Protecting Digital Legal Professional Privilege (LPP) Data

Frank Y.W. Law, Pierre K.Y. Lai, Zoe L. Jiang, Ricci S.C. Ieong,
Michael Y.K. Kwan, K.P. Chow, Lucas C.K. Hui, S.M. Yiu, C.F. Chong
The University of Hong Kong
{ywlaw, kylai, ljiang, scieong, ykkwan, chow, hui, smyiu, chong}@cs.hku.hk

Abstract

To enable free communication between legal advisor and his client for proper functioning of the legal system, certain documents, known as Legal professional privilege (LPP) documents, can be excluded as evidence for prosecution. In physical world, protection of LPP information is well addressed and proper procedure for handling LPP articles has been established. However, there does not exist a forensically sound procedure for protecting "digital" LPP information. In this paper, we try to address this important, but rarely addressed, issue. We point out the difficulties of handling digital LPP data and discuss the shortcomings of the current practices, then we propose a feasible procedure for solving this problem.

1. Introduction

Digital crime investigation replicates many legal practices in real world crime investigation. For example, taking cryptographic hash is used to preserve the integrity of digital evidence, resembling taking snapshot of the scene of crime in real world crime investigation. However, not all real world legal practices have been incorporated into the digital forensics investigation framework. One issue, that is essential to proper administration of justice but rarely addressed, is the protection of privilege rights in digital world.

Privilege is the rights of one person (in Common Law countries) to exclude evidence that would be adverse to himself. He/she can refuse to testify or withhold a particular document from presenting as evidence against him/her if it is classified as privileged document [1]. The core concept of privilege is to protect the accused from being prosecuted based on private or unintentional discussion [8]. There are three main types of privileges under Common Law jurisdiction, namely: (1) privileged against self-incrimination; (2) legal professional privilege; and (3) privilege arising from statements made "without prejudice".

Among these three main types of privileges, legal professional privilege carries the greatest implication to crime investigation. Legal professional privileges (LPP) focus on the protection of communications between a professional legal adviser and his client (or person representing his client) made in connection with giving legal advice to the client [8]. The rationale of this privilege is to enable free communications between clients and their lawyers to facilitate proper functioning of the legal system [1]. Nowadays, with the advancement in information technology, these communications are no longer limited to paper or telephone conversations and have extended to various kinds of electronic communications like emails, instant messaging chats, VoIP phones and digital video conferences. Furthermore, the documents prepared for legal proceedings may not exist as hardcopies but may be stored in a computer as Word documents or Excel spreadsheet files. This causes an implication to traditional investigation approach because crime investigators are now required to handle LPP documents in digital format, which is a new area required to be addressed and a systemic

978-0-7695-3171-7/08 $25.00 © 2008 IEEE
DOI 10.1109/SADFE.2008.19

approach is needed to assist investigator in handling privileged digital articles properly and effectively.

Unfortunately, majority of the existing published digital forensics investigation model or procedures have not incorporated the procedure for supporting legal professional privilege data protection. For instance, in the DFRWS framework [7], digital investigation covers the Identification, Preservation, Collection, Examination, Analysis and Presentation of digital evidence. It focuses on the technical aspects in collecting, examining and explaining the hypothesis of incidents without fully incorporating the legal practices inside [9]. Thus, without inheritance of privileged rights preservation into the existing digital forensics investigation procedures or model, legal privileged information can only be protected through standard operating procedures used by practitioners.

In this paper, we address the proper protection of digital privileged documents, in the hope of establishing a set of forensically sound procedures and proposing a practical and efficient scheme for the task. The rest of the paper is organized as follows. Section 2 highlights the difficulties in handling digital LLP documents when compared to the physical world. Current practices to deal with this problem, together with their shortcomings, are presented in Section 3. Then, we propose a possible solution in Sections 4 and 5. Section 6 concludes the paper.

2. LPP documents – Physical vs. Digital

In physical world, LPP articles are handled with extreme caution because the disclosure of any LPP information may jeopardize the legal proceedings involved. Under the Common Law, investigators should not inspect any documentary articles for which privilege is claimed. However, privilege does not extend to articles that could provide evidence of criminal or unlawful acts. If an investigator thinks an article is likely to be related to a criminal case, he could seize it and seal it into a suitable container, like an exhibit envelope, and later on submit to the court for determining if the article could be used for prosecution [12].

When it comes to the digital world, thousands upon thousands of digital files may be stored in a single physical hard drive. When some of the digital files are claimed to be privileged, one intuitive way is to put the whole hard drive into an exhibit envelope and let the court to decide the proper way to handle the individual digital files stored there. However, it may result in a very lengthy process as the court may not have the expertise for the said task. Also, due to the special nature of digital files, it is no longer a straightforward task to separate LPP files from the non-LPP ones. Simply deleting LPP files from the hard drive or simply copying out those non-LPP files from the hard drive may not work. Careful considerations should be given to the copying and deleting processes or valuable evidence may be missed or LPP information may be leaked as logically deleted files may still exist in the hard drive.

3. Current practices and their shortcomings

There is no standardized, forensically sound procedure to protect LPP information. Two common approaches, clone and erase, selective cloning, are being adopted to handle these files.

3.1. Clone and erase

Clone and erase is a straightforward approach. It first prepares a cloned image, that is a bit stream image acquired from the target digital storage media, and then erases the LPP documents from it. The sanitized disk image would be used for later investigation. This

process should be carried out in front of both parties so as to prevent potential evidence in non-LPP files from being removed intentionally.

One obvious problem is that, the image would replicate all the digital data, including the (deleted) LPP articles, that exist at the storage media. With the assistance of standard computer forensic tools, one could easily inspect all data including logical files, deleted files or fragmented file data that are existed at unallocated space within the image. This is an obstacle to the proper protection of LLP articles as previously existed (deleted) LPP information may still be accessible in the context of investigation if the erasion is not thorough. Also, the data owner may take a very long time to view and segregate LPP documents from the enormous digital data stored at the storage media, and the LPP identification may be error-prone under a stressful environment. For better accuracy and efficiency, the process that requires face-to-face interaction should be kept minimal.

3.2. Selective cloning

To avoid any duplication of sensitive LPP articles, selective cloning tries to conduct a selective data copy [10, 12] instead of cloning the whole storage medium. This is, to copy the non-LPP files from the source hard drive to another storage media for later investigation. The examiner may firstly connect to the target storage media with a write blocker device and then selectively extract digital data, excluding the LPP materials, that are relevant to the investigation. To avoid any dispute about unauthorized access to LPP data, the whole process should be carried out in the presence of the data owner, who is responsible to identify any LPP materials and monitor the actions being performed by the examiner. Without questions, this method offers the best protection to the LPP files. However, as the copying is performed with a logical view, deleted files or fragmented file data at unallocated spaces, which are invisible in the logical file system view, may be missed out. It can be very unfavorable for the investigation. Even though the examiner could utilize computer forensic tool to search for deleted or relevant data at unallocated spaces, the process would be very time-consuming and is not practical to be conducted at the scene of crime. Philip Turner suggested utilizing a selective imaging approach [11] to perform a selective acquisition of data on a hard drive using the concept of digital evidence bags [13]. This method is obviously in contrast to the traditional bit stream cloning but derives a way to properly handle large amount of digital information in a forensically sound manner. Also, it still involves a very lengthy face-to-face process.

4. Proposed approach

In order to comply with ordinary principles of computer forensics, it is observed that a bit stream image of the entire storage device should be taken whenever practicable. To avoid replicated LPP articles at cloned image being accessed in the context of computer forensic examination, the acquired image should not be examined until the content has been sanitized. For the removal of the LPP articles, the data owner would be invited to identify the privileged data from the image. The LPP articles would then be selected and an assessment would be made to determine if the articles are legally privileged or not. This assessment may be conducted by a trusted third party, for example, other investigator who is not involved in the case or any independent person who is not involved in the investigation. After the confirmation of the article nature, the LPP articles are destroyed from the data image. The original digital storage media would then be sealed whilst the sanitized image would be ready for computer forensic examination [12].

Taking all these factors into account, we propose the following procedure for handling LPP information:

1. When come across a digital storage media where valid claim of LPP exists, the content of the digital storage media should not be examined but is sealed to prevent tampering from both parties, i.e. prosecution and defense.
2. To preserve the data at the subject storage media, the seal is broken and a bit-stream image is then obtained under the supervision of both parties to prevent any dispute of unauthorized access to LPP articles.
3. Upon the completion of cloning, the original storage media will be sealed again and kept at a safe location by the prosecution, whilst the acquired image will be given to the data owner for a reasonable period of time to remove any LPP articles that are existed therein by a forensically sound method.
4. To prevent any further access to the removed LPP information, it is suggested that the data owner should erase the LPP data completely from its physical storage location rather than the logical location at the storage media. This can be done by zeroing out the data content or replacing the content by some easily identifiable characters like “This is LPP data” at its storage sector(s).
5. After the removal of LPP articles, the data owner will return a sanitized image and a list of removed files to the prosecution for verification and record.
6. If there is any dispute or error in the context of LPP data removal, either party could still recover the erased data from the original media.

Note that in the above proposed procedure, the data owner will be given enough time to examine the image, without the presence of the examiner, in order to identify all LPP files (including those logically deleted, but still exist in the image) to be removed. This provides a more feasible solution to the problem as the volume of storage media is getting bigger and bigger. Requiring face-to-face interaction during the examination process will soon be impractical. This procedure also solves the problem of having the examiner look at the LPP files (as in the case of selective cloning).

On the other hand, to realize the above procedure, we need an effective scheme to check the integrity of the sanitized image to make sure that only the claimed files have been deleted from the image since the deletion process is done without the presence of the examiner. A bit-by-bit checking is not practical as it requires the use of the sealed original storage media and also, it requires the presence of both parties again to overlook the lengthy checking process. In the next section, we describe a scheme that makes use of hash values, without the need to access the sealed original storage media, to perform the integrity check.

5. Integrity issue

To prove the integrity of original bit stream image, we normally use the technique of cryptographic hash value comparison. File hash comparison could prove the logical file at the image is an exact copy of the logical file stored at the original digital storage device, whilst disk hash comparison could prove the whole bit-by-bit imaging or cloning process is successful and has caused no affect to the physical level data of the storage device.

When LPP digital articles are removed from the cloned image, the digital signature of the whole image data could not be maintained, i.e. disk hash change. To verify the integrity of data that are contained in the image, we can use file hash comparison to validate files at logical level. However, it is impossible to verify data at physical level since we could not use the previous disk hash as an index for verification. To overcome the problem, the simplest way is to pre-calculate all the physical sector hash of the original storage device and use that hash set to verify the physical level data at the modified image. In this way, after the relevant sectors are removed, one can easily verify if the integrity of the rest of the storage media is still preserved. Nevertheless, we note that the hash set is huge. Table 1 summarizes the number of hashes, to be calculated against sector size of 512 bytes, that are required for hard disks with typical sizes.

Table 1.

Size	No. of hashes required
160 GB	335,544,320
320 GB	671,088,640
500 GB	1,048,576,000

Though the above approach devours large space, it offers the best accuracy among the other schemes. However, with the rapid changes in technology, the size of hard drive becomes larger and larger and the number of hashes required would be exponentially increased. We note that this methodology may no longer be competent to handle the task practically. To enhance the efficiency, and at the same time maintain the accuracy of the process, we propose a more efficient scheme in the following.

5.1. K-Dimensional hashing scheme

In [14, 15], the authors proposed a k-dimensional hashing scheme to address the issue for checking the integrity of a hard drive even if some of the sectors become bad sectors without storing the hash value for each sector. We develop our scheme based on their idea. Assuming that $k = 2$, their scheme order the sectors in a 2-dimentional plan. Each sector can be represented by two coordinates, denoted as $s_{i,j}$ where $1 \le i, j \le N^{1/2}$, N is total number of sectors. Instead of computing one hash value for each sector, for each i, they form a Row Hashing chain using the sectors $s_{i,j}$ for all j. Only one hash value is computed for each Row Hashing chain. Similarly, for each j, they form a Column Hashing chain using the sectors $s_{i,j}$ for all i. compute one hash value for each Column Hashing chain.

Each sector has been used to compute two hash values. For each good sector, the integrity can be verified as long as there is no bad sector in either the corresponding Row Hashing chain and Column Hashing chain. In our scenario, sectors (containing LPP information) deleted by the owner can be treated as bad sectors.

The advantage of the 2-D scheme is to greatly decrease the number of hash values needed to be stored with $2N^{\frac{1}{2}}$ (See Table 2) compared to N. It becomes feasible to store these hash values easily.

Table 2.

Size	No. of hashes required
160 GB	36634
320 GB	51810
500 GB	64762

5.2. Our scheme

Recall that we want to solve the following problem. Let N be the number of sectors in the hard disk. Let l be the number of sectors (containing LPP information) to be deleted. We want to verify the integrity of the remaining $N-l$ sectors without doing a bit-by-bit comparison with the "sealed" original hard disk.

For convenience, the set of l sectors (the ones that have been crossed in Figure 1) to be deleted is denoted as

$$Sd = \{s_{i,j} \mid 1 \le i \le N^{\frac{1}{2}}, 1 \le j \le N^{\frac{1}{2}}\} \subset S$$

and the remaining $N-l$ sectors denoted as

$$Snd = \{s_{x,y} \mid 1 \le x \le N^{\frac{1}{2}}, 1 \le y \le N^{\frac{1}{2}}\} = S \setminus Sd$$

So the problem can be described as how to verify all $s_{x,y} \in Snd$ after sectors in Sd have been deleted.

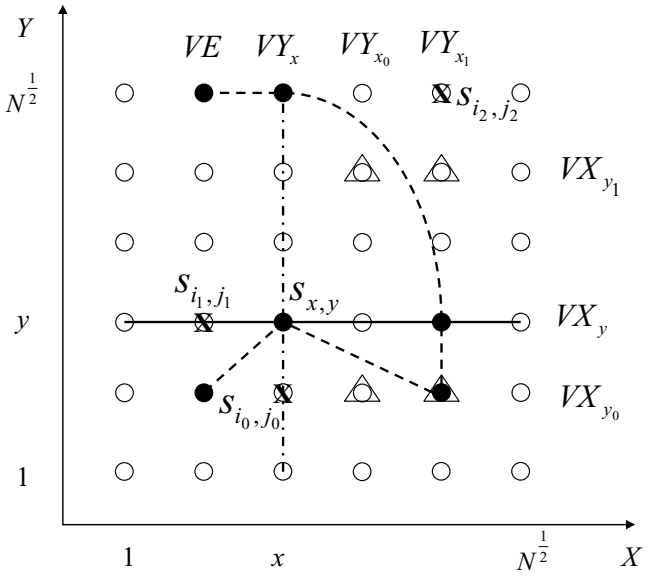

Figure 1. 2-D structure

Let the hash values for the Row Hashing chain and Column Hashing chain be denoted, respectively, as follows (see Figure 1).

$$VX_y = Hash(s_{1,y} \| s_{2,y} \| \cdots \| s_{N^{\frac{1}{2}},y})(1 \le y \le N^{\frac{1}{2}})$$

$$VY_x = Hash(s_{x,1} \| s_{x,2} \| \cdots \| s_{x,N^{\frac{1}{2}}})(1 \le x \le N^{\frac{1}{2}})$$

These hash values for Row Hashing chains and Column Hashing chains can be pre-computed. After the deletion of the l sectors, based on the pre-computed hash values, a

sector $s_{x,y} \in Snd$ can still be verified if no sectors in its corresponding Row Hashing chain or Column Hashing chain have been deleted. If that's the case, to verify whether a $s_{x,y} \in Snd$ is changed, we do the following.

VERIFICATION (1): We recalculate either the hash value of sector chain in column x or that in row y, $VX_y^{'}, VY_x^{'}$ respectively. Obviously if it is satisfied that at least one of the following two equations holds.

$$VX_y = VX_y^{'} \qquad (1)$$

$$VX_y = VX_y^{'} \qquad (2)$$

However in some special cases when there exist two sectors to be deleted s_{i_0,j_0} and s_{i_1,j_1} satisfying that $i_0 = x$ and $j_1 = y$ at the same time, both Eq.(1) and (2) fail.

Formally speaking, for each $s_{x,y}$, it will fail the verification

$$\text{iff } \exists\, s_{i_0,j_0} \in Sd \text{ where } i_0 = x \text{ and } \exists\, s_{i_1,j_1} \in Sd \text{ where } j_1 = y.$$

Otherwise, $s_{x,y}$ is verifiable.

Since it is unacceptable that with certain probability some sectors are not verifiable in real application, we need to further adjust the 2-D hash scheme (modified 2-D hash scheme) as follows:

Let $Sf = \{s_{\alpha,\beta}\} \subset Snd$ represents the sectors that fail the verification. For example, all the black sectors illustrated in Figure 1 are all affected sectors by Sd. These sectors have the common property that they are on the intersection points of two chains, where there is at least one deleted sector in each of the two chains. To verify these sectors, we construct an extra hash chain (see the dash line in Figure 1) of all sectors $\{s_{\alpha,\beta}\}$:

$$VE = Hash(\{s_{\alpha,\beta}\}).$$

Note that it is easy to define an order for the sectors in $\{s_{\alpha,\beta}\}$ for the computation of *VE*. For example, we can sort the sectors according to its first index, then its second index.

VERIFICATION (2): To verify the sectors $s_{\alpha,\beta} \in Sf$, without using Eq.(1) and (2), we compute $VE^{'}$ as the hash value for the sectors in *Sf* and check if

$$VE = VE^{'} \qquad (3).$$

Note that to apply this scheme, we need to modify the "Procedure for Handling LPP information" given in Section IV as follows. Firstly, we need to modify Step 2 to compute all the 2-D hash values when cloning the bit-stream image. Secondly, the following steps needed to be added before Step 4.

3.1 The data owner provides the list of sectors Sd to be deleted. The examiner then computes the list of sectors Sf that cannot be verified using the pre-computed 2-D hash values.

3.2 The value of VE is computed accordingly.

Note that both parties should keep a copy of all hash values computed in the process. Step 3.2 can be computed by the examiner using the original copy of the storage device, even without the presence of the data owner since the data owner can verify the *VE* value himself using the image. We expect that the l may not be a very big number compared to the total number of sectors in the hard drive. Therefore, this computation can be done efficiently. After all hash values have been computed, there is no need to refer to the sealed original hard drive for integrity verification.

5.3. Identification Modified or Wrongly Deleted Sectors

In this scheme, based on the verification process, it is possible to identify the set of sectors that may have been wrongly modified or deleted when there are mismatched hash values that do not satisfy the verification equations (1) or (2).

After the verification, let the set of hash chain values

$$VF = \{VX_{y_0}, VX_{y_1}, \cdots, VX_{y_c}, VY_{x_0}, VY_{x_1}, \cdots, VY_{x_d}, VX_j, VY_i \mid s_{i,j} \in Sd\},$$

be the hash values that fail the verification equations (1) and (2), and

$$VD = \{VX_j, VY_i \mid s_{i,j} \in Sd\}$$

be the set of chain hash values which are not useful in the verification process, that is, there exist deleted sectors in the corresponding Row Hashing chain or Column Hashing chain.

Then, $VF - VD$ are the set of hash chains in which there are sectors $s_{x,y} \in Snd$ which are purposely deleted. To locate these problematic sectors, we can identify all the intersections of these hash chains, i.e.

$$Sp = \{s_{\alpha,\beta} \mid \alpha = x_0, x_1, \cdots, x_d, \beta = y_0, y_1, \cdots, y_c, \alpha \neq i, \beta \neq j\}.$$

For example, referring to Figure 1, if

$$VF = \{VX_{y_0}, VX_{y_1}, VY_{x_0}, VY_{x_1}, VX_j, VY_i \mid s_{i,j} \in Sd\}.$$

$$Sp = \{s_{x_0,y_0}, s_{x_0,y_1}, s_{x_1,y_0}, s_{x_1,y_1}\}.$$

Note that not all of these sectors have been modified. For example, since s_{x_1,y_1} is on the hash chain for *VE*, so if verification equation (3) is satisfied, this sector should not be the problematic sector. In fact, the problematic sectors can only be s_{x_0,y_0}, s_{x_1,y_1} only. However, *Sp* should give a reasonable scope for further investigation.

There is a special case we need to consider. If all the unmatched hash values correspond to the same direction, say all are the Row Hashing chain, then the set of possible problematic sectors will be all the sectors in the related rows.

5.4. Extending Modified 2-D Hash Scheme to 3-D Hash Scheme

There may be a concern on the modified 2-D hash scheme described in the above if there are a lot of sectors that cannot be verified by the pre-computed 2-D hash values. In fact, the number of such sectors is upper bounded by $l(l-1)/2$ since this is the maximum number of intersection points that can be created by the sectors in *Sd*. In practice, the actual number of such sectors should be smaller than this bound. On the other hand, we can easily extend the modified 2-D hash scheme to three dimensions.

For 3-D hash scheme, the N sectors can be arranged in the form of a cube. Let the set of l sectors to be deleted denoted as

$$Sd = \{s_{i,j,k} \mid 1 \le i \le N^{\frac{1}{3}}, 1 \le j \le N^{\frac{1}{3}}, 1 \le k \le N^{\frac{1}{3}}\} \subset S,$$

and the remaining $N-l$ sectors denoted as

$$Snd = \{s_{x,y,z} \mid 1 \le x \le N^{\frac{1}{3}}, 1 \le y \le N^{\frac{1}{3}}, 1 \le z \le N^{\frac{1}{3}}\} = S \setminus Sd.$$

Besides calculating the hash values for row and column chain, hashing chain in the third direction is constructed such that the verification depends on any of the three hash values, as illustrated in Figure 2:

$$VX_{y,z} = Hash(s_{1,y,z} \,||\, s_{2,y,z} \,||\, \cdots \,||\, s_{N^{\frac{1}{3}},y,z}),$$
$$VY_{x,z} = Hash(s_{x,1,z} \,||\, s_{x,2,z} \,||\, \cdots \,||\, s_{x,N^{\frac{1}{3}},z}),$$
$$VZ_{x,y} = Hash(s_{x,y,1} \,||\, s_{x,y,2} \,||\, \cdots \,||\, s_{x,y,N^{\frac{1}{3}}}).$$

The number of hash values to be stored, which is $3N^{\frac{2}{3}}$, will be more than that in the case of 2-D hash scheme (see Table 3). It is still substantially smaller that the number of sectors (that is, computing a hash value for each sector in the hard drive).

Table 3.

Size	No. of hashes required
160 GB	1448619
320 GB	2299539
500 GB	3096382

Again, the sectors that are not verifiable using pre-computed hash values can be made to form an additional hash chain and the corresponding hash value can be computed accordingly. Based on the unmatched hash values during the verification

process, we can also identify a set of possible problematic sectors for further investigation. Extending to 4-D and 5-D hash schemes can be done in a similar way.

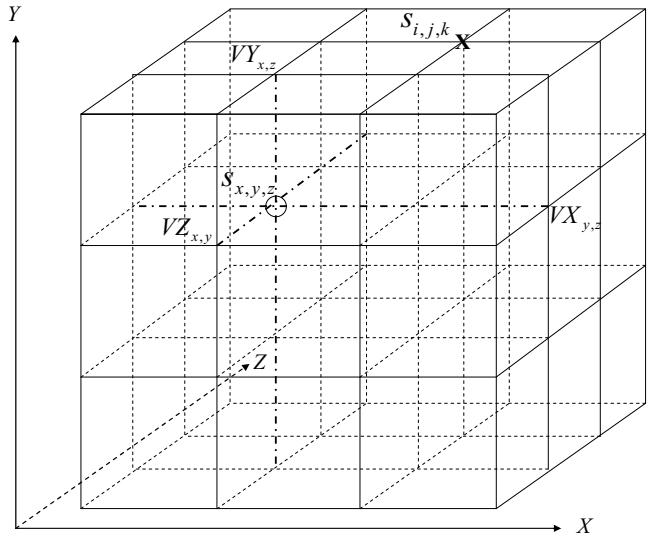

Figure 2. 3-D structure

6. Discussion and Conclusions

In this paper, we address an important, but not adequately addressed in the community, issue for protecting digital Legal Professional Privilege (LPP) information during forensics investigation. We highlighted the differences of digital LPP information and physical LPP information and discussed the difficulties of handling digital LPP data. We also investigated the current practices for handling this kind of information and concluded that these practices cannot guarantee the protection of LLP data or may create obstacles for forensics investigation. Also, both practices rely on the face-to-face interaction between the examiner and the data owner during the identification of LPP information in the target storage media. As the volume of storage device become larger, this involves a lengthy process and it is not practical to require face-to-face interaction.

We then propose a feasible solution to solve this problem. In our proposed approach, there is no need for both parties to get together to identify the LPP information, thus providing a better protection to the privacy of the LPP information and avoiding the lengthy and impractical face-to-face interaction between both parties. A core component of the proposed solution is the integrity checking scheme for the sectors which should not be deleted. The scheme is based on a *k*-D hash scheme developed for checking the integrity of a storage device even if some of the sectors become bad sectors. In the paper, we use $k = 2$ to illustrate our idea on how to modify the *k*-D hash scheme to solve our problem. In fact, the solution can be extended to general *k*.

Using different *k* values has implications on the number of hash values to be stored; and the number of sectors that cannot be verified by pre-computed hash values. As *k* increases, we need to store more hash values. In fact, the number of hash values to be stored is $k \cdot N^{(k-1)/k}$ where *N* is the total number of sectors in the storage device. On the other hand, with a larger value of *k*, it is easier for a sector to be verifiable using pre-

computed hash values since any one of the k hash chains can be used to verify the integrity of the sector. Thus, the number of sectors that cannot be verified using pre-computed hash values will be smaller. More investigation is required to determine what should be the best value of k to be used in practice.

Future research directions include the followings. Based on real cases, a detailed study on the proposed scheme should be carried out to verify the feasibility of the approach as well as to understand the effect of the value of k. The proposed scheme, of course, is not the only solution to the problem. Finding a better scheme and procedure to solve this digital LPP protection problem is always desirable. We hope that this paper can catch the attention of the community to help developing a forensically sound procedure to solve this problem.

7. Acknowledgement

The work described in this paper was partially supported by two grants from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. HKU 7136/04E and HKU 7132/06E)

8. References

[1] P. E. Nygh, P. Butt, *Butterworths Concise Australian Legal Dictionary*, Sydney: Butterworths, 1997.

[2] Legal Professional Privilege, FOI Guide No. 1, Clause 7, (http://www.foi.wa.gov.au/FOIGuides/Clause7.pdf); accessed on 31st January, 2008.

[3] Military Rules of Evidence, Part III, Division IX, Solicitor-Client Privilege, (http://www.canlii.org/ca/regu/crc1049/sec77.html); accessed on 31st January, 2008.

[4] P.R. Rice, *Attorney-Client Privilege in the United States*, 2nd edition, Thompson West, 1999.

[5] R v Peterborough Justice, ex p. Hicks [1977] 1 W.L.R. 1371.

[6] R v King [1983] 1 WLR 411.

[7] DFRWS, Report from the *First Digital Forensic Research Workshop*. DTR-T001-01 FINAL A Road Map for Digital Forensic Research. Final version, November 6, 2001.

[8] *Cavendish lawcards series – Evidence*, Cavendish Publishing Ltd., London, 2004

[9] Ricci S. C. Ieong, "FORZA – Digital forensics investigation framework that incorporate legal issues", *Digital Forensics Research Workshop (DFRWS)*, 2006.

[10] Association of Chief Police Officers (ACPO) - Good practice guide for computer based electronic evidence, (http://www.dataclinic.co.uk/ACPO%20Guide%20v3.0.pdf); accessed on 31st January, 2008.

[11] P. Turner, Selective and intelligent imaging using digital evidence bags, *Digital Investigation*, Volume 3, Supplement 1, pp. 59-64.

[12] Anti Cartel Enforcement Manual, International Competition Network, April 2006, http://www.internationalcompetitionnetwork.org/media/library/conference_5th_capetown_2006/DigitalEvidenceGathering.pdf; accessed on 30th January, 2008.

[13] P. Turner, Unification of evidence from disparate sources (digital evidence bags), *Digital Forensic Research Workshop (DFRWS)*, 2005

[14] Z.L. Jiang, L.C.K. Hui, K.P. Chow, S.M. Yiu, and P.K.Y. Lai. "Improving Disk Sector Integrity Using 3-Dimension Hashing Scheme", to appear in Proceedings of the *2007 International Workshop on Forensics for Future Generation Communication*, 2007.

[15] Z. L. Jiang, L.C.K. Hui, and S.M. Yiu. "Analysis of K-Dimension Hashing Scheme to Improve Disk Sector Integrity", to appear in Proceedings of the *4th Annual IFIP WG 11.9 International Conference on Digital Forensics (ICDF 2008)*, 2008.