of the US digital image evidence acceptance theory, it is necessary to seriously examine the rapidly increasing standards of image evidence in our judicial system.[5]

2.3. Acquisition and Utilization of Digital Image Records of Investigators

Investigators can be divided into judicial police officers and special judicial police officers.A judicial police officer may enforce all investigative duties other than the jurisdiction of a special judicial police officer, including forcible disposition of arrest, seizure, search and verification under Article 197 of the Criminal Procedure Act.Special law enforcement officers are public officials engaged in certain duties, such as medicines, environment, and labor, appointed by the district attorney general, who can conduct investigations into their own jurisdiction.

In the past, these investigators mainly used sketches or analog photographs to record the scene of the crime scene and to obtain evidence. Recently, digital cameras have been popularized by mobile phones and digital video equipment.In this case, among the vast digital video recordings taken by the investigators, only about 10 pictures or less than 5% of the videos are used. The unused video recordings are stored in the personal computer of the investigator, and those are deleted or lost by the mistake of users.

Figure 1. Digital Picture of Crime Scene

2.4. How to Give Authenticity of Digital Video Evidence

The authenticity of digital image evidence means that the person who submitted the evidence must furnish a reliable basis to the judge and that the evidence presented is a true copy. Digital image recordings can be fatal because of the same original and copy, easy forgery or tampering, and very small manipulations, which can compromise the authenticity of the copy and undermine the court's competence.Investigators should carefully consider the accuracy of the software and hardware, expertise, laws, regulations, and rules that are similar to the three elements of digital forensics in order to recognize the nature of these digital evidence and to ensure authenticity from the initial collection stage. [6]

As digital video equipment such as car black boxes and CCTV become common, investigative agencies basically track, acquire, and analyze video related to the incident during investigation.Especially, as the CCTV analysis becomes digital evidence that can be the result of many investigations, precedent about the digital image evidence is

increasing. Among them, the precedent for the video recordings dealt with in the case of the former president of the National Defense Commission is representative. [7]

In the case above, the defendant attempted to fire a firebomb at the home of the former head of the National Assembly on May 5, 2013, but attempted to fire, and the investigating agency obtained 52 CCTV images related to the case and asked an expert, Handy Kelly.As a result of the analysis, the results of the defendant guilty verdict, such as the gait of the characters photographed on the CCTV, and the gait of the defendant are the same in the whole process from the residence of the defendant to the place of the crime.However, the final judgment does not allow the authenticity of the submitted digital image evidence, finally the innocence was pronounced. Thirty of the video record files submitted as evidence were copied from the CCTV storage device through USB of the police officer and repeatedly copied back to the police officer's cell phone and 22 were photographed by the police officer on the cell phone screen, and the shooting date of most image recordings was not displayed. So how can we get the authenticity of digital video evidence?

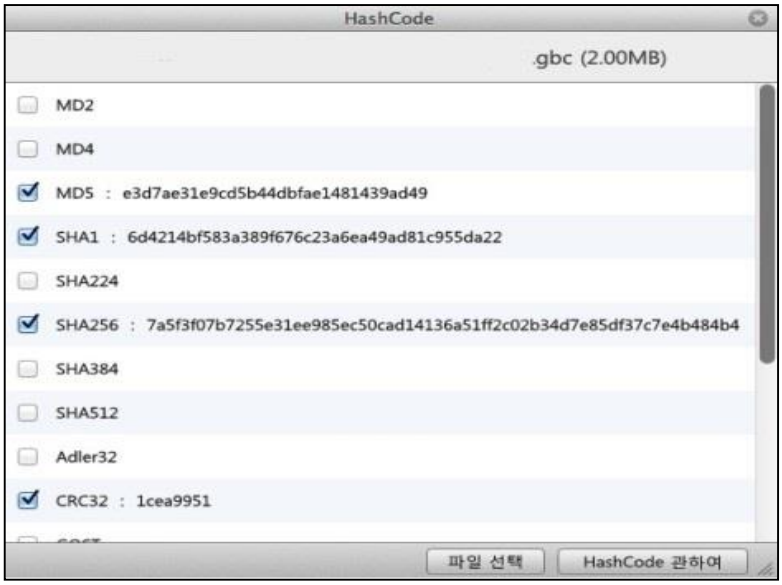

Figure 2. Hash Values that Prove the Authenticity of Digital Evidence

2.4.1. Granting Authenticity through Hash Value and Digital Signature of Digital Image Evidence

A hash function is a function for inputting a message having an arbitrary length and outputting a hash value having a fixed length. Standard hash functions such as MD5 and SHA-1 currently used output hash values of 160 to 256 bits. Unlike cryptographic algorithms, hash functions do not use keys, so they always have the same output value for the same input. Therefore, if the hash value of digital image evidence is extracted using this hash function and the original and the copy are collated, it can be confirmed whether it is forged or altered.

The hash function is used with an electronic signature to enable efficient signature generation. If you are signing for a long message, you do not have to sign it directly for the whole message, but rather a short hash value and sign it. In the digital signing method, a short hash value of 160 bits to 256 bits is input by inputting specific information, and a signature operation is performed on the short hash value, and the calculated value is recognized as a signature for the original message. In order for a signature for a hash value to be recognized as a signature for the original message, it must be computationally infeasible to find another message with the same hash value. If the same hash value can

be created with the value of another input message, the electronic signature can not be trusted and can not be used for electronic transactions.

The method of giving authenticity of digital image evidence through hash value is summarized in the following figure.

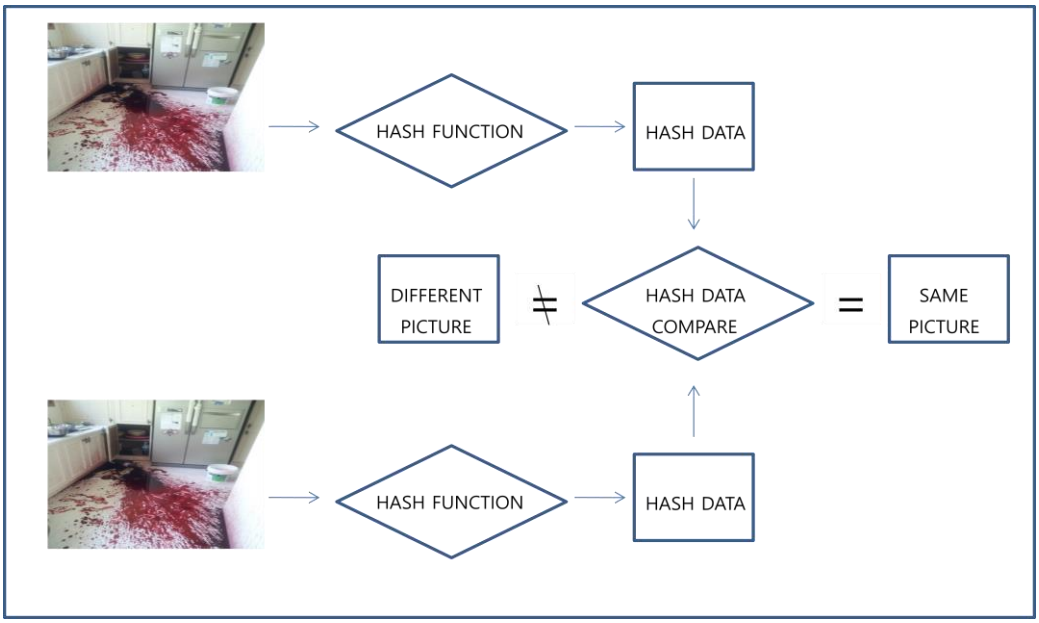

Figure 3. The Way of Comparing Hash Data

2.4.2. Using Metadate

Metadate is information about information. In other words, it provides systematic information about a collection of data such as an image file, so that the file can be accessed and used more efficiently. The Metadate contains the date and time the file was created, the date it was last modified, the camera and lens used, the aperture value, and the shutter speed. The use of this metadate is a very useful tool to ensure that the only authentic digital image is being used as evidence, but the following problems also arise.Metadate can also be changed in many ways and is not a constant truth. To change a specific domain to favor Metadate, it is necessary to have a high level of computer knowledge at the level of a professional hacker, but it is not impossible and not a constant truth.

Once the digital image has been downloaded from the camera to the computer's hard drive, the creation date shown in the file Browser, such as Window Explorer or Mac Finder, is changed to indicate the date the file was created through the monitor. Metadate is also very easy to change with the Microsoft Window photo feature, and there are programs completely to remove Metadate from files. Just open the image file or resave it, but the date in the image's Metadate will be changed.**[8]** This fact gives the litigants, including investigators handling digital evidence, the principles that must be understood and followed to ensure authenticity, especially for those who use digital video evidence.

3. Permanent Storage Method

Currently there is a limit to the permanent storage of digital video evidence. However, in the case of video footage, crime and criminal characteristics are stored as they are at the scene of the incident. So the preservation of digital video evidence should be very careful.

Table 1. Retention Period Up To the Crime Type

Type	Retention period	Remarks
A flush case	Statute of limitation	
Prosecution	3years	
An important event	National Security Law etc.	Permanent, semi-permanent

3.1. How to Interact with Criminal Justice Portal

Currently, the National Police Agency, prosecutors, and the courts are coworking with electric records of criminal cases such as violation of road traffic laws and drunken driving which has no special dispute.The purpose of the criminal justice system is to provide the public with transparency and information access rights to the entire process from the proceeding to the end, along with the digitization of the paperless procedure.

It is the **'Criminal Justice portal site'** where all contents of the investigation are opened to the public. For the investigators who are in charge of the actual investigation, the **'Criminal Investigation Network'** is established so that it can be used for the initiation of investigation and the search for related cases. In the course of such a series of procedures, a method of automatically uploading and preserving digital photographs taken by investigators together with the name of the investigator is required from the beginning of the investigation, registration, and report. In particular, if the metadata and hash value are stored together for retrieval, the reliability will be further increased.

Figure 4. Picture Criminal Justice Portal

3.2. How to Work With a Special Law Enforcement Officer (VPN)

The **Criminal Investigation Network** is currently a network linking judicial police officers with police stations, public prosecutors' offices, courts, and prisons, and requires special networking or certification procedures for special law enforcement officers. In order to support investigation special law enforcement officers should be given a certificate using VPN.

Especially, since smart phone has digital camera shooting function and moving picture shooting function, it can be a method of authorizing using VPN and uploading a digital photo document when approaching the criminal law.

3.3. The Need for a Third Certification Authority

The criminal justice system and the criminal justice portal are organized by the Ministry of Justice and constructed and operated by the Supreme Prosecutors' Office, which may raise the issue of fairness to the preserved evidence. A revtiew of the validity of an investigating agency in granting authenticity to digital image evidence obtained by an investigator should continue to be studied in the future.

In order to alleviate concerns about the leakage of personal information and to secure authenticity in digital image evidence, there is a method of entrusting to a judging agency like a court and a method of establishing a third certification authority. However, As the research field is a fusion of understanding and legal knowledge, we will present the idea as shown in the following figure and leave it as an in-depth study.

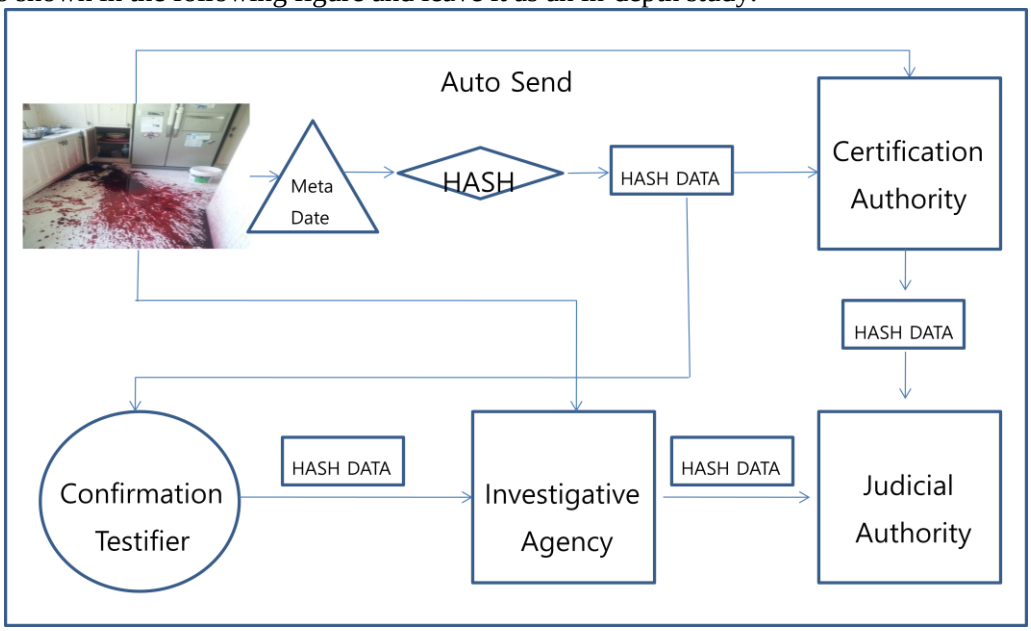

Figure 5. How to give Authenticity through the Third Certification Authority

4. Conclusion

The amount of digital image evidence is increasing exponentially. However, there is not enough system to preserve and manage systematically, and many digital image evidence is not available. To prevent this, the system should be constructed so that metadata is extracted from the digital image evidence generation step and the hash value is given and stored in a certified portal such as the criminal justice system. Analog evidence may have difficulties with long-term preservation, but digital evidence can be retained for as long as server capacity is supported.

In the case of a recent murder case in which criminal cases are reexamined or the statute of limitations disappears, the period of review is permanent.

Plans are under way to digitize and permanently preserve analog evidence from past investigations, including the Supreme Prosecutors' Office. At the same time, the investigators in the field are aware of the importance of digital image evidence and pay close attention to all stages of the investigation so that the authenticity can be secured. We must make an effort to manage with confidence that we will find the key to solving the video evidence.

If the social consensus that gives the authenticity to the digital image evidence through the third certification body will come after the above efforts, it will open the way to the actual truth which is the ultimate goal of the criminal case.

Acknowledgments

"This paper is a revised and expanded version of a paper entitled [Study on the Storage of Digital Photographs by an Investigator] presented at [the 6th International Conference on Next Generation Computer and Information Technology (NGCIT 2017) which was held in Liberty Central Saigon Riverside Hotel, Ho Chi Minh City, Vietnam last August 16-18, 2017]."

References

[1] Supreme Court, 2006Do 2556, **(2008)**.
[2] H. S. Park, "Evidence of Digital Evidence in the Revised Criminal Procedure Act", Seoul, **(2013)**, pp.22.
[3] http : //www.pmg.co.kr.
[4] Z.B. Parry, "Digital manipulation and Photographic evidence", Journal of Law, Technology & Policy, **(2009)**, pp.185.
[5] O. GulKweon, "Introducing foreign country's example about the authenticity of digital photographs", IT & Law Reserch, vol.7, **(2013)**, pp.186-187.
[6] Authur Best, "Evidence", Wolter Kluwer, **(2012)**, pp.213.
[7] 2013Go Hab, 805, "Decision of Fire Prevention Law".
[8] O. GulKweon, "Introducing foreign country's example about the authenticity of digital photographs", IT & Law Reserch, vol.7, **(2013)**, pp.189.

Authors

Yong Jin Kim, he is the Chief of the Army Consolidated Administrative School of ROKA (Republic of Korea Army).
derOO

GyuAn Lee, he is a Ph. D of Engineering in SungSil University.