Forensic Analysis of Database Tampering

Kyriacos E. Pavlou
and
Richard T. Snodgrass
University of Arizona

Regulations and societal expectations have recently expressed the need to mediate access to valuable databases, even by insiders. One approach is tamper detection via cryptographic hashing. This paper shows how to determine when the tampering occurred, what data was tampered, and thus perhaps ultimately who did the tampering, via forensic analysis. We present four successively more sophisticated forensic analysis algorithms: the Monochromatic, RGBY, Tiled Bitmap, and a3D Algorithms, and characterize their "forensic cost" under worst-case, best-case, and average-case assumptions on the distribution of corruption sites. A lower bound on forensic cost is derived, with RGBY and a3D being shown optimal for a large number of corruptions. We also provide validated cost formulæ for these algorithms and recommendations for the circumstances in which each algorithm is indicated.

Categories and Subject Descriptors: H.2.0 [**Database Management**]: General—*security, integrity, and protection*

General Terms: Algorithms, Performance, Security
Additional Key Words and Phrases: a3D Algorithm, compliant records, forensic analysis algorithm, forensic cost, Monochromatic Algorithm, Polychromatic Algorithm, RGBY Algorithm, Tiled Bitmap Algorithm.

1. INTRODUCTION

Recent regulations require many corporations to ensure trustworthy long-term retention of their routine business documents. The US alone has over 10,000 regulations [11] that mandate how business data should be managed [6; 31] , including the Health Insurance Portability and Accountability Act: HIPAA [29], Canada's PIPEDA, Sarbanes-Oxley Act [30], and PITAC's advisory report on health care [1]. Due to these and to widespread news coverage of collusion between auditors and the companies they audit (e.g., Enron, WorldCom), which helped accelerate passage of the aforementioned laws, there has been interest within the file systems and database communities about built-in mechanisms to detect or even prevent tampering.

One area in which such mechanisms have been applied is *audit log security*. The Orange Book [8] informally defines audit log security in Requirement 4: "Audit

Authors' address: Kyriacos E. Pavlou and Richard T. Snodgrass, Department of Computer Science, University of Arizona, Tucson, AZ 85721-0077, {kpavlou, rts}@cs.arizona.edu

information must be selectively kept and protected so that actions affecting security can be traced to the responsible party. A trusted system must be able to record the occurrences of security-relevant events in an audit log. ... Audit data must be protected from modification and unauthorized destruction to permit detection and after-the-fact investigations of security violations."

The need for audit log security goes far beyond just the financial and medical information systems mentioned above. The 1997 U.S. Food and Drug Administration (FDA) regulation "part 11 of Title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures" (known affectionately as "21 CFR Part 11" or even more endearingly as "62 FR 13430") requires that analytical laboratories collecting data used for new drug approval employ "user independent computer-generated time stamped audit trails" [9].

Audit log security is one component of more general *record management systems* that track documents and their versions, and ensure that a previous version of a document cannot be altered. As an example, *digital notarization services* such as Surety (`www.surety.com`), when provided with a digital document, generate a *notary ID* through secure one-way hashing, thereby locking the contents and time of the notarized documents [14]. Later, when presented with a document and the notary ID, the notarization service can ascertain whether that specific document was notarized, and if so, when.

Compliant records are those required by myriad laws and regulations to follow certain "processes by which they are created, stored, accessed, maintained, and retained" [11]. It is common to use Write-Once-Read-Many (WORM) storage devices to preserve such records [32]. The original record is stored on a write-once optical disk. As the record is modified, all subsequent versions are also captured and stored, with metadata recording the timestamp, optical disk, filename, and other information on the record and its versions.

Such approaches cannot be applied directly to high-performance databases. A copy of the database cannot be versioned and notarized after each transaction. Instead, audit log capabilities must be moved into the DBMS. We previously proposed an innovative approach in which cryptographically-strong one-way hash functions prevent an intruder, including an auditor or an employee or even an unknown bug within the DBMS itself, from silently corrupting the audit log [27]. This is accomplished by hashing data manipulated by transactions and periodically *validating* the audit log database to detect when it has been altered.

The question then arises, what do you do when an intrusion has been detected? At that point, all you know is that at some time in the past, data somewhere in the database has been altered. *Forensic analysis* is needed to ascertain *when* the intrusion occurred, *what* data was altered, and ultimately, *who* the intruder is.

In this paper, we provide a means of systematically performing forensic analysis after an intrusion of an audit log has been detected. (The identification of the intruder is not explicitly dealt with.) We first summarize the originally proposed approach, which provides exactly one bit of information: has the audit log been tampered? We introduce a schematic representation termed a "corruption diagram" for analyzing an intrusion. We then consider how additional validation steps provide a sequence of bits that can dramatically narrow down the "when" and "where." We

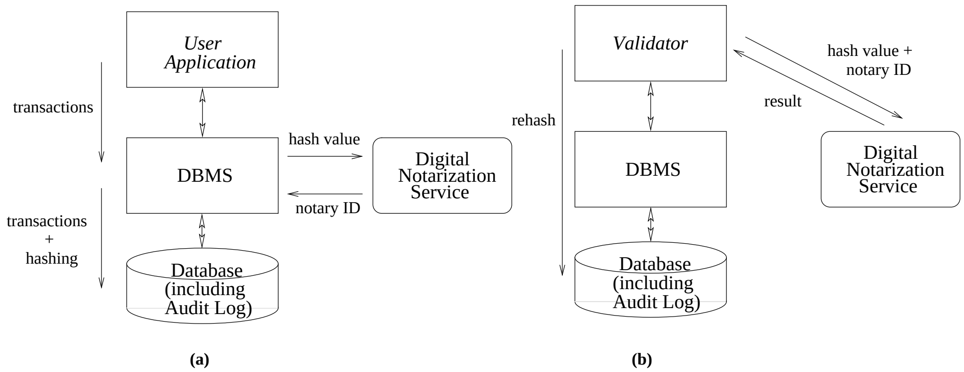


Fig. 1. Online processing (**a**) and Audit log validation (**b**).

examine the corruption diagram for this initial approach; this diagram is central in all of our further analyses. We characterize the "forensic cost" of this algorithm, defined as a sum of the external notarizations and validations required and the area of the uncertainty region(s) in the corruption diagram. We look at the more complex case in which the *timestamp* of the data item is corrupted, along with the data. Such an action by the intruder turns out to greatly increase the uncertainty region. Along the way, we identify some configurations that turn out not to improve the precision of the forensic algorithms, thus helping to cull the most appropriate alternatives.

We then consider computing and notarizing additional sequences of hash values. We first consider the Monochromatic Algorithm; we then present the RGBY, Tiled Bitmap, and a3D Algorithms. For each successively more powerful algorithm, we provide an informal presentation using the corruption diagram, the algorithm in pseudocode, and then a formal analysis of the algorithm's asymptotic run time and forensic cost. We end with a discussion of related and future work. The appendix includes an analysis of the forensic cost for the algorithms, using worst-case, best-case, and average-case assumptions on the distribution of corruption sites.

2. TAMPER DETECTION VIA CRYPTOGRAPHIC HASH FUNCTIONS

In this section we summarize the *tamper detection* approach we previously proposed and implemented [27]. We just give the gist of our approach, so that our forensic analysis techniques can be understood.

This basic approach differentiates two execution phases: *online processing*, in which transactions are run and hash values are digitally notarized, and *validation*, in which the hash values are recomputed and compared with those previously notarized. It is during validation that tampering is detected, when the just-computed hash value doesn't match those previously notarized. The two execution phases constitute together the *normal processing phase* as opposed to the *forensic analysis phase*. Figure 1 illustrates the two phases of normal processing.

In Figure 1(**a**), the user application performs transactions on the database, which insert, delete, and update the rows of the current state. Behind the scenes, the DBMS maintains the audit log by rendering a specified relation as a *transaction-time* table. This instructs the DBMS to retain previous tuples during update and deletion, along with their insertion and deletion/update time (the start and stop timestamps), in a manner completely transparent to the user application [3]. An important property of all data stored in the database is that it is *append-only*: modifications only add information; no information is ever deleted. Hence, if old information is changed in any way, then tampering has occurred. Oracle 11g supports transaction-time tables with its workspace manager [23]. The Immortal DB project aims to provide transaction time database support built into Microsoft SQL Server [19]. How this information is stored (in the log, in the relational store proper, in a separate "archival store" [2]) is not that critical in terms of forensic analysis, as long as previous tuples are accessible in some way. In any case, the DBMS retains for each tuple hidden Start and Stop times, recording when each change occurred. The DBMS ensures that only the current state of the table is accessible to the application, with the rest of the table serving as the audit log. Alternatively, the table itself could be viewed by the application as the audit log. In that case, the application only makes insertions to the audited table; these insertions are associated with a monotonically increasing Start time.

We use a *digital notarization service* that, when provided with a digital document, provides a *notary ID*. Later, during audit log validation, the notarization service can ascertain, when presented with supposedly unaltered document and the notary ID, whether that document was notarized, and if so, when.

On each modification of a tuple, the DBMS obtains a timestamp, computes a *cryptographically strong one-way hash function* of the (new) data in the tuple and the timestamp, and sends that hash value, as a digital document, to the notarization service, obtaining a notary ID. The DBMS stores that ID in the tuple.

Later, an intruder gets access to the database. If he changes the data or a timestamp, the ID will now be inconsistent with the rest of the tuple. The intruder cannot manipulate the data or timestamp so that the ID remains valid, because the hash function is one-way. Note that this holds even when the intruder has access to the hash function itself. He can instead compute a new hash value for the altered tuple, but that hash value won't match the one that was notarized.

An independent audit log validation service later scans the database (as illustrated in Figure 1**(b)**), hashes the data and the timestamp of each tuple, provides it with the ID to the notarization service, which then checks the notarization time with the stored timestamp. The validation service then reports whether the database and the audit log are consistent. If not, either or both have been compromised.

Few assumptions are made about the threat model. The system is secure until an intruder gets access, at which point he has access to everything: the DBMS, the operating system, the hardware, and the data in the database. We still assume that the notarization and validation services remain in the trusted computing base. This can be done by making them geographically and perhaps organizationally separate from the DBMS and the database, thereby effecting correct tamper detection even when the tampering is done by highly-motivated insiders. (A recent FBI study indicates almost half of attacks were by insiders [7].)

The basic mechanism just described provides correct tamper detection. If an intruder modifies even a single byte of the data or its timestamp, the independent validator will detect a mismatch with the notarized document, thereby detecting the tampering. The intruder could simply re-execute the transactions, making whatever changes he wanted, and then replace the original database with his altered one. However, the notarized documents would not match in time. Avoiding tamper detection comes down to inverting the cryptographically-strong one-way hash function. Refinements to this approach and performance limitations are addressed elsewhere [27].

A series of implementation optimizations minimize notarization service interaction and speed up processing within the DBMS: opportunistic hashing, linked hashing, and a transaction ordering list. In concert, these optimizations reduce the run time overhead to just a few percent of the normal running time of a high-performance transaction processing system [27]. For our purposes, the only detail that is important for forensic analysis is that at commit time, the transaction's hash value and the previous hash value are hashed together to obtain a new hash value. Thus, the hash value of each individual transaction is linked in a sequence, with the final value being essentially a hash of all changes to the database since the database was created. For more details on exactly how the tamper detection approach works, please refer to our previous paper [27], which presents the threat model used by this approach, discusses performance issues, and clarifies the role of the external notarization service.

The validator provides a vital piece of information, that tampering has taken place, but doesn't offer much else. Since the hash value is the accumulation of every transaction ever applied to the database, we don't know when the tampering occurred, or what portion of the audit log was corrupted. (Actually, the validator does provide a very vague sense of when: sometime before now, and where: somewhere in the data stored before now.)

It is the subject of the rest of this paper to examine how to perform a forensic analysis of a detected tampering of the database.

3. DEFINITIONS

We now examine tamper detection in more detail. Suppose that we have just detected a *corruption event* (or *CE*), which is any event that corrupts the data and compromises the database. (Table I summarizes the notation used in this paper. Some of the symbols are introduced in subsequent sections.)

The corruption event could be due to an intrusion, some kind of human intervention, a bug in the software (be it the DBMS or the file system or somewhere in the operating system), or a hardware failure, either in the processor or on the disk. There exists a one-to-one correspondence between a CE and its *corruption time* (t_c), which is the actual time instant (in seconds) at which a CE has occurred.

The CE was detected during a validation of the audit log by the *notarization service*, termed a *validation event* (or *VE*). A validation can be scheduled (that is, is periodic) or could be an *ad hoc VE*. The time (instant) at which a *VE* occurred is termed the *time of validation event*, and is denoted by t_v. If validations are periodic, the time interval between two successive validation events is termed the validation interval, or I_V. Tampering is indicated by a *validation failure*, in which the validation service returns *false* for the particular query of a hash value and a

Table I. **Summary of notation used.**

Symbol	Name	Definition
CE	Corruption event	An event that compromises the database
VE	Validation event	The validation of the audit log by the notarization service
NE	Notarization event	The notarization of a document (hash value) by the notarization service
l_c	Corruption locus data	The corrupted data
t_n	Notarization time	The time instant of a NE
t_v	Validation time	The time instant of a VE
t_c	Corruption time	The time instant of a CE
t_l	Locus time	The time instant that l_c was stored
I_V	Validation interval	The time between two successive VEs
I_N	Notarization interval	The time between two successive NEs
R_t	Temporal detection resolution	Finest granularity chosen to express temporal bounds uncertainty of a CE
R_s	Spatial detection resolution	Finest granularity chosen to express spatial bounds uncertainty of a CE
t_{RVS}	Time of most recent validation success	The time instant of the last NE whose revalidation yielded a true result
t_{FVF}	Time of first validation failure	Time instant at which the CE is first detected
USB	Upper spatial bound	Upper bound of the spatial uncertainty of the corruption region
LSB	Lower spatial bound	Lower bound of the spatial uncertainty of the corruption region
UTB	Upper temporal bound	Upper bound of the temporal uncertainty of the corruption region
LTB	Lower temporal bound	Lower bound of the temporal uncertainty of the corruption region
V	Validation factor	The ratio I_V/I_N
N	Notarization factor	The ratio I_N/R_s

notarization time. What is desired is a *validation success*, in which the notarization service returns *true*, stating that everything is OK: the data has not been tampered.

The validator compares the hash value it computes over the data with the hash value that was previously notarized. A *notarization event* (or NE) is the notarization of a document (specifically, a hash value) by the notarization service. As with validation, notarization can be scheduled (is periodic) or can be an *ad hoc notarization event*. Each NE has an associated *notarization time* (t_n), which is a time instant. If notarizations are periodic, the time interval between two successive notarization events is termed the notarization interval, or I_N.

There are several variables associated with each corruption event. The first is the data that has been corrupted, which we term the *corruption locus data* (l_c).

Forensic analysis involves *temporal detection*, the determination of the corruption time, t_c. Forensic analysis also involves *spatial detection*, the determination of "where," that is, the location in the database of the data altered in a CE. (Note that the use of the adjective "spatial" does not refer to a spatial database, but rather *where in the database* the corruption occurred.)

Recall that each transaction is hashed. Therefore, in the absence of other information, such as a previous dump (copy) of the database, the best a forensic analysis can do is to identify the particular transaction that stored the data that was corrupted. Instead of trying to ascertain the corruption locus data, we will instead be concerned with the *locus time* (t_l), the time instant that locus data (l_c) was originally stored. The locus time specifically refers to the time instant when the transaction storing the locus data commits. (Note that here we are referring to the specific *version* of the data that was corrupted. This version might be the original version inserted by the transaction, or a subsequent version created through an update operation.) Hence the task of forensic analysis is to determine two times, t_c and t_l.

A CE can have many l_c's (and hence, many t_l's) associated with it, termed *multi-locus*: an intruder (hardware failure, etc.) might alter many tuples. A CE having only one l_c (such as due to an intruder hoping to remain undetected by making a single, very particular change) is termed a *single-locus CE*.

The finest spatial granularity of the corrupted data would be an explicit attribute of a tuple, or a particular timestamp attribute. However, this proves to be costly and hence we define R_s which is the finest granularity chosen to express the uncertainty of the spatial bounds of a CE. R_s is called the *spatial detection resolution*. This is chosen by the DBA.

Similarly, the finest granularity chosen by the DBA to express the uncertainty of the temporal bounds of a CE is the *temporal detection resolution*, or R_t.

4. THE CORRUPTION DIAGRAM

To explain forensic analysis, we introduce the *Corruption Diagram*, which is a graphical representation of CE(s) in terms of the temporal-spatial dimensions of a database. We have found these diagrams to be very helpful in understanding and communicating the many forensic algorithms we have considered and so we will use them extensively in this paper.

Definition: *A* corruption diagram *is a plot in $\mathbb{R}^2$ having its ordinate associated with real time and its abscissa associated with a partition of the database according to transaction time. This diagram depicts corruption events and is annotated with hash chains and relevant notarization and validation events. At the end of forensic analysis, this diagram can be used to visualize the regions ($\subset \mathbb{R}^2$) where corruption has occurred.*

Let us first consider the simplest case. During validation, we have detected a corruption event. Though we don't know it (yet), assume that this corruption event is a single-locus CE. Furthermore, assume that the CE just altered the *data* of a tuple; no timestamps were changed.

Figure 2 illustrates our simple corruption event. While this figure may appear to be complex, the reader will find that it succinctly captures all the important information regarding what is stored in the database, what is notarized, and what can be determined by the forensic analysis algorithm about the corruption event.

The x-axis represents when the data are stored in the database. The database was created at time 0, and is modified by transactions whose commit time is monotonically increasing along the x-axis. (In temporal database terminology [16], the

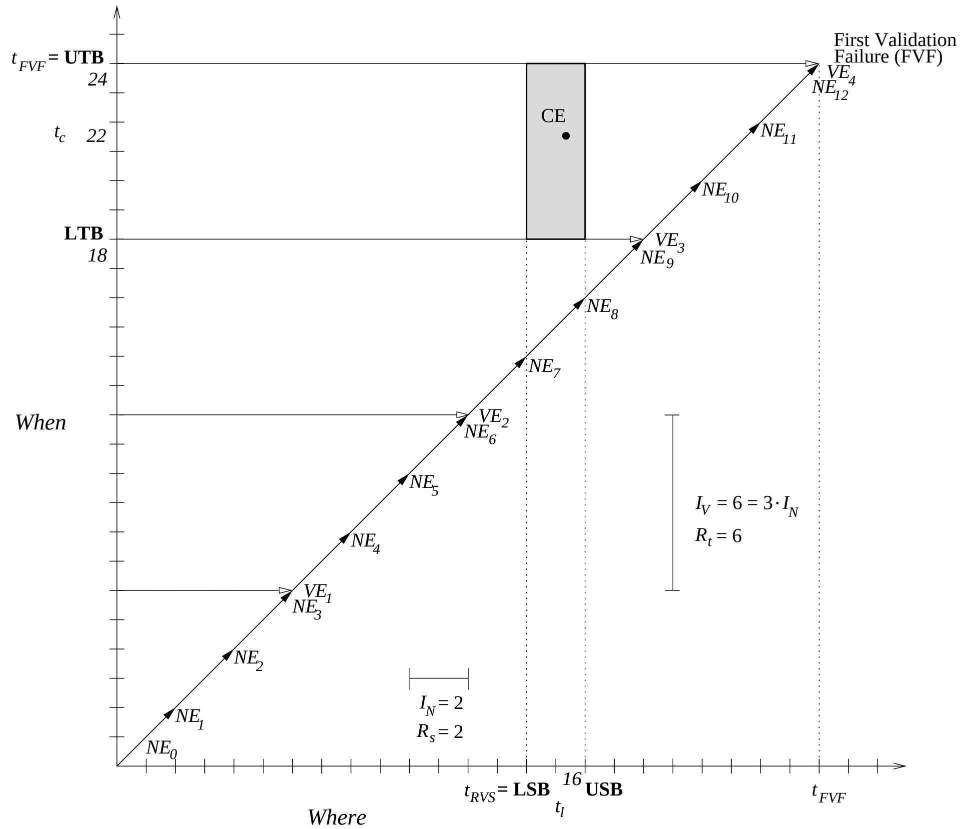


Fig. 2. Corruption diagram for a data-only single-locus retroactive corruption event.

x-axis represents the transaction time of the data.) In this diagram, time moves inexorably to the right.

This axis is labeled "*Where.*" The database grows monotonically as tuples are appended (recall that the database is append-only). As above, we designate "where" a tuple or attribute is in the database by the time of the transaction that inserted that tuple or attribute. The unit of the x-axis is thus (transaction-commit) time. We delimit the days by marking each midnight, or, more accurately, the time of the last transaction to commit before midnight.

A 45-degree line is shown and is termed the *action line*, as all the action in the database occurs on this line. The line terminates at the point labeled "FVF," which is the validation event at which we first became aware of tampering. The *time of first validation failure* (or t_{FVF}) is the time at which the corruption is first detected. (Hence the name: a corruption diagram always terminates at the VE that detected the corruption event.) Note that t_{FVF} is an instance of a t_v, in that t_{FVF} is a specific instance of the time of a validation event, generically denoted by t_v. Also note that in every corruption diagram, t_{FVF} coincides with the current time. For example, in Figure 2 the VE associated with t_{FVF} occurs on the action line, at its terminus, and turns out to be the fourth such validation event, VE_4.

The actual corruption event is shown as a point labeled "CE," which always resides above or on the action line, and below the last *VE*. If we project this point onto the x-axis, we learn "where" (in terms of the locus of corruption, l_c) the corruption event occurred. Hence, the x-axis, which being ostensibly commit time, can also be viewed as a spatial dimension, labeled in locus time instants (t_l). This is why we term the x-axis the *where axis*.

The y-axis represents the temporal dimension (actual time-line) of the database, labeled in time instants. Any point on the action line thus indicates a transaction committing at a particular transaction time (a coordinate on the x-axis) that happened at a clock time (the same coordinate on the y-axis). (In temporal database terminology, the y-axis is valid time, and the database is a *degenerate bitemporal database*, with valid time and transaction time totally correlated [17]. For this reason, the action line is always a 45-degree line. Projecting the CE onto the y-axis tells us when in clock time the corruption occurred, that is, the corruption time, t_c. We label the y-axis with "*When*." The diagram shows that the corruption occurred on day 22 and corrupted an attribute of a tuple stored by a transaction that committed on day 16.

There is a series of points along the action line denoted with "*NE*." These (naturally) identify notarization events, when a hash value was sent to the notarization service. The first notarization event, NE_0, occurs at the origin, when the database was first created. This event hashes the tuples containing the database schema and notarizes that value.

Notarization event NE_1 hashes the transactions occurring during the first two days (here, the notarization interval, I_N, is two days), linking these hash values together using *linked hashing*. This is illustrated with the upward-right-pointing arrow with the solid black arrowhead originating at NE_0 (since the linking starts with the hash value notarized by NE_0) and terminating at NE_1. Each transaction at commit time is hashed; here the "where" (transaction commit time) and "when" (wall-clock time) are synchronized; hence, this occurs on the diagonal. The hash value of the transaction is linked to the previous transaction, generating a linked sequence of transactions that is associated with a hash value notarized at midnight of the second day in wall-clock time and covering all the transactions up to the last one committed before midnight (hence, NE_1 resides on the action line). NE_1 sends the resulting hash value to the digital notarization service.

Similarly, NE_2 hashes two days' worth of transactions, links it with the previous hash value, and notarizes that value. Thus, the value that NE_{12} (at the top right corner of Figure 2) notarizes is computed from all the transactions that committed over the previous 24 days.

In general, all notarization events (except NE_0) occur at the tip of a corresponding *black* hash chain, each starting at the origin and cumulatively hashing the tuples stored in the database between times 0 and that NE's t_n.

Also along the action line are points denoted with "*VE*." These are validation events for which a validation occurred. During VE_1, which occurs at midnight on the sixth day (here, the validation interval, I_V, is six days), rehashes all the data in the database in transaction commit order, denoted by the long right-pointing arrow with a white arrowhead, producing a linked hash value. It sends this value to the notarization service, which responds that this "document" is indeed the one that was previously notarized (by NE_3, using a value computed by linking together the values from NE_0, NE_1, NE_2, and NE_3, each over two days' worth of transactions), thus assuring us that no tampering has occurred in the first six days. (We know this from the diagram, because this *VE* is not at the terminus.) In fact, the diagram shows that VE_1, VE_2, and VE_3 were successful (each scanning a successively larger portion of the database, the portion that existed at the time of validation). The diagram also shows that VE_4, immediately after NE_{12}, failed, as it is marked as FVF; its time t_{FVF} is shown on both axes.

In summary, we now know that at each of the *VE*s up to but not including FVF succeeded. When the validator scanned the database as of that time (t_v for that *VE*), the hash value matched that notarized by the *VE*. Then, at the last *VE*, the FVF, the hash value *didn't* match. The corruption event, CE, occurred before midnight of the 24^{th} day, and corrupted some data stored sometime during those twenty four days. (Note that as the database grows, more tuples must be hashed at each validation. Given that *any* previous hashed tuple could be corrupted, it is unavoidable to examine *every* tuple during validation.)

5. FORENSIC ANALYSIS

Once the corruption has been detected, a *forensic analyzer* (a program) springs into action. The task of this analyzer is to ascertain, as accurately as possible, the *corruption region*: the bounds on "where" and "when" of the corruption.

From the last validation event, we have exactly one bit of information: validation failure. For us to learn anything more, we have to go to other sources of information.

One such source is a backup copy of the database. We could compare, tuple-by-tuple, the backup with the current database to determine quite precisely the "where" (the locus) of the CE. That would also delimit the corruption time, to after the locus time (one cannot corrupt data that has not yet been stored!). Then, from knowing where and very roughly when, the chief information officer (CIO) and chief security officer (CSO) and their staff can examine the actual data (before and after values) to determine who might have made that change.

However, it turns out that the forensic analyzer can use just the database itself to determine bounds on the corruption time and the locus time. The rest of this paper will propose and evaluate the effectiveness of several forensic analysis algorithms.

In fact, we already have one such algorithm, the *trivial forensic analysis algorithm*: on validation failure, return the upper-left triangle, delimited by the when and action axes, denoting that the corruption event occurred before t_{FVF} and altered data stored before t_{FVF}.

Our next algorithm, termed the *Monochromatic Forensic Analysis Algorithm* for reasons that will soon become clear, yields the rectangular corruption region illustrated in the diagram, with an area of 12 days^2 (two days by six days). We provide the trivial and Monochromatic Algorithms as an expository structure to frame the more useful algorithms introduced later.

The most recent *VE* before FVF is VE_3 and it was successful. This implies that the corruption event has occurred in this time period. Thus t_c is somewhere within the last I_V, which always bounds the "when" of the CE.

To bound the "where," the Monochromatic Algorithm can validate prior portions of the database, at times that were earlier notarized. Consider the very first notarization event, NE_1. The forensic analyzer can rehash all the transactions in the database in order, starting with the schema and then from the very first transaction (such data will have a commit time earlier than all other data), and proceeding up to the last transaction before NE_1. (The transaction timestamp stored in each tuple indicates when the tuple should be hashed; a separate tuple sequence number stored in the tuple during online processing indicates the order of hashing these tuples within a transaction.) If that *de novo* hash value matches the notarized hash value, the validation result will be *true*, and this validation will succeed, just like the original one would have, had we done a validation query then. Assume likewise that NE_2 through NE_7 succeed as well.

Of course, the original VE_1 and VE_2, performed during normal database processing, succeeded, but we already knew that. What we are focusing on here are validations of portions of the database performed by the forensic analyzer after tampering was detected. Computing the multiple hash values can be done in parallel by the forensic analyzer. The hash values are computed for each transaction during a single scan of the database and linked in commit order. Whenever a midnight is encountered as a transaction time, the current hash value is retained. When this scan is finished, these hash values can be sent to the notarization service to see if they match.

Now consider NE_8. The corruption diagram implies that the validation of all transactions occurring during day 1 through day 16 failed. That tells us that the "where" of this corruption event was the single I_N interval between the midnight notarizations of NE_7 and NE_8, that is, during day 15 or day 16. Note also that all validations after that, NE_9 through NE_{11}, also fail. In general, we observe that revisiting and revalidating the cumulative hash chains at past notarization events will yield a sequence of validation results that start out to be true and then at some point switch to false (TT...TF...FF). This single switch from true to false is a consequence of the cumulative nature of the black hash chains. We term the time of the last NE whose revalidation yielded a true result (before the sequence of false results starts) the *time of most recent validation success* (t_{RVS}). This t_{RVS} helps bound the where of the CE because the corrupted tuple belongs to a transaction which committed between t_{RVS} and next time database was notarized (whose validation now evaluates to false). t_{RVS} is marked on the *Where* axis of the of the corruption diagram as seen in Figure 2.

In light of the above observations, we define four values,

—the *lower temporal bound*: $LTB := \max(t_{FVF} - I_V, t_{RVS})$,

—the *upper temporal bound*: $UTB := t_{FVF}$,

—the *lower spatial bound*: $LSB := t_{RVS}$, and

—the *upper spatial bound*: $USB := t_{RVS} + I_N$.

These define a corruption region, indicated in Figure 2 as a narrow rectangle, within which the CE must fall. This example shows that, when utilizing the Monochromatic Algorithm, the notarization interval, here $I_N = 2$ days, bounds the "where," and the validation interval, here $I_V = 6$ days, bounds the "when." Hence for this

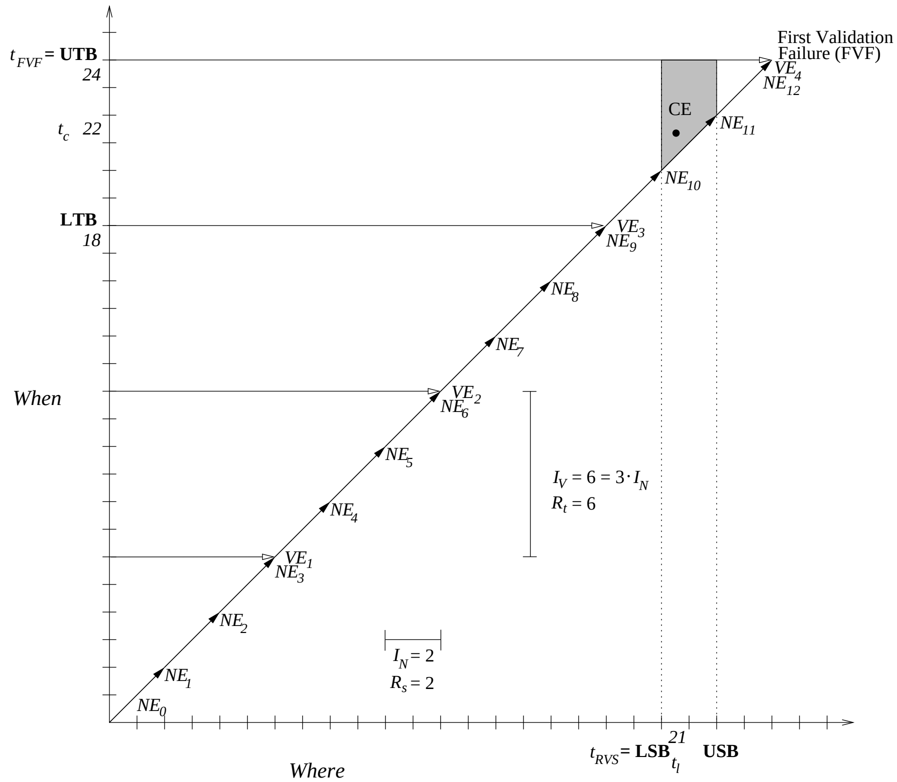


Fig. 3. Corruption diagram for a data-only single-locus introactive corruption event.

algorithm, $R_s = I_N$ and $R_t = I_V$. (More precisely,

$$R_t = UTB - LTB = \min(I_V, t_{FVF} - t_{RVS})$$

due to the fact that R_t can be smaller than I_V for late-breaking corruption events, such as that illustrated in Figure 3.)

The CE just analyzed is termed a *retroactive corruption event*: a CE with locus time t_l appearing before the next to last validation event. Figure 3 illustrates an *introactive corruption event*: a CE with a locus time t_l appearing after the next to last validation event. In this figure, the corruption event occurred on day 22, as before, but altered data on day 21 (rather than day 16 in the previous diagram). NE_{10} is the most recent validation success. Here the corruption region is a trapezoid in the corruption diagram, rather than a rectangle, due to the constraint mentioned earlier that a CE must be on or above the action line ($t_c \geq t_l$). This constraint is reflected in the definition of LTB.

It is worth mentioning here that the CEs described above are ones which only corrupt data. It is conceivable that a CEs can alter the timestamp (transaction commit time) of a tuple. This creates two new independent types of CEs termed postdating or backdating CEs depending on how the timestamp was altered. An analysis of timestamp corruption will be provided in Section 7.

6. NOTARIZATION AND VALIDATION INTERVALS

The two corruption diagrams we have thus far examined assumed a notarization interval of $I_N = 2$ and validation interval of $I_V = 6$. In this case, notarization occurs more frequently than validation and the two processes are in phase, with I_V a multiple of I_N. In such a scenario, we saw that the spatial uncertainty is determined by the notarization interval and the temporal uncertainty by the validation interval. Hence, we obtained tall, thin CE regions. One naturally asks, what about other cases?

Say notarization events occur at midnight every two days, as before, and validation events occur every three days, but at noon. So we might have NE_1 on Monday night, NE_2 on Wednesday night, NE_3 on Friday night, VE_1 on Wednesday at noon, and VE_2 on Saturday at noon. VE_1 rehashes the database up to Monday night and checks that linked hash value with the digital notarization service. It would detect tampering prior to Monday night; tampering with a t_l after Monday would not be detected by VE_1. VE_2 would hash through Friday night; tampering on Tuesday *would* then be detected. Hence, we see that a non-aligned validation just delays detection of tampering. Simply speaking, one can validate only what one has previously notarized.

If the validation interval were shorter than the notarization interval, e.g. $I_N = 2$, $I_V = 1$, say every day at midnight, then a validation on Tuesday at midnight could again only check through Monday night.

Our conclusion is that the validation interval should be equal to or longer than the notarization interval, should be a multiple of the notarization interval, and should be aligned, that is, validation should occur immediately after notarization. Thus we will speak of the *validation factor* V such that $I_V = V \cdot I_N$. As long as this constraint is respected, it is possible to change V, or both I_V and I_N, as desired. This, however, will affect the size of the corruption region and subsequently the cost of the forensic analysis algorithms, as emphasized in Section 9.

7. ANALYZING TIMESTAMP CORRUPTION

The previous section considered a *data-only* corruption event, a CE that does not change timestamps in the tuples. There are two other kinds of corruption events with respect to timestamp corruption. In a *backdating corruption event*, a timestamp is changed to indicate a previous time/date with respect to the original time in the tuple. We term the time a timestamp was backdated *to* the *backdating time*, or t_b. It is always the case that $t_b < t_l$. Similarly, a *postdating corruption event* changes a timestamp to indicate a future time/date with respect to the original commit time in the tuple, with the *postdating time* (t_p) being the time a timestamp was postdated to. It is always the case that $t_l < t_p$. Combined with the previously introduced distinction of retroactive and introactive, these considerations induce six specific corruption event types.

$$\left\{ \begin{array}{c} \textit{Retroactive} \\ \textit{Introactive} \end{array} \right\} \times \left\{ \begin{array}{c} \textit{Data-only} \\ \textit{Backdating} \\ \textit{Postdating} \end{array} \right\}$$

For backdating corruption events, we ask that the forensic analysis determine, to the extent possible, "when" (t_c), "where" (t_l), and "to where" (t_b). Similarly, for postdating corruption events, we want to determine t_c, t_l, and t_p. This is quite challenging given the only information we have, which is a single bit for each query on the notarization service.

It bears mention that neither postdating nor backdating CEs involve movement of the actual tuple to a new location on disk. Instead, these CEs consist entirely of changing an insertion-date timestamp attribute. (We note in passing that in some transaction-time storage organizations the tuples are stored in commit order. If an insertion date is changed during a corruption event, the fact that that tuple is out of order provides another clue, one that we don't exploit in the algorithms proposed here.)

Figure 4 illustrates a retroactive postdating corruption event (denoted by the forward-pointing arrow). On day 22, the timestamp of a tuple written on day 10 was changed to make it appear that that tuple was inserted on day 14 (perhaps to avoid seeming that something happened on day 10). This tampering will be detected by VE_4, which will set the lower and upper temporal bounds of the CE, shown in Figure 4 as $LTB = 18$ and $UTB = 24$. The Monochromatic Algorithm will then go back and rehash the database, querying with the notarization service at NE_0, NE_1, NE_2, ... It will notice that NE_4 is the most recent validation success, because the rehashed sequence will not contain the tampered tuple: its (altered) timestamp implies it was stored on day 14. Given that the query at NE_4 succeeds and that at NE_5 fails, the tampered data must have been originally stored sometime during those two days, thus bounding t_l to day 9 or day 10. This provides the corruption region shown as the left-shaded rectangle in the figure.

Since this is a postdating corruption event, t_p, the date the data was altered to, must be after the local time, t_l. Unfortunately, all subsequent revalidations, from NE_5 onward, will fail, then giving us absolutely no additional information as to the value of t_p. The "to" time is thus somewhere in the shaded trapezoid to the right of the corruption region. (We show this on the corruption diagram as a two-dimensional region, representing the uncertainty of t_c and t_p. Hence, the two shaded regions denote just three uncertainties, in t_c, t_l, and t_p.)

Figure 4 also illustrates a retroactive backdating corruption event (backward-pointing arrow). On day 22, the timestamp of a tuple written on day 14 was changed to make it appear that the tuple in question was inserted on day 10 (perhaps to imply something happened before it actually did). This tampering will be detected by VE_4, which will set the lower and upper temporal bounds of the CE (as in the postdating case). Going back and rehashing the data at NE_0, NE_1, ...the Monochromatic Algorithm will compute that NE_4 is the most recent validation success. The rehashing up to NE_5 will fail to match its notarized value, because the rehashed sequence will erroneously contain the tampered tuple that was originally was stored on day 14. Given that the query at NE_4 succeeds and that at NE_5 fails, the new timestamp must be sometime within those two days, thus bounding t_b to day 9 or day 10. The left-shaded rectangle in the figure illustrates the extent of the imprecision of t_b.

Since this is a backdating corruption event, the date the data was originally

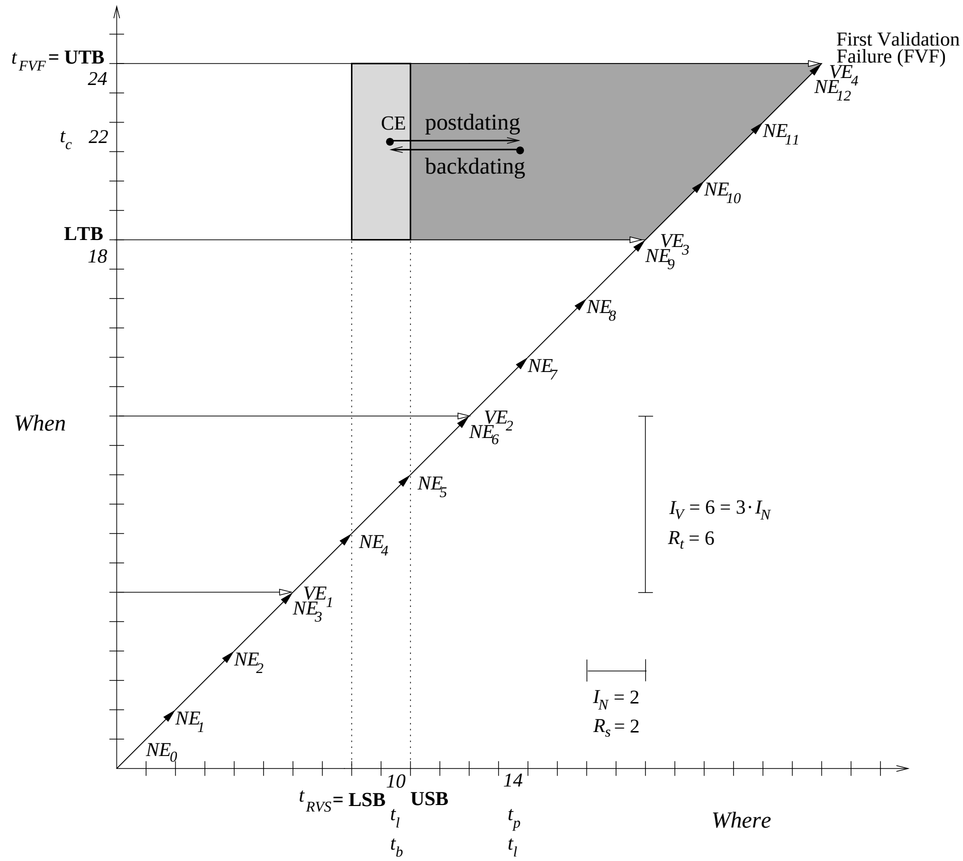


Fig. 4. Corruption diagram for postdating and backdating corruption events.

stored, t_l, must be after the "to" time, t_b. As with postdating CEs, all subsequent revalidations, from NE_5 onward, will fail, then giving us absolutely no additional information as to the value of t_l. The corruption region is thus the shaded trapezoid in the figure.

While we have illustrated backdating and postdating corruption events separately, the Monochromatic Algorithm is unable to differentiate these two kinds of events from each other, or from a data-only corruption event. Rather, the algorithm identifies the RVS, the most recent validation success, and from that puts a two-day bound on *either* t_l or t_b. Because the black link chains that are notarized by NEs are cumulative, once one fails during a rehashing, all future ones will fail. Thus future NEs provide no additional information concerning the corruption event.

To determine more information about the corruption event, we have little choice but to utilize to a greater extent the external notarization service. (Recall that the notarization service is the only thing we can trust after an intrusion.) At the same time, it is important to not slow down regular processing. We'll show how both are possible.

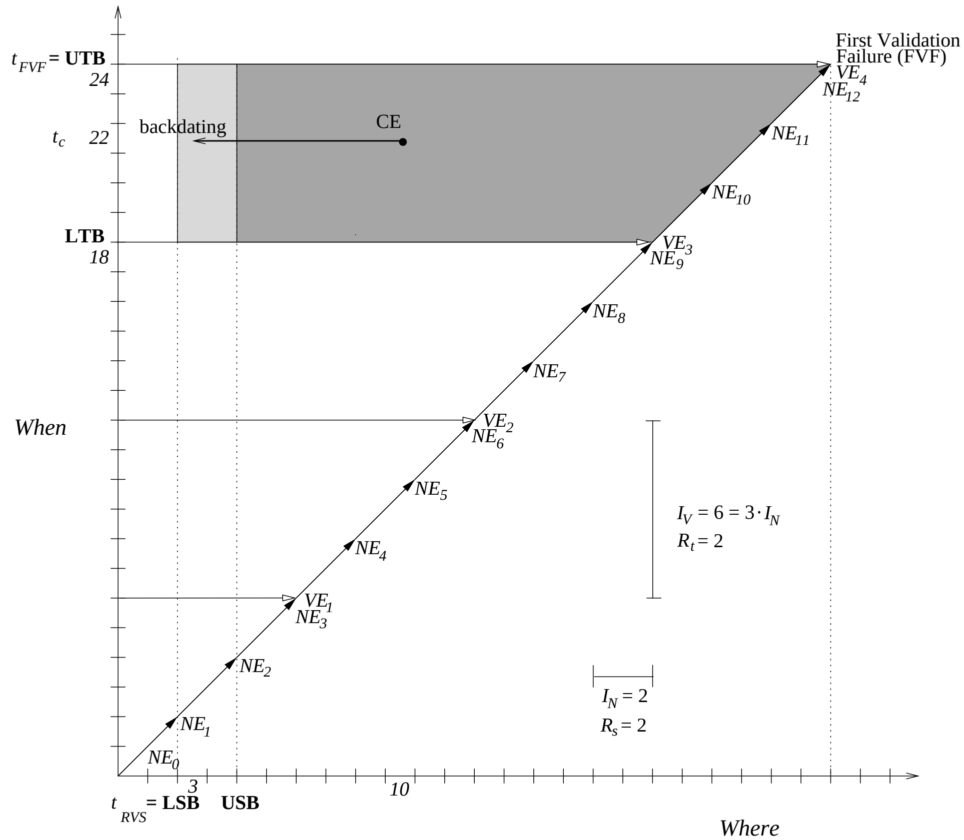


Fig. 5. Corruption diagram for a backdating corruption event.

8. FORENSIC ANALYSIS ALGORITHMS

In this section we provide a uniform presentation and detailed analysis of forensic analysis algorithms. The algorithms presented are the original Monochromatic Algorithm, the RGBY Algorithm, the Tiled Bitmap Algorithm [25], and the a3D Algorithm. Each successive algorithm introduces additional chains during normal processing in order to achieve more detailed results during forensic analysis. This comes at the increased expense of maintaining—hashing and validating—a growing number of hash chains. We show in Section 9 that the increased benefit in each case more than compensates for the increased cost.

The Monochromatic Algorithm uses only the cumulative (black) hash chains we have seen so far, and as such it is the simplest algorithm in terms of implementation.

The RGBY Algorithm introduced here is an improvement of the original RGB Algorithm [24]. The main insight of the previously presented *Red-Green-Blue forensic analysis algorithm* (or simply, the *RGB Algorithm*) is that during notarization events, in addition to reconstructing the entire hash chain (illustrated with the long right-pointed arrows in prior corruption diagrams), the validator can also rehash *portions* of the database and notarize those values, separately from the full chain. In the RGB Algorithm, three new types chains are added, denoted with the colors red, green, and blue, to the original (black) chain in the so-called Monochromatic Algorithm. These hash chains can be computed in parallel; all consist of linked sequences of hash values of individual transactions in commit order. While additional hash values must be computed, no additional disk reads are required. The additional processing is entirely in main memory. The RGBY Algorithm retains the red, green, and blue chains and adds a yellow chain. This renders the new algorithm more regular and more powerful.

The Tiled Bitmap Algorithm extends the idea of the RGBY Algorithm of using partial chains. It lays down a regular pattern (a "tile") of such chains over contiguous segments of the database. What is more, the chains in the tile form a bitmap which can be used for easy identification of the corruption region [25].

The a3D Algorithm introduced here is the most advanced algorithm in the sense that it does not lay repeatedly a "fixed" pattern of hash chains over the database. Instead, the lengths of the partial hash chains change (decrease or increase) as the transaction time increases, in such as way so that at each point in time a complete binary tree (or forest) of hash chains exists on top of the database. This enables forensic analysis to be sped up significantly.

8.1 The Monochromatic Algorithm

We provide the pseudocode for the Monochromatic Algorithm in Figure 6. This algorithm takes three input parameters, as indicated below. t_{FVF} is the *time of first validation failure*, i.e, the time at which the corruption of the log is first detected. In every corruption diagram, t_{FVF} coincides with the current time. I_N is the notarization interval while V, called the validation factor, is the ratio of the validation interval to the notarization interval ($V = I_V/I_N$, $V \in \mathbb{N}$). The algorithm assumes that a single CE transpires in each example. The resolutions for the Monochromatic Algorithm are $R_s = I_N$ and $R_t = I_V = V \cdot I_N$. (The DBA can set the resolutions indirectly, by specifying I_N and V.) Hence, if a CE involving a timestamp transpires and t_l and t_p/t_b are both within the same I_N, such a (backdating or postdating) corruption cannot be distinguished from a data-only CE and hence it is treated as such.

The algorithm first identifies t_{RVS}, the time of most *recent validation success*, and from that puts an I_N bound on *either* t_l or t_b. Then depending on the value of t_{RVS} it distinguishes between introactive and retroactive CEs. It then reports the ("where") bounds on t_l and t_p (or t_b) of both data-only and timestamp CEs since it cannot differentiate between the two. These bounds are given in terms of the upper spatial bound (USB) and the lower spatial bound (LSB). The time interval where time of corruption t_c lies is bounded by the lower and upper temporal bounds (LTB and UTB).

It is worth noting here that the points (t_l, t_c) and (t_p, t_c)—or (t_b, t_c)—must always share the same *when*-coordinate, since both refer to a single CE. The algorithm reports multiple possibilities for the CEs, as the algorithm can't differentiate between all the different types of corruption. Also, the bounds are given in a way that is readable and quite simple. The results are captured by a system of linear inequalities whose solution conveys the extent of the corruption region.

The find_t_{RVS} function, which is used on line 2 above, finds the time of most recent

// input: t_{FVF} is the time of first validation failure
// I_N is the notarization interval
// V is the validation factor
// output: types of and bounds on CE
procedure Monochromatic(t_{FVF}, I_N, V):
1: $I_V \leftarrow V \cdot I_N$
2: $t_{RVS} \leftarrow$ find_t_{RVS}(t_{FVF}, I_N)
3: $USB \leftarrow t_{RVS} + I_N$
4: $LSB \leftarrow t_{RVS}$
5: $UTB \leftarrow t_{FVF}$
6: $LTB \leftarrow \max(t_{FVF} - I_V, t_{RVS})$
7: **if** $t_{RVS} \geq (t_{FVF} - I_V)$ **then report** Introactive CE
8: **else if** $t_{RVS} < (t_{FVF} - I_V)$ **then report** Retroactive CE
9: **report** Data-only CE, $LSB < t_l \leq USB$, $LTB < t_c \leq UTB$
10: **report** Postdating CE, $LSB < t_l \leq USB$, $LTB < c \leq UTB$, $USB < t_p \leq t_{FVF}$
11: **report** Backdating CE, $LSB < t_b \leq USB$, $LTB < t_c \leq UTB$, $USB < t_l \leq t_{FVF}$

// input: t_{FVF} is the time of first validation failure
// I_N is the notarization interval
// output: Schema Corruption if it exists
// t_{RVS} is the time of most recent validation success
procedure find_t_{RVS}(t_{FVF}, I_N):
1: $left \leftarrow 1$
2: $right \leftarrow t_{FVF}$
3: $t_{RVS} \leftarrow \lfloor (left + right)/2 \rfloor$
// since t_{RVS} may not coincide with a NE
4: **if** $(t_{RVS} \bmod I_N) \neq 0$ **then** $t_{RVS} \leftarrow t_{RVS} - (t_{RVS} \bmod I_N)$
5: **while** $(\neg\, BlackChains[\max(1 + (t_{RVS}/I_N), 0)] \vee BlackChains[t_{RVS}/I_N])$
$\wedge\ (right \geq left)$ **do**
6: **if** $\neg\, BlackChains[t_{RVS}/I_N]$ **then**
7: **if** $t_{RVS} = 0$ **then**
8: **report** "Schema Corruption: cannot proceed..."
9: **exit**
10: **if** $t_{RVS} - I_N < 0$ **then** $right \leftarrow 0$ **else** $right \leftarrow t_{RVS} - I_N$
11: **else**
12: **if** $t_{RVS} + I_N > t_{FVF}$ **then** $left \leftarrow t_{FVF}$ **else** $left \leftarrow t_{RVS} + I_N$
13: $t_{RVS} \leftarrow \lfloor (left + right)/2 \rfloor$
14: **if** $(t_{RVS} \bmod I_N) \neq 0$ **then** $t_{RVS} \leftarrow t_{RVS} - (t_{RVS} \bmod I_N)$
15: **return** t_{RVS}

Fig. 6. The Monochromatic Algorithm.

validation success by performing binary search on the cumulative black chains. It revisits past notarizations and by validating them it decides whether to recurse to the right or to the left of the current chain.

In the above algorithm we use an array *BlackChains* of Boolean values to store the results of validation during forensic analysis. The Boolean results are indexed by the subscript of the notarization event considered: the result of validating NE_i is stored at index i, i.e., $BlackChains[i]$. Since we do not wish to pre-compute all this information, the validation results are computed lazily, i.e., whenever needed. On line 7 we report only if there is schema corruption and no other special checks are made in order to deal with this special case of corruption.

Note that on lines 6 and 11 these are the only possibilities for the validation results of the *NE*s in question. No other case ever arises since the results of the validations of the cumulative black chains, considered from right to left, always follow a (single) change from false to true.

The running time of the Monochromatic Algorithm is dominated by the simple binary search required to find t_{RVS}. It ultimately depends on the number of cumulative black hash chains maintained. Hence, the running time of the Monochromatic Algorithm is $O(\lg(t_{FVF}/I_N))$.

8.2 The RGBY Algorithm

We now present an improved version of the RGB Algorithm that we call the *RGBY Algorithm*. RGBY has a more regular structure and avoids some of RGB's ambiguities. The RGBY chains are of the same types as in the original RGB Algorithm. The black cumulative chains are used in conjunction with new *partial hash chains*, i.e., chains which do not extend all the way back to the origin of the corruption diagram. Another difference is that these partial chains are evaluated and notarized during a validation scan of the entire database, and for this reason they are shown running parallel to the *Where* axis (instead of being on the action axis) in Figure 7. The introduction of the partial hash chains will help us deal with more complex scenarios, e.g., multiple data-only CEs or CEs involving timestamp corruption.

The partial hash chains in RGB are computed as follows. (We assume throughout that the validation factor $V = 2$ and I_N is a power of two.)

—for odd i the *Red* chain covers $NE_{2\cdot i-3}$ through $NE_{2\cdot i-1}$

—for even i the *Green* chain covers $NE_{2\cdot i-3}$ through $NE_{2\cdot i-1}$

—for even i the *Blue* chain covers $NE_{2\cdot i-2}$ through $NE_{2\cdot i}$

In this new algorithm we simply introduce a new *Yellow* chain, computed as follows:

—for odd i the *Yellow* chain covers $NE_{2\cdot i-2}$ through $NE_{2\cdot i}$.

In Figure 7 the colors of the partial hash chains are denoted along the *When* axis with the labels **R***ed*, **G***reen*, **B***lue*, and **Y***ellow* (the figure is still in black and white). We use subscripts to differentiate between chains of the same color in the corruption diagram. Each chain takes its subscript from the corresponding *VE*. In the pseudocode instead we use a two-dimensional array called *Chain*. It is indexed as $Chain[color, number]$, where *number* refers to the subscript of the chain while *color* is an integer between 0 and 3 with the following meaning.

—if $color = 0$ then *Chain* refers to a *Blue* chain

—if $color = 1$ then *Chain* refers to a *Green* chain

—if $color = 2$ then *Chain* refers to a *Red* chain

—if $color = 3$ then *Chain* refers to a *Yellow* chain

We also introduce the following comparisons.

$$Chain[color_1, number_1] \prec Chain[color_2, number_2] \textit{ iff}$$
$$(number_1 < number_2) \vee (number_1 = number_2 \wedge color_1 < color_2)$$
$$Chain[color_1, number_1] = Chain[color_2, number_2] \textit{ iff}$$
$$(number_1 = number_2 \wedge color_1 = color_2)$$

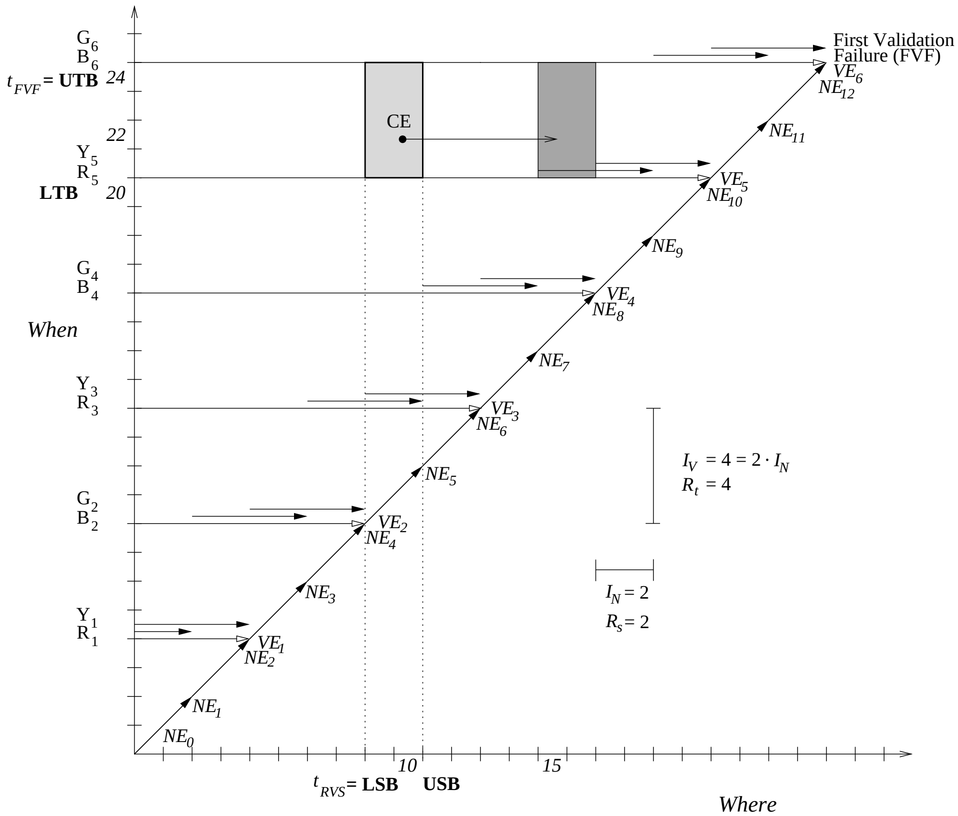


Fig. 7. Corruption diagram for the RGBY Algorithm.

The algorithm requires that $V = 2$. This is because the chains are divided into two groups: red/yellow added at odd-numbered validation events and blue/green added at even-numbered validation events. Note that the find_t_{RVS} routine from the Monochromatic Algorithm is used here. As with the Monochromatic Algorithm, the spatial detection resolution is equal to the validation interval ($R_s = I_V$) and the temporal detection resolution is equal to the notarization interval ($R_t = I_N$).

In this algorithm (shown in Figure 8), as well as in all subsequent ones, instead of using an array *BlackChains* to store the Boolean values of the validation results, as that used in find_t_{RVS}, we use a helper function called val_check. This function takes a hash chain as a parameter and returns the Boolean result of the validation of that chain.

During the normal processing the cumulative black hash chains are evaluated and notarized. During a *VE* the entire database is scanned and validated while the partial (colored) hash chains are evaluated and notarized.

On line 2 we initialize a set which accumulates all the corrupted granules (in this case days). Line 3 computes t_{RVS} and lines 4–7 set the temporal and spatial bounds of the oldest corruption. On lines 9–10 we compute what is the most recent partial chain (*lastChain*) while on lines 11–13 we compute the rightmost chain covering

```
// input:    t_FVF is the time of first validation failure
//           I_N is the notarization interval
// output:   C_set is the set of corrupted granules
//           UTB, LTB are the temporal bounds on t_c
procedure RGBY(t_FVF, I_N):
1:  I_V ← 2 · I_N        // V = 2
2:  C_set ← ∅
3:  t_RVS ← find_t_RVS(t_FVF, I_N)
4:  USB ← t_RVS + I_N
5:  LSB ← t_RVS
6:  UTB ← t_FVF
7:  LTB ← max(t_FVF − I_V, t_RVS)
8:  C_set ← C_set ∪ {t_RVS + 1}
9:  v ← (t_FVF/I_V)
10: lastChain ← Chain[1 + v mod 2, v]
11: n ← (LSB/I_N)
12: s ← ⌈(n/2.0)⌉ + 1
13: currChain ← Chain[(n + 3) mod 4, s]
14: while currChain ⪯ lastChain do
15:     if (currChain.color = Green) ∨ (currChain.color = Yellow) then
16:         succChain.number ← currChain.number + 1
17:     else succChain.number ← currChain.number
18:     succChain.color ← (currChain.color + 1) mod 4
19:     if ¬ val_check(currChain) then
20:         if ¬ val_check(succChain) then
21:             if currChain.color = Blue ∨ currChain.color = Red then
22:                 C_set ← C_set ∪ {2 · (currChain.number − 1) · I_N + 1}
23:             else C_set ← C_set ∪ {2 · currChain.number · I_N − I_N + 1}
24:     currChain ← succChain
25: return C_set, LTB < t_c ≤ UTB
```

Fig. 8. The RGBY Algorithm.

the oldest corruption (*currChain*). In Figure 7 the oldest corruption is in the I_N covering days 9 and 10 so *currChain* is $Yellow_3$. The "while" loop on line 14 linearly scans all the partial chains to the right of t_{RVS}, i.e., from *currChain* to *lastChain* and checks for the pattern ...TFFT... in order to identify the corrupted granules. To achieve this the algorithm must check the validation result of *chainChain* and its immediate successor. Lines 15–18 compute this successor denoted by *succChain*. If both the validation of *currChain* and *succChain* return false then we have located a corruption and the appropriate granule is added to C_{set} (lines 21–23).

The RGBY Algorithm was designed so that it attempts to find more than one CE. However, the main disadvantage of the algorithm is that it cannot distinguish between three contiguous corruptions and two corruptions with an intervening I_N between them. In both cases, the pattern of truth values of the validated partial chains is ...TFFFFT.... Hence, in the latter case the algorithm will report all three $I_V \times I_N$ rectangles as corrupted. This is not desirable because it introduces a false positive result. (Appendix B explains this in more detail.)

The running time of the RGBY Algorithm is $O(\lg(t_{FVF}/I_N) + (t_{FVF}/I_V)) = O(t_{FVF}/I_V)$. The $\lg(t_{FVF}/I_N)$ term arises from invoking find_t_{RVS}. The (t_{FVF}/I_V) term is due to the linear scan of all the colored partial chains which in the worst case would be twice the number of *VE*s.

8.3 The Tiled Bitmap Algorithm

Appendix C presents an improved version of the Polychromatic Algorithm [24] called the *Tiled Bitmap Algorithm*. The original Polychromatic Algorithm utilized multiple *Red* and *Blue* chains while retaining the *Green* chain from the RGB Algorithm. These two kinds of chains and their asymmetry complicated this algorithm. The Tiled Bitmap Algorithm relocates these chains to be more symmetric, resulting in a simpler pattern.

The algorithm also uses a logarithmic number of chains for each "tile" of duration I_N. The spatial resolution in this case can thus be arbitrarily shrunk with the addition of a logarithmic number of chains in the group. The result is that for this algorithm, and not for the previous two, R_s can be less than I_N. More specifically, the number of chains which constitute a tile is $1 + \lg(I_N/R_s)$. We denote the ratio I_N/R_s by N, the *notarization factor*. We require N to be a power of 2. (NB: In the previous two algorithms $N = 1$.) This implies that for all the algorithms, $I_N = N \cdot R_s$ and $R_t = V \cdot I_N = V \cdot N \cdot R_s$. Also, because of the fact that R_s can vary we define D to be the number of R_s units in the time interval from the start until t_{FVF}, that is, $D = t_{FVF}/R_s$.

As an example, in Figure 9, $R_s = 1$, $I_N = N = 2^4 = 16$, $V = 2$, $R_t = 32$, and $D = 64$. If we wanted an R_s of, say, 90 minutes (1/16 day), we would need another 4 chains: $1 + \lg(I_N/R_s) = 1 + \lg(16/\frac{1}{16}) = 9$. (Appendix C explains this figure in much more detail.)

In all of the algorithms presented thus far, discovering corruption (CEs or post-dating intervals) to the right of t_{RVS} is achieved using a linear search which visits potentially all the hash chains in this particular interval. Due to the nature of these algorithms, this linear search is unavoidable. The Tiled Bitmap algorithm reduces the size of the linear search by just iterating on the longest partial chains ($c(0)$) that cover each tile. The running time of the Tiled Bitmap Algorithm is shown in Appendix C to be $O(D)$.

In addition, the Tiled Bitmap Algorithm may handle multiple CEs but it potentially overestimates the degree of corruption by returning the candidate set with granules which may or may not have suffered corruption (false positives). The number of false positives in the Tiled Bitmap Algorithm could be significantly higher than the number of false positives observed in the RGBY Algorithm. Figure 9 shows that the Tiled Bitmap Algorithm will produce a candidate set with the following granules (in this case, days): 19, 20, 23, 24, 27, 28, 31, 32. The corruptions occur on granules 19, 20 and 27 while the rest are false positives. In order to overcome these limitations we introduce the next algorithm.

8.4 The a3D Algorithm

We have seen that the existence of multi-locus CEs can be better handled by summarizing the sites of corruption via candidate sets, instead of trying to find their precise nature. We proceed now to develop a new algorithm that avoids the limitations of all the previous algorithms and at the same time handles the existence of multi-locus CEs successfully. We call this new algorithm the a3D Algorithm for reasons that will become obvious when we analyze it. The a3D Algorithm is illustrated in Figure 10. Even though the corruption diagram shows only VEs, it is

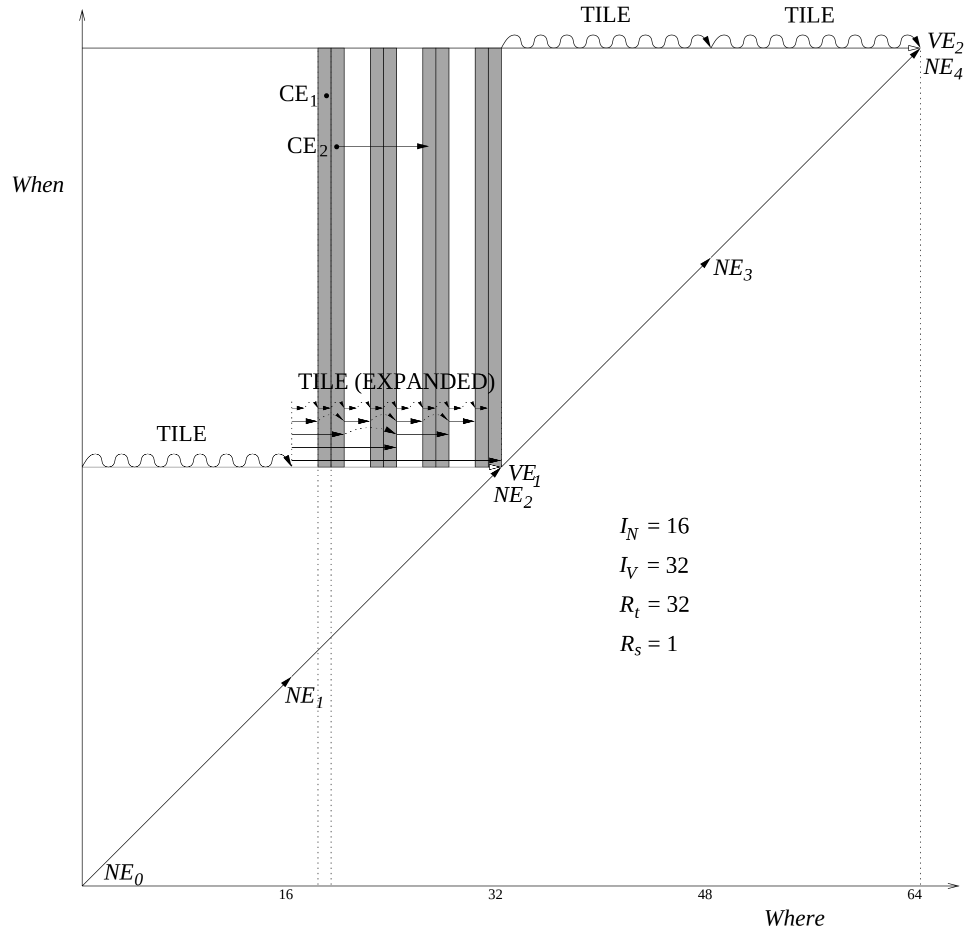


Fig. 9. Corruption diagram for the Tiled Bitmap Algorithm.

implicit that these were preceded immediately by notarization events (not shown). The difference between the Tiled Bitmap Algorithm and a3D is that in the latter each chain is contiguous, that is, it has no gaps. It was the gaps that necessitated the introduction of the candidate sets. Figure 10 shows that the corruption regions in the a3D Algorithm each correspond to a single corruption. All existing corruptions at granules 4, 7, and 10 are identified with no false positives. The difference between a3D and the other algorithms is a slowly increasing number of chains at each validation. In Figure 10, the chains are named using letters B for the *black* cumulative chains and P for the partial chains. Observe that there is one diagonal full chain at VE_1 and two partial chains. VE_2 has a full black chain (B_2, with the subscript the day—R_s unit—of the validation event), retains the chains ($P_{2,0,2}$ and $P_{2,0,3}$) and adds a longer partial chain ($P_{2,1,1}$). (We will explain these three subscripts shortly.) We add another chain at VE_4 ($P_{4,2,1}$) and another chain at VE_8 ($P_{8,3,1}$).

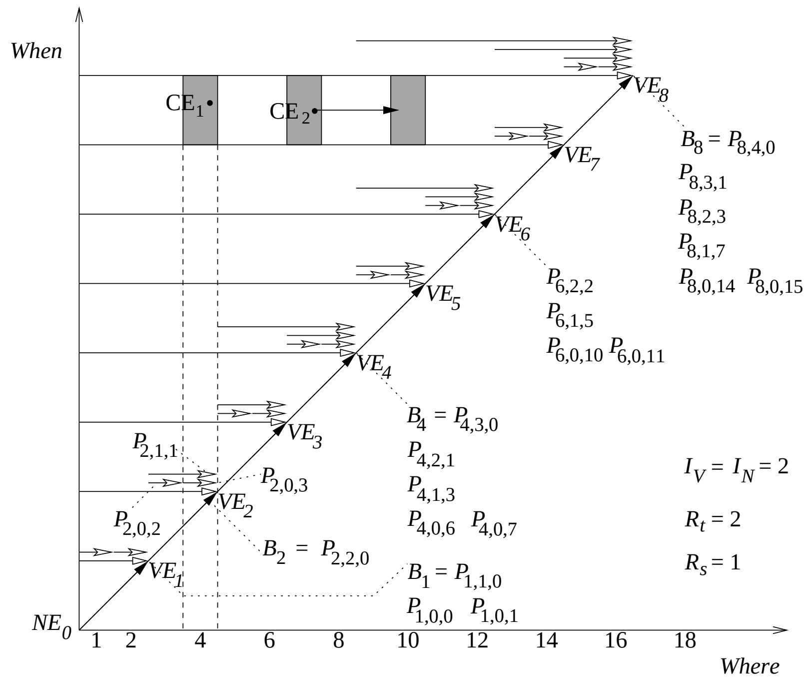


Fig. 10. Corruption diagram for the a3D Algorithm.

The a3D Algorithm assumes that given an R_s, $t_{FVF} \neq 0$, $D = t_{FVF}/R_s$, and $V = 1$ (which implies that $R_t = I_N$).

The beauty of this algorithm is that it decides what chains to add based on the current day/R_s unit. In this way the number of chains increases dynamically, which allows us to perform binary search in order to locate the corruption. If we dissociate the decision of how many chains to add from the current day then we are forced to repeat a certain fixed pattern of hash chains which results in the drawbacks seen in the Tiled Bitmap Algorithm.

During normal processing the algorithm adds partial hash chains (shown with white-tipped arrows). These partial chains are labeled as P with three subscripts. The first subscript is the number m of the current VE, such as $P_{4,2,1}$ added at VE_4. The second subscript, *level*, identifies the (zero-based) "vertical" position of the chain P within a group of chains added at VE_m. This subscript also provides the length of the partial chain as 2^{level}. For example, chain $P_{4,2,1}$ has length $2^2 = 4$. The final subscript, *comp* (for component), determines the "horizontal" position of the chain: all chains within a certain *level* have a position *comp* which ranges from 0 to $2^{level} - 1$. For example, hash chain $P_{4,2,1}$ is the second chain at level 2. The first chain at level 2 is $P_{2,2,0}$ which just happens to be the black chain B_2; the third chain at this level is $P_{6,2,2}$; and the fourth chain is $P_{8,2,3}$.

The addition of partial hash chains allows the algorithm to perform a bottom-up creation of a *binary tree* whose nodes represent the hash chains (see Figure 11). Depending on when the CE transpires there maybe nodes missing from the complete

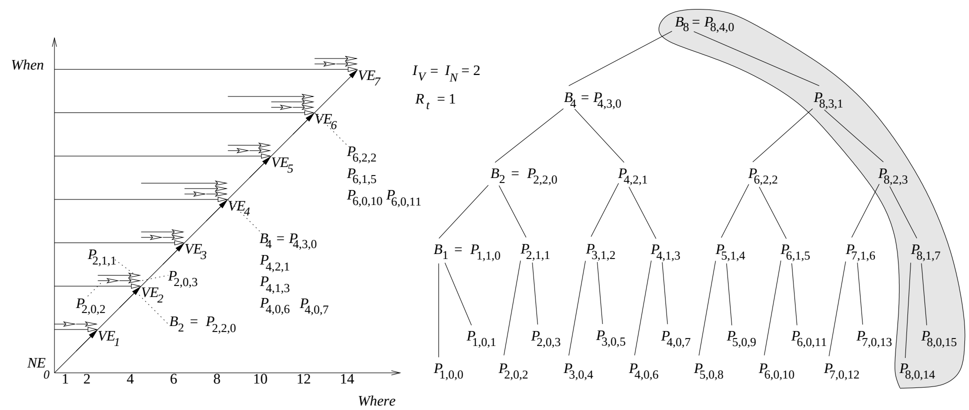


Fig. 11. The a3D Algorithm performs a bottom-up creation of a binary tree.

tree so in reality we have multiple binary trees which are subtrees of the next complete tree. In the above example the nodes/chains missing are those in the shaded region, while there are three complete subtrees each rooted at $B_4 = P_{4,3,0}$, $P_{6,2,2}$, and $P_{7,1,6}$ respectively.

The a3D Algorithm is given in Figure 12. Note that when val_check is called with a hash chain $P[m, level, comp]$ for whom m is a power of 2, $level \geq \lg(N)$, and $comp = 0$, these chains are actually black chains whose validation result can be obtained through $BlackChains[m]$. All black chains appear only on the leftmost path from the root to the leftmost child; however, not all chains on this path are black.

The a3D function evaluates the *height* of the complete tree, regardless of whether we have a single tree or a forest (line 5). Then it calls the recursive a3D_helper function which performs the actual search. In the recursive part of a3D_helper, the function calls itself (lines 8–9, 11–12) with the appropriate hash (sub-)chain only if the current chain does not exist or evaluates to false (line 6). In this case we are relying on short-circuit Boolean evaluation for correctness. All of the compromised granules are accumulated into C_{set}.

The running time of the algorithm is dominated by the successive calls to the recursive function a3D_helper. The worst-case running time is captured by the recursion $T(D) = 2 \cdot T(D/2) + O(1)$, i.e., we have to recurse to both the left and right children. The solution to this recursion gives us $T(D) = \Theta(D)$, so the algorithm is linear in the number of R_s units. In the best case, the algorithm recurses on only one of the two children and thus the running time is $O(\lg D)$.

The algorithm takes its name from the fact that for a given D, the algorithm makes in the worst case $3 \cdot D$ number of notarization contacts, as shown below.

$$\begin{aligned} \textit{Total Number of Notarizations} &= \textit{number of chains in tree} \\ &\quad + \textit{number of black chains not in tree} \\ &= \mathcal{N}(D) \\ &\quad + D/N - (1 + \lfloor \lg(D/N) \rfloor) \end{aligned} \tag{1}$$

```
// input:     t_FVF is the time of first validation failure
//            I_N is the notarization interval
//            R_s spatial detection resolution
// output:    C_set is the set of corrupted granules
//            UTB, LTB are the temporal bounds on t_c
procedure a3D(t_FVF, I_N, R_s):
    C_set ← ∅
    D ← t_FVF / R_s
    N ← I_N / R_s
    m_max ← 2^⌈lg(D/N)⌉
    height ← lg N + lg(m_max)
    C_set ← a3D_helper(P[m_max, height, 0], C_set, N)
    min ← C_set[0]
    if min < t_FVF − I_N then LTB ← t_FVF − I_N
    else LTB ← min
    UTB ← t_FVF
    return C_set, LTB < t_c ≤ UTB
```

```
// input:     P[m, level, comp] is a hash chain that was evaluated on VE_m
//              and whose length depends on level
//            N is the notarization factor
//            C_set an empty set in which the corrupted granules will be accumulated
// output:    C_set is the set of corrupted granules
procedure a3D_helper(P[m, level, comp], C_set, N):
    if level = 0 then
      if exists(P[m, level, comp]) then
        if ¬ val_check(P[m, level, comp]) then C_set ← C_set ∪ {comp}
      return C_set
    else
      if ¬ exists(P[m, level, comp]) ∨ ¬ val_check(P[m, level, comp]) then
        if ¬ (level ≤ lg N) then
            return a3D_helper (P[1/2 · (m + m − (2^level/N)), level − 1, 2 · comp], C_set, N)
            return a3D_helper (P[m, level − 1, 2 · comp + 1], C_set, N)
        else
            return a3D_helper (P[m, level − 1, 2 · comp], C_set, N)
            return a3D_helper (P[m, level − 1, 2 · comp + 1], C_set, N)
```

Fig. 12. The a3D Algorithm.

where

$$\mathcal{N}(D) = \begin{cases} 0 & , D = 0 & (i) \\ 2^{i+1} - 1 = 2 \cdot D - 1 & , D = 2^i, i \in \mathbb{N}, D > 0 & (ii) \\ \mathcal{N}(2^{\lfloor \lg D \rfloor}) + \mathcal{N}(D - 2^{\lfloor \lg D \rfloor}) & , D \bmod 2 = 0 \wedge D \neq 2^i, D > 0 & (iii) \\ \mathcal{N}(D-1) & , D \bmod 2 = 1 & (iv) \end{cases}$$

$\mathcal{N}$ is the number of hash chains which is the same as the number of nodes in the complete binary tree or the forest.

Case (iv) of the above recursion shows that for odd D, $\mathcal{N}(D)$ is always equal to the number of hash chains of the previous even D. For this reason, we only need consider the case when D is even. What case (iii) essentially does at each stage of the recursion is to decompose D into a sum of powers of 2; each such power under the action of $\mathcal{N}$ yields $2^{i+1} - 1$ notarizations. (This is also the number of nodes in the subtree of height i.) Thus, to evaluate this recurrence we examine the binary representation of D. Each position in the binary representation where there is a '1' corresponds to a power of 2 with decimal value 2^i. Summing the results of each one of these decimal values under the action of $\mathcal{N}$ gives the desired solution to $\mathcal{N}(D)$. This solution can be captured mathematically using Iverson brackets [13, p. 24] (here, & is a bit-wise *AND* operation):

$$\mathcal{N}(D) = \sum_{i=0}^{\lfloor \lg D \rfloor} (2^{i+1} - 1) \cdot [D \& 2^i \neq 0] \ .$$

The total number of notarizations is bounded above by the number $3 \cdot D$. This loose bound can be derived by simply assuming that the initial value of D is a power of 2. Assuming also that the complete binary tree has height $H = \lg D$, then

$$\begin{aligned} \textit{Total Number of Notarizations} \ &\leq \ 2 \cdot D - 1 + D/N - (1 + \lfloor \lg(D/N) \rfloor) \\ &< \ 2 \cdot D + D/N \qquad \text{minimum value of } N = 1 \\ &\leq \ 3 \cdot D \end{aligned}$$

8.5 Summary

We have presented four forensic analysis algorithms: Monochromatic, RGBY, Tiled Bitmap, and a3D.

Assuming worst case scenarios, the running time of the Monochromatic Algorithm is $O(\lg D)$; for the rest it is $O(D)$. Each of these algorithms manages the trade-off between effort during normal processing and effort during forensic analysis; the algorithms differ in the precision of their forensic analysis. So while the Monochromatic Algorithm has the fastest running time, it offers no information beyond the approximate location of the earliest corruption. The other algorithms work harder, but also provide more precise forensic information. In order to more comprehensively compare these algorithms, we desire to capture this tradeoff and resulting precision in a single measure.

9. FORENSIC COST

We define the forensic cost as a function of D (expressed as the number of R_s units), N, the notarization factor (with $I_N = N \cdot R_s$), V, the validation factor (with $V = I_V / I_N$), and κ, the number of *corruption sites* (the total number of t_l's, t_b's, and t_p's). A corruption site differs from a CE because a single timestamp CE has two corruption sites.

$$\begin{aligned} FC(D,N,V,\kappa) \ = \ &\alpha \cdot \textit{NormalProcessing}(D,N,V) + \beta \cdot \textit{ForensicAnalysis}(D,N,V,\kappa) \\ &+ \gamma \cdot \ \textit{Area}_P(D,N,V,\kappa) + \delta \cdot \ \textit{Area}_U(D,N,V,\kappa) \end{aligned}$$

Forensic cost is a sum of four components, each representing a cost that we would like a forensic analysis algorithm to minimize, and each weighted by a separate constant factor: α, β, γ, and δ. The first component, *NormalProcessing*, is the number of notarizations and validations made during normal processing in a span of D days. The second component, *ForensicAnalysis*, is the cost of forensic analysis in terms of the number of validations made by the algorithm to yield a result. Note that this is different from the running time of the algorithm. The rationale behind this quantity is that each notarization or validation involves an interaction with the external digital notarization service, which costs real money.

The third and fourth components informally indicate the manual labor required after automatic forensic analysis to identify exactly where and when the corruption happened. This manual labor is very roughly proportional to the uncertainty of the information returned by the forensic analysis algorithm. It turns out that there are two kinds of uncertainties, formalized as different areas (to be described shortly). That these components have different units than the first two components is accommodated by the weights.

In order to make the definition of forensic cost applicable to multiple corruption events we need to distinguish between three regions within the corruption diagram. These different areas are the result of the forensic analysis algorithm identifying the corrupted granules. This distinction is based on the *information content* of each type.

—$Area_P$ or *corruption positive area* is the area of the region in which the forensic algorithm has established that corruption has definitively occurred.

—$Area_U$ or *corruption unknown area* is the area of the region in which we don't know *if* or *where* a corruption has occurred.

—$Area_N$ or *corruption negative area* is the area of the region in which the forensic algorithm has established that *no* corruption has occurred.

Each corruption site is associated with these three types of regions of varying area. More specifically, each site induces a partition of the horizontal trapezoid bound by the latest validation interval into three types of forensic area. Figure 13 shows this for a specific example of the RGBY Algorithm with two corruption events (CE_1, CE_2) and three corruption sites ($\kappa = 3$). For each corruption site, the sum of the areas, denoted by $TotalArea = Area_P + Area_U + Area_N$, corresponds to the horizontal trapezoid as shown. Hence, $TotalArea = (V \cdot N) \cdot (D - (1/2) \cdot V \cdot N)$. Moreover, the forensic cost is a function of the number of corruption sites κ, each associated with the three areas $Area_P$, $Area_U$, $Area_N$. Hence, in evaluating the forensic cost of a particular algorithm we have to compute $Area_P$ and $Area_U$ for all κ, e.g., $Area_P(D, N, V, \kappa) = \sum_\kappa Area_P$. The stronger the algorithm the less costly it is, with smaller $Area_P$ and $Area_U$. It is also desirable that $Area_N$ is large but since $TotalArea$ is constant this is achieved automatically by minimizing $Area_P$ and $Area_U$.

We now proceed to compute the forensic cost of our algorithms. We ignore the weights, as these constant factors will not be relevant when we use order notation.

9.1 The Monochromatic Algorithm

In the Monochromatic Algorithm, the spatial detection resolution (R_s) is the notarization interval, I_N, i.e., $N = 1$. Recall that the Monochromatic Algorithm can only detect a single corruption site, even though there could be κ of them in a single corruption diagram.

$$\begin{aligned} NormalProcessing_{mono} &= \textit{Number of Notarizations} \\ &\quad + \textit{Number of Validations} \\ &= D \\ &\quad + D/V \end{aligned}$$

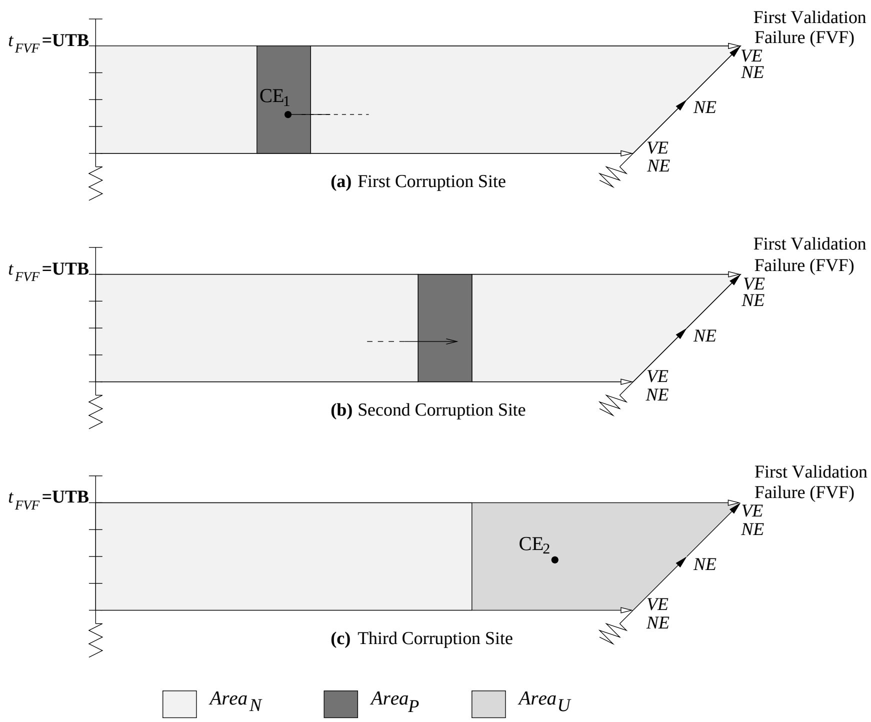


Fig. 13. Three types of forensic area for RGBY and $\kappa = 3$.

In forensic analysis calculations we require D to be a multiple of V because t_{FVF} is a multiple of I_V and only at that time instant can the forensic analysis phase start. $\mathit{ForensicAnalysis}_{mono} = 2 \cdot \lg D$ since t_{RVS} is found via binary search on the black chains; the factor of two is because a pair of contiguous chains must be consulted to determine which direction to continue the search.

For the detected corruption site $Area_P$ has a different shape depending on the position of the corruption site. As the corruption site moves from left to right (from earlier days to later days), the shape of the region changes from rectangular, to trapezoidal, and finally, to triangular. However, since we are dealing with worst case scenario, the upper bound of $Area_P$ is $V \cdot N^2 = V$. Figure 14 shows such a worst case distribution of κ corruption sites and how each site partitions the horizontal trapezoid into different forensic areas. In the worst case, the corruption detected occurs within the first I_N which makes $Area_P = 0$ of all other corruption sites because they cannot be detected. This results in

$$\begin{aligned} Area_U &= (\kappa - 1) \cdot (\mathit{TotalArea} - V) \\ &= (\kappa - 1) \cdot [V \cdot (D - (1/2) \cdot V) - V] \\ &= (\kappa - 1) \cdot V \cdot (D - (1/2) \cdot V - 1) \end{aligned}$$

as shown in Table II.

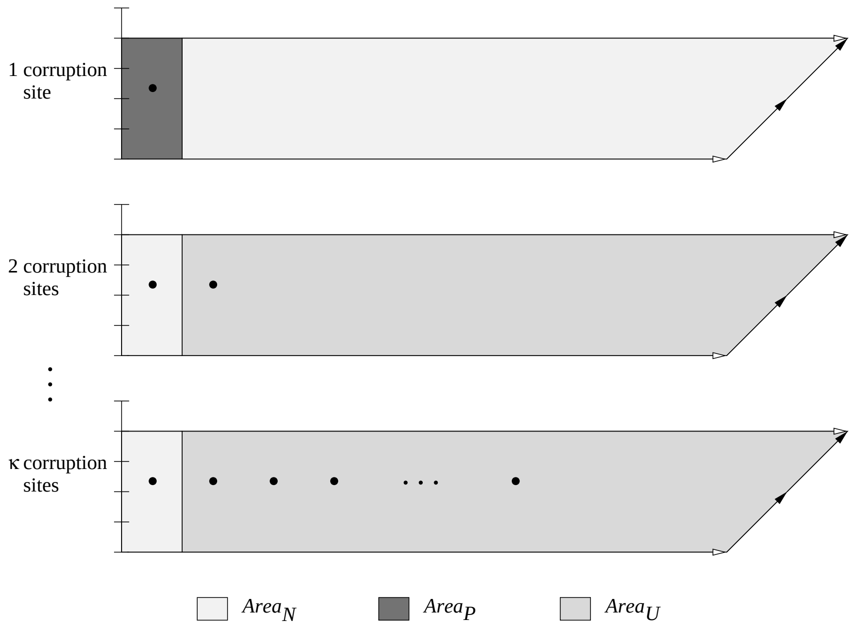


Fig. 14. Three types of forensic area for Monochromatic and κ corruption sites.

Table II. **The forensic areas for $1 \leq \kappa \leq D$ corruption sites (Monochromatic).**

# Corruption Sites ($1 \leq \kappa \leq D$)	$Area_P$	$Area_U$	$Area_N$
1	V	0	$TotalArea - V$
2	0	$TotalArea - V$	V
⋮	⋮	⋮	⋮
κ	0	$TotalArea - V$	V

Hence the forensic cost for the Monochromatic Algorithm is as follows.

$$
\begin{aligned}
FC_{mono}(D, I_N, V, \kappa) \;=\; & (D + D/V + 2 \cdot \lg D) \\
& + (V + \sum_{i=2}^{\kappa} (TotalArea - V))
\end{aligned}
$$

We consider the forensic cost of a single corruption site ($\kappa = 1$) separately from the cases where $\kappa > 1$, the reason being the area breakdown is different in the two cases. Note that for $\kappa = 1$, $\sum_{i=2}^{\kappa}(TotalArea - V)$ is an empty sum, equal to zero.

$$
\begin{aligned}
FC_{mono}(D,1,V,1) &= (D + D/V + 2 \cdot \lg D) + V \\
&= O(V + D) \\
FC_{mono}(D,1,V,\kappa \geq 2) &= (D + D/V + 2 \cdot \lg D) \\
&\quad + (V + (\kappa - 1) \cdot (\mathit{TotalArea} - V)) \qquad (2) \\
&= O(\kappa \cdot V \cdot D)
\end{aligned}
$$

In order to arrive at the order notation we make, here and in the following sections, the simplifying assumptions that $1 \leq V \leq \kappa \leq D$ and $1 \leq N \leq \kappa \leq D$.

9.2 Summary

In Appendix D we perform a similar worst-case forensic cost analysis for the RGBY, Tiled Bitmap, and a3D Algorithms; Appendices E and F provide best-case and average-case analyses, respectively, for all four algorithms.

We summarize the forensic cost for worst-case distribution of corruption sites of the algorithms in Table III. Tables IV and V summarize the forensic cost for average-case and best-case forensic cost, respectively. In the first two tables, we consider the number of corruptions $\kappa = 1$ separately from $1 < \kappa \leq D$ for the Monochromatic Algorithm. Recall that the forensic cost is a function of D, N, V, and κ and that for some of the algorithms N or V may be fixed.

In Table III we see in the rightmost column that Monochromatic depends on the product of κ and D whereas RGBY depends on their sum. Tiled Bitmap has a complex combination of N and V and a3D adds a $\lg D$ multiplier to κ. If we consider the case when $\kappa = 1$ for all algorithms we see that they are generally linear in D, except for Tiled Bitmap.

Observe that Table IV (average case) mirrors almost exactly the forensic cost of the worst-case distribution shown in Table III. This is not the case with Table V where the Monochromatic Algorithm is very cheap under best-case distribution and thus has a clear advantage over Tiled Bitmap and a3D. However, this only happens in the unlikely case where the position of the κ corruption sites allows the Monochromatic Algorithm to definitively identify them all.

In Table V (best case), for the Monochromatic Algorithm we see that the forensic cost is lowest under best-case distribution while for average-case and worst-case the forensic costs are asymptotically the same. Specifically, the number of granules D starts as an additive factor $O(\kappa \cdot V + D)$ in the best case and becomes a multiplicative factor $O(\kappa \cdot V \cdot D)$ in the average and worst cases. The forensic cost of the RGBY algorithm under all assumed distributions remains the same and is equal $O(\kappa + D)$. The forensic cost of the Tiled Bitmap Algorithm differs under each distribution. The difference lies with the exponent of N in the first term which starts from 1, goes to $\lg 3$ and then to 2. The a3D Algorithm, like the RGBY Algorithm, is very stable, with the same forensic cost of $O(\kappa \cdot N + D + \kappa \cdot \lg D)$ under any assumed distribution of corruption events.

9.3 Audit System Implementation

A full implementation of the audit system was built on top of the TUC (Temporal Upward Compatibility), CLK (Clock), and STP (Stamper) modules that were previously added to an underlying Berkeley DB system so that it could support

Table III. **Summary of the forensic cost assuming worst-case distribution of corruption sites.**

Algorithm	Worst-Case Forensic Cost	
	($\kappa = 1$)	($1 < \kappa \leq D$)
Monochromatic	$O(V + D)$	$O(\kappa \cdot V \cdot D)$
RGBY	$O(\kappa + D)$	
Tiled Bitmap	$O(\kappa \cdot V \cdot N^2 + (D \cdot \lg N)/N + \lg D)$	
a3D	$O(\kappa \cdot N + D + \kappa \cdot \lg D)$	

Table IV. **Summary of the forensic cost assuming average-case distribution of corruption sites.**

Algorithm	Average-Case Forensic Cost	
	($\kappa = 1$)	($1 < \kappa \leq D$)
Monochromatic	$O(V + D)$	$O(\kappa \cdot V \cdot D)$
RGBY	$O(\kappa + D)$	
Tiled Bitmap	$O(\kappa \cdot V \cdot N^{\lg 3} + (D \cdot \lg N)/N + \lg D)$	
a3D	$O(\kappa \cdot N + D + \kappa \cdot \lg D)$	

Table V. **Summary of the forensic cost assuming best-case distribution of corruption sites.**

Algorithm	Best-Case Forensic Cost
	($1 \leq \kappa \leq D$)
Monochromatic	$O(\kappa \cdot V + D)$
RGBY	$O(\kappa + D)$
Tiled Bitmap	$O(\kappa \cdot V \cdot N + (D \cdot \lg N)/N + \lg D)$
a3D	$O(\kappa \cdot N + D + \kappa \cdot \lg D)$

transaction time [27]. A notarization service requester utility and a database validator utility were implemented as separately running programs; both send requests to and receive responses from an external digital notarization service, in this case Surety. The existence of the audit system imposed a 15% increase in time in the worst case when tuples are sufficiently small (10 bytes). The impact on time when record size and record number were larger was even less than 15%. Hence the overhead for runtime hashing is small. The Monochromatic forensic analysis algorithm has been incorporated into this system, and the rest of the algorithms are

Table VI. **Settings used in experimental validation of forensic cost assuming worst-case distribution of corruption sites. (Values in bold are non-configurable.)**

Parameters	**Algorithm**			
	Monochromatic	RGBY	Tiled Bitmap	a3D
R_s	1	1	1	1
N	**1**	**1**	8	8
V	8	**2**	1	**1**
D	256	256	256	256

in the process of being incorporated. We can make the following observations. We have an idea of what the overhead is for the Monochromatic Algorithm because the normal processing part was evaluated before [27]; the only part that is missing is the forensic analysis phase which revalidates past hash chains. All algorithms have the same number of I/O operations (and hence performance in terms of time) as the Monochromatic for the normal processing phase, since for all algorithms the database is scanned entirely only during validations.

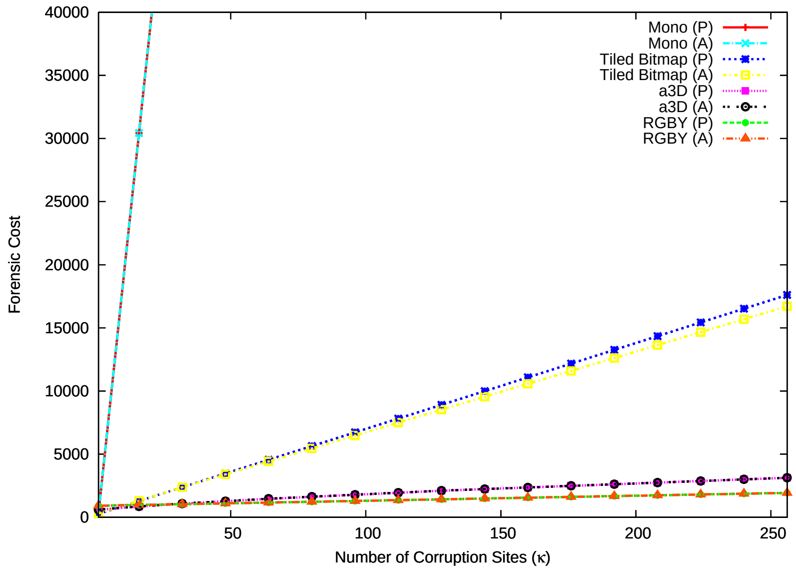
9.4 Illustrating and Validating the Forensic Cost

We have implemented the Monochromatic, RGBY, Tiled Bitmap, and a3D Algorithms in C. The entire implementation is approximately 1480 lines long and the source code is available at `http://www.cs.arizona.edu/projects/tau/tbdb/`. The forensic cost has been validated experimentally by inserting counters in the appropriate places in the code. More specifically, the forensic cost and its normal processing component have been validated for values $1 \leq D \leq 256$ and $1 \leq \kappa \leq 256$ as shown in Figures 15, 16, and 17.

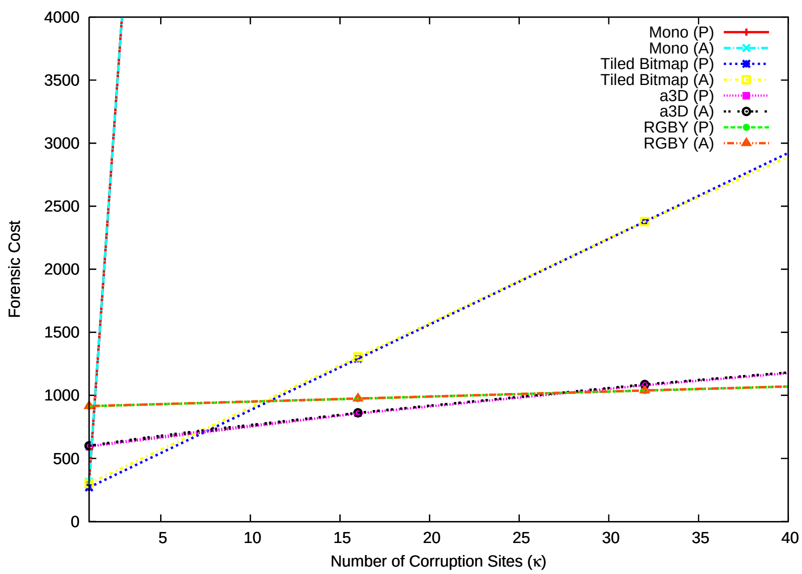
To examine the effects of the various parameters on the theoretical cost, we provide graphs showing the growth of forensic cost against these parameters. These are drawn on the same set of axes as the graphs derived experimentally. In all graphs, we have uniformly used $D = 256$ and $R_s = 1$. For the Monochromatic Algorithm, N is required to be 1, so $I_N = 1$, and we also set $V = 8$. For the RGBY Algorithm, N is also required to be 1 and V is required to be 2, so this dictates $R_t = 2$. For the Tiled Bitmap Algorithm, we set $N = 8$ which implies four chains, and we also set $V = 1$. For the a3D Algorithm, we similarly set $N = 8$ and $V = 1$. All algorithms have $R_t = 8$ except for RGBY. The settings used in the experimental validation are summarized in Table VI.

Rather than using the cost formulas in order notation to create the graphs, we used the more involved (and more accurate) cost functions derived for each algorithm: equation (2) on page 31 for the Monochromatic Algorithm, equation (3) on page App–11 for the RGBY Algorithm, and equation (4) on page App–13 for the Tiled Bitmap Algorithm. For the a3D Algorithm we used the even more precise recursive formula equation (5) on page App–14 to calculate the cost of normal processing instead of the one shown within (6) on page App–17. Also, for values of D that are not a multiple of $V \cdot I_N$ we use the largest multiple of $V \cdot I_N$ less than D to calculate the cost of the forensic analysis stage.

Note that all cost plots show both the predicted forensic cost (denoted by "(P)" in the plot legend) and the actual forensic cost values (denoted by "(A)" in the plot



(a) $1 \leq \kappa \leq 256$



(b) $1 \leq \kappa \leq 40$

Fig. 15. Forensic cost against κ for $D = 256$.

legend). The different types of symbols on the curves were added for clarity and correspond to a subset of the actual data points.

We start by examining the growth of forensic cost of the algorithms against κ, as shown in the graphs in Figure 15. Figure 15**(a)** shows how the forensic cost increases with κ. Most of the predicted forensic costs are very close to the actual values and in these cases (e.g., a3D algorithm) the two lines overlap. Figure 15**(b)**

Table VII. **Sample forensic costs for the four implemented algorithms.**

Forensic Cost	Monochromatic	RGBY	Tiled Bitmap	a3D
Predicted	512352	1934	17610	3128
Actual	512354	1935	16714	3134

is a magnification of the region in Figure 15(**a**) where κ takes values between 1 and 40. The cheapest algorithm for $\kappa = D$ is RGBY while the most expensive is Monochromatic. Observe in Figure 15(**b**) that for $\kappa = 1$ the costs of Monochromatic and Tiled Bitmap are comparable and have the lowest value *of all other* algorithms.

Even more interestingly, the RGBY algorithm starts off as being the most expensive algorithm and then becomes the cheapest. This can be explained by observing that ambiguity in the corruption region (large $Area_U$ for $\kappa > 1$) increases the cost of the Monochromatic Algorithm. The Tiled Bitmap Algorithm suffers considerably from false positives (for every true corruption site there exist $N - 1$ false positives) On the other hand the comparison of a3D to RGBY is more subtle. a3D starts below RGBY but eventually becomes more expensive. The reason is that initially RGBY has to linearly scan all its partial chains whereas a3D does not (this happens only for $D/2 \leq \kappa \leq D$). However, the overhead of validating the a3D tree outweighs the impact of the presence of false positives produced by RGBY.

Figure 16 shows how the forensic cost increases with time D for different numbers of corruption sites, namely, $\kappa = 1$, and $\kappa = 2$. As expected for $\kappa = 1$ (Figure 16(**a**)), the Monochromatic Algorithm has the lowest forensic cost for roughly the first half of the range of values of D. For the second half, the Tiled Bitmap Algorithm becomes the cheapest because it is able to definitively identify all the corruption negative areas through a logarithmic number of chains.

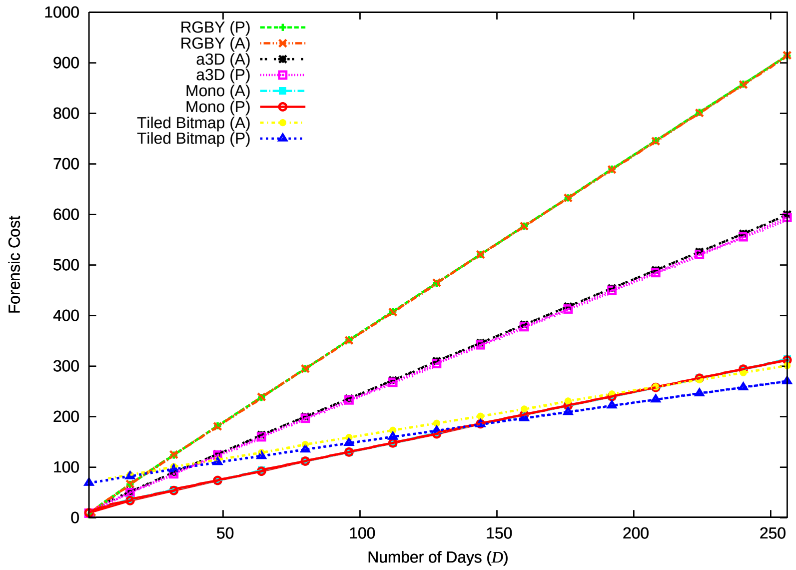
When $\kappa = 2$ the Tiled Bitmap Algorithm is cheapest, as shown in Figure 16(**b**). This is because Tiled Bitmap need only identify a single additional tile, whereas a3D (the second cheapest algorithm) has to process an entire subtree of maximal height. Also, for this value of κ the Monochromatic Algorithm becomes the most expensive algorithm.

Finally, Figure 17 shows how the cost of only the normal processing phase varies with the number of days D. Note that this cost is independent of κ. Here we see clearly that the most expensive normal processing phase belongs to the RGBY Algorithm. a3D is the next most expensive algorithm while Tiled Bitmap is the cheapest in terms of normal processing. This suggests that shifting the cost/amount of work done to the normal processing phase may not always pay off during forensic analysis.

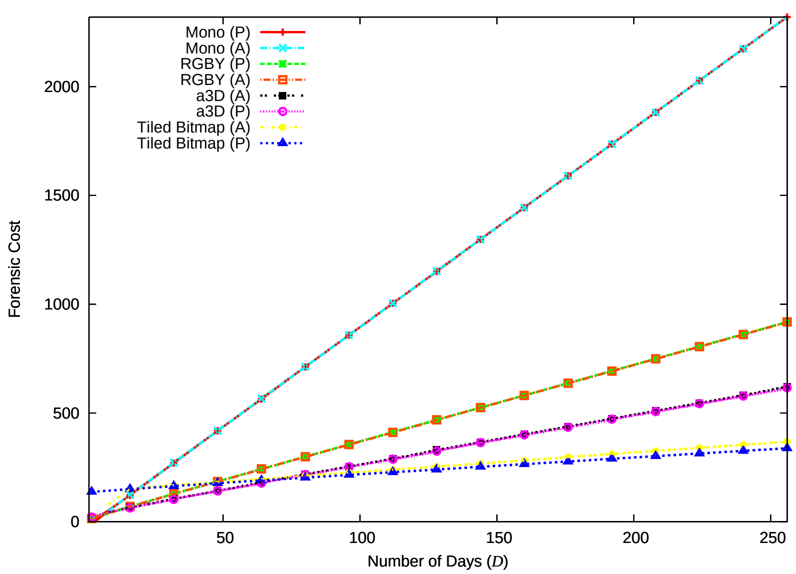
Table VII shows the predicted and actual forensic costs for the four implemented algorithms when $D = \kappa = 256$. The two values in each of the four cases differ by about 6% for Tiled Bitmap; for the other three the actual and predicted were nearly identical.

10. A LOWER BOUND FOR FORENSIC COST

We wish to derive a realistic lower bound for the *Forensic Cost* measure in terms of κ corruption sites, validation factor V, notarization interval I_N, and D days before the corruption is first detected.



(a) $\kappa = 1$



(b) $\kappa = 2$

Fig. 16. Forensic cost against D for $\kappa = 1$ and $\kappa = 2$.

The optimal value for $Area_U$ is 0 whereas the optimal value for $Area_P$ is $\kappa \cdot V \cdot I_N \cdot w$, where w is the width and $V \cdot I_N = I_V$ is the height of the rectangle in which the corruption site is located.

Keep in mind that these algorithms do not aim at reducing the t_c uncertainty. The size of the uncertainty of this temporal dimension depends solely on the size of the validation interval (I_V) and therefore it can be reduced if and only if I_V

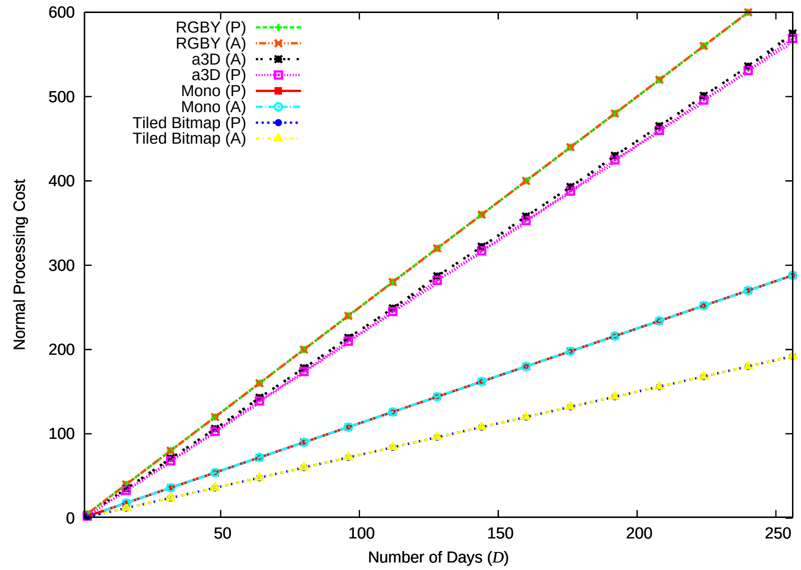


Fig. 17. Cost of *Normal Processing* against D.

is reduced. No other factor involving external notarization can have any impact on it. This is due to the fact that the t_c uncertainty is bounded above by the current time—the time the CE was discovered—and is also bounded below by the last time we checked the database, the last *VE* time. This is by definition the validation interval. Any new strategies introduced which are purely "native" to the system cannot be trusted and thus violate the working premise of this approach: no extra assumptions should be made about the system.

To obtain bounds on the *Normal Processing* and *Forensic Analysis* phases we start with a rather optimistic scenario. Suppose that we had *a priori* knowledge (both "when" and "where") of the exact κ granules to be corrupted in the future. Then the optimal algorithm would notarize κ hash chains of length one each covering the granule to be corrupted. Similarly, the forensic analysis would validate those κ hash chains and that would find all corruption sites, each bounded by a rectangle of height $V \cdot I_N$ and width $w = 1$ granule (where a granule is a unit of R_s). Thus a lower bound would be

$$\begin{aligned} FC_{\texttt{lower bound}_1} &= (\kappa + \kappa) \\ &+ \kappa \cdot V \cdot I_N \cdot 1 = 2 \cdot \kappa + \kappa \cdot V \cdot I_N \ . \end{aligned}$$

However, we do not feel it is fair to tax our algorithms with the burden of precognition. While we still assume that κ and D are known, we have no *a priori* knowledge of "where" the corruption sites are going to occur (within D). Given this information we seek to find the optimal value for $n \geq \kappa$, the number of notarizations during normal processing. The cost of *Normal Processing* $= n$, while the cost of *Forensic Analysis* $= \kappa \cdot \lg n$. This is because for every κ we must perform binary search in order to locate it. The width w for $Area_P$ is $D/2^n$ because each notarization provides a single bit of information in the "where" dimension.

$$FC_{\texttt{lower bound}_2} = (n + \kappa \cdot \lg n) + \kappa \cdot V \cdot I_N \cdot D/2^n$$

If we assume that the width w can take a minimum value of $w = 1$ then it follows that $n = \lg D$. If we substitute this value of n into the above FC expression we get

$$FC_{\texttt{lower bound}_2} = (\lg D + \kappa \cdot \lg\lg D) + \kappa \cdot V \cdot I_N \ .$$

This lower bound makes fewer assumptions about the information available and therefore $FC_{\texttt{lower bound}_1} \leq FC_{\texttt{lower bound}_2}$. Our final lower bound is

$$\begin{aligned} FC_{\texttt{lower bound}} &= \kappa \cdot V \cdot I_N + \kappa \cdot \lg\lg D + \lg D \ , \quad \kappa \leq D \\ &= O(\kappa \cdot V \cdot N + \lg D) \ . \end{aligned}$$

Table VIII compares this lower bound with the worst-case forensic cost of our algorithms, characterized for "small κ" and "large κ." In particular, we eliminate κ by assuming it is either equal to $O(1)$ or $O(D)$ respectively. Note that for the Monochromatic Algorithm if $\kappa = O(1)$, we assume that $V \ll D$ thus simplifying the cost from $O(V+D)$ to $O(D)$. Tables IX and X repeat this comparison with average- and best-case forensic costs derived in Appendices E and F. The lower bound across all three tables is the same because the only way for the lower bound to decrease in the best-case and average-case analysis is for the binary search to be faster during forensic analysis. All other components are essential, i.e., n notarizations are required, and the width w must equal 1. Binary search in the best-case takes $O(1)$ eliminating the $\lg\lg D$ factor which in asymptotic notation is irrelevant. In the average-case forensic cost the average running time of binary search is $O(\lg n)$ so the lower bound remains the same. Hence, there is only the notion of a single lower bound.

For best-case forensic cost the Monochromatic algorithm (which requires $N = 1$) and the RGBY algorithm (which requires $N = 1$ and $V = 2$) are optimal for large κ. Observe also that the asymptotic forensic cost of both the RGBY Algorithm and that of the a3D Algorithm (which requires $V = 1$) for all possible cases (worst, best, average) is optimal for large κ and is close to optimal for small κ.

11. RECOMMENDATIONS

Given the forensic cost formulæ and the insights from the previous sections, our recommendation is that it is best to provide users with three algorithms: Monochromatic, a3D and, depending on the application requirements, RGBY or Tiled Bitmap. The reason for considering RGBY and Tiled Bitmap as optional is that both these algorithms unlike the Monochromatic and a3D suffer from false positives. The RGBY Algorithm has the same optimal characteristics as a3D and is the cheapest when a large number of corruptions is expected. On the other hand, the Tiled Bitmap Algorithm has the lowest forensic cost in the long term for a fixed small number of corruptions but suffers from more false positives than RGBY which translates into more human effort when trying to pinpoint the exact corruptions at a later stage. The Tiled Bitmap Algorithm is also indicated when efficiency during normal processing is critical.

Table VIII. **Worst-case forensic cost and lower bound.**

Algorithm	**Worst-Case Forensic Cost**	
	Small κ ($\kappa = O(1)$)	Large κ ($\kappa = O(D)$)
Monochromatic	$O(D)$	$O(V \cdot D^2)$
RGBY	$O(D)$	
Tiled Bitmap	$O(V \cdot N^2 + (D \cdot \lg N)/N + \lg D)$	$O(V \cdot N^2 \cdot D)$
a3D	$O(N + D)$	$O(N \cdot D)$
Lower Bound	$O(V \cdot N + \lg D)$	$O(V \cdot N \cdot D)$

Table IX. **Average-case forensic cost and lower bound.**

Algorithm	**Average-Case Forensic Cost**	
	Small κ ($\kappa = O(1)$)	Large κ ($\kappa = O(D)$)
Monochromatic	$O(D)$	$O(V \cdot D^2)$
RGBY	$O(D)$	
Tiled Bitmap	$O(V \cdot N^{\lg 3} + (D \cdot \lg N)/N + \lg D)$	$O(V \cdot N^{\lg 3} \cdot D)$
a3D	$O(N + D)$	$O(N \cdot D)$
Lower Bound	$O(V \cdot N + \lg D)$	$O(V \cdot N \cdot D)$

Table X. **Best-case forensic cost and lower bound.**

Algorithm	**Best-Case Forensic Cost**	
	Small κ ($\kappa = O(1)$)	Large κ ($\kappa = O(D)$)
Monochromatic	$O(D)$	$O(V \cdot D)$
RGBY	$O(D)$	
Tiled Bitmap	$O(V \cdot N + (D \cdot \lg N)/N + \lg D)$	$O(V \cdot N \cdot D)$
a3D	$O(N + D)$	$O(N \cdot D)$
Lower Bound	$O(V \cdot N + \lg D)$	$O(V \cdot N \cdot D)$

If only two algorithms are to be used then both Monochromatic and a3D should be implemented. If only one algorithm is needed the choice would be again between the Monochromatic and a3D Algorithms. The Monochromatic Algorithm is by far the simplest one to implement and it is best-suited for cases when multiple corruptions are not anticipated or when only the earliest corruption is desired. The a3D Algorithm is the second easiest algorithm to implement and it is the only algorithm which exhibits all three of the most desirable characteristics: (i) it identifies multiple corruptions, (ii) it does not produce false positives, and (iii) it is stable and optimal for large κ (and near optimal for small κ). Hence, this algorithm is indicated in situations where accuracy in forensic analysis is of the utmost importance.

12. RELATED WORK

There has been a great deal of work on records management, and indeed, an entire industry providing solutions for these needs, motivated recently by Sarbanes-Oxley and other laws requiring audit logs. In this context, a "record" is a version of a document. Within a document/record management system (RMS), a DBMS is often used to keep track of the versions of a document and to move the stored versions along the storage hierarchy (disk, optical storage, magnetic tape). Examples of such systems are the EMC Centera Compliance Edition Content Addressed Storage System[1], the IBM System Storage DR series[2], and NetApp's SnapLock Compliance[3]. Interestingly, these systems utilize magnetic disks (as well as tape and optical drives) to provide WORM storage of compliant records. As such, they are implementations of *read-only file systems* (also termed *append-only*), in which new files can only be added. Several designs of read-only file systems have been presented in the research literature [10; 20]. Both of these systems (as well as Ivy [22]) use cryptographic signatures so that programs reading a file can be assured that it has not been corrupted.

Hsu and Ong have proposed an end-to-end perspective to establishing trustworthy records, through a process they term *fossilization* [15]. The idea is that once a record is stored in the RMS, it is "cast in stone" and thus not modifiable. An index allows efficient access to such records, typically stored in some form of WORM storage. Subsequently, they showed how the index itself could be fossilized [32]. Their approach utilizes the WORM property provided by the systems just listed: that the underlying storage system supports reads from and writes to a random location, while ensuring that any data that has been written cannot be overwritten.

This is an appealing and useful approach to record management. We have extended this perspective by asserting that every tuple in a database is a record, to be managed. The challenge was two-fold. First, a record in a RMS is a heavyweight object: each version is stored in a separate file within the file system. In a DBMS, a tuple is a light-weight object, with many tuples stored on a single page of a file storing all or a good portion of a database. Secondly, records change quite slowly (examples include medical records, contacts, financial reports), whereas tuples change very rapidly in a high-performance transactional database. It is challenging to achieve the functionality of tracked, tamper-free records with

[1] `http://www.emc.com/products/detail/hardware/centera.htm` (accessed April 28, 2008)
[2] `http://www.ibm.com/systems/storage/disk/dr/` (accessed April 28, 2008)
[3] `http://www.netapp.com/us/products/protection-software/snaplock.html` (accessed April 28, 2008)

the performance of a DBMS.

This raises the interesting question: since record management systems often use relational databases internally, how effective can these systems really be? Given the central role of audit logs in performing auditing of interactions with the records (tracking, modifications, exposure), the audit logs themselves are as valuable as the records they reference. It is critical that such audit logs and tracking information be correct and unalterable. It is not sufficient to say, "the records we store in our RMS are correct, because we store all interactions and tracking data in a separate audit log." The integrity of the underlying database is still in question. While Zhu and Hsu [32] provide a partial answer through their fossilized index (mentioned above), the rest of the database might still be tampered.

Johnson goes back thousands of years to show that in many cases, tamperproofing is economically inferior to tamper detection: "Often, it's just not practical to try to stop unauthorized access or to respond to it rapidly when detected. Frequently, it's good enough to find out some time after the fact that trespassing took place" [18].

The first work to show that records management could be effectively merged with conventional databases was that by Barbará et al. on using checksums to detect data corruption [4]. By computing two checksums in different directions and using a secret key, they were able to dramatically increase the effort an intruder would have to make to tamper the database. Our paper on tamper detection removed one assumption, that the system could keep a secret key that would not be seen by insiders [27]. We showed that cryptographic techniques coupled with a carefully-considered architectural design and an external digital notarization service could solve one part of the puzzle: detecting tampering. In this paper we consider another part of the puzzle: forensic analysis once tampering has been detected.

Computer forensics is now an active field, with over fifty books published in the last ten years[4] and another dozen already announced for 2008. However, these books are generally about preparing admissible evidence for a court case, through discovery, duplication, and preservation of digital evidence. There are few computer tools for these tasks, in part due to the heterogeneity of the data. One substantive example of how computer tools can be used for forensic analysis is Mena's book [21]. The more narrow the focus, the more specialized tools there are that can help. Carvey and Kleiman's book [5] cover just variants of that operating system and explains how to use the author's *Forensic Server Project* system to obtain data from a Windows system in a forensically sound manner. Closer to home, Schneier and Kelsey [26] describe a secure audit log system, but do not consider forensic analysis of such audit logs.

Goodrich et al. introduce new techniques for using indexing structures for data forensics [12]. The usual way of detecting malicious tampering of a digital object using cryptographic one-way hashes to store a cryptographic hash of the item and then to use it later as a reference for comparison. The approach of Goodrich et al. goes beyond the single bit (true/false) of information provided by a hash: they store multiple hashes (and attempt to minimize the required number of such values) to pinpoint which of a given set of items has been modified. They encode authentication information in the topology of the data structure of items (not in the stored

[4] `http://www.e-evidence.info/books.html` (accessed April 28, 2008)

values themselves) so that alterations can be detected. This is important because this approach requires no additional space other than the cryptographic master key used by the auditing agent. Their techniques are based on a new reduced-randomness construction for nonadaptive combinatorial group testing (CGT). In particular, they show how to detect up to d defective items out of a total of n items, with the number of tests being $O(d^2 \lg n)$. Moreover, they provide forensic constructions of several fundamental data structures, including binary search trees, skip lists, arrays, linked lists, and hash tables.

Several differences exist between Goodrich's approach and the one outlined in the current paper.

—The threat model in Goodrich et al. does not allow changes in the topology of the data structure whereas ours places no such restrictions.

—The objective in Goodrich et al. is to minimize the number of hashes stored that would allows to identify d corruptions given a particular data structure. In the current paper we seek a structure of hash chains with the lowest forensic cost, which includes both normal processing and forensic analysis components.

—Their CGT method is probabilistic whereas ours is deterministic.

—Goodrich et al.'s work applies to main-memory structures, whereas ours applies to disk-resident data items.

—There exists an upper bound on the number of modified items that can be detected, e.g., for a balanced binary search tree storing n elements the bound is $O(n^{1/3} / \log^{2/3} n)$. Our approach can detect up to $\kappa = n$ corruptions.

Goodrich's approach in constructing forensic data structures might be generalizable to detecting changes in key values stored in a B-tree. This could then provide some information about data values, thereby possibly reducing the number of hashes needed and thus the forensic cost.

Earlier we introduced the approach of using cryptographic hash functions for tamper detection [27] and introduced the first forensic analysis algorithms for database tampering [24]. The present paper significantly extends that research, with pseudocode for one previous algorithm (Monochromatic) and three new algorithms: the RGBY (a refinement of the previous RGB Algorithm), Tiled Bitmap (a refinement of the previous Polychromatic Algorithm), and a3D forensic analysis Algorithms.

We refine the definition of forensic strength to arrive at a notion of "forensic cost" that encompasses multiple corruption events. The objective is to minimize this cost in order to achieve a higher forensic strength. The definition of forensic cost retains some of the key characteristics of the original definition [24], while adopting a more sophisticated treatment of the region and uncertainty areas returned by the forensic algorithms, and incorporating the notions of temporal and spatial resolution. We characterize and validate experimentally the forensic cost for all four algorithms presented in this paper. We also present a lower bound that considers multiple corruption events.

13. SUMMARY AND FUTURE WORK

New laws and societal expectations are raising the bar concerning stewardship of stored data. Corporate and governmental databases are now expected and in many cases required to mediate access, to preserve privacy, and to guard against tampering, even by insiders.

Previously-proposed mechanisms can detect that tampering has occurred. This paper considers the next step, that of determining *when*, *what*, and hence indirectly providing clues as to *who*, through the use of various forensic analysis algorithms that utilize additional information (in this case, partial hash chains) computed during periodic validation scans of the database.

We introduced corruption diagrams as a way of visualizing corruption events and forensic analysis algorithms. We presented four such algorithms, the Monochromatic, RGBY, Tiled Bitmap, and a3D Algorithms, and showed through a formal forensic cost comparison (with worst-case, best-base, and average-case assumptions), validated with an implementation, that each successive algorithm adds extra work in the form of main-memory processing, but that the resulting additional precision in the obtained information more than counterbalances this extra work. Finally, we provided a lower bound for forensic cost and showed that only the a3D Algorithm is optimal for a large number of corruptions and close to optimal in all cases, without producing false positives.

Our recommendation is that at an initial stage it is best to provide users with the Monochromatic and a3D Algorithms. The Monochromatic Algorithm is the easiest to implement and is indicated when multiple corruptions are not anticipated or when only the earliest corruption site is desired. The a3D Algorithm is stable with optimal forensic cost (for large κ), is able to determine the "where", and the "when" of a tampering quite precisely and efficiently, and is able to effectively handle multiple corruption events. The other two algorithms produce false positives and can be provided as dictated by the application requirements. The RGBY Algorithm has optimal cost (for large κ) and is cheapest when many corruption sites are anticipated. The Tiled Bitmap Algorithm has the lowest forensic cost in the long term for a fixed number of corruptions and is also indicated when efficiency during normal processing is critical.

We are integrating these algorithms into a comprehensive enterprise solution for tamper detection and analysis that manages multiple databases with disparate security risks and requirements. Also, we are examining the interaction between a transaction-time storage manager and an underlying magnetic-disk-based WORM storage. As archival pages are migrated to WORM storage, they would be thus protected from tampering, and so would not need to be rescanned by the validator. It is an open question how to extend the forensic analysis algorithms to accommodate schema corruption.

Our challenge is in a sense the dual of that considered by Stahlberg et al. [28]. As mentioned in Section 2, we utilize a transaction-time table to retain previous states and perform forensic analysis on this data once tampering is detected. Stahlberg considers the problem of forensic analysis uncovering data that has been previously deleted, data that shouldn't be available. It is an open question as to how to augment our approach for forensic analysis to accommodate *secure deletion*.

Finally, it might make sense to augment database storage structures such as indexes in a manner similar to that proposed for main-memory structures by Goodrich et al. [12], to aid in forensic analysis.

ACKNOWLEDGMENTS

NSF grants IIS-0415101, IIS-0639106, and EIA-0080123 and a grant from Microsoft provided partial support for this work. Huilong Huang, Qing Ju, Melinda Malmgren, and Shilong (Stanley) Yao contributed to the implementation. We thank Travis Wheeler for his help with the characterization of forensic cost and thank the reviewers for their concrete suggestions which helped improve the presentation of the material.

ELECTRONIC APPENDIX

The electronic appendix for this article can be accessed in the ACM Digital Library by visiting the following URL: `http://www.acm.org/pubs/citations/journals/tods/2008-V-N/p1-pavlou`. The appendix discusses the subtleties involved in the forensic analysis of introactive corruption events, and demonstrates how false positives arise in the RGBY Algorithm. It also describes the Tiled Bitmap Algorithm, discusses the notion of a candidate set, and gives the running time of the algorithm. Finally, it analyzes the forensic cost for the algorithms, using worst-case, best-case, and average-case assumptions on the distribution of corruption sites.

REFERENCES

[1] R. Agrawal, T. Grandison, C. Johnson, and J. Kiernan, "Enabling the 21st Century Healthcare IT Revolution," *Communications of the ACM*, 50(2):34–42, February 2007.

[2] I. Ahn and R. T. Snodgrass, "Partitioned Storage Structures for Temporal Databases," *Information Systems*, 13(4):369–391, December 1988.

[3] J. Bair, M. Böhlen, C. S. Jensen, and R. T. Snodgrass, "Notions of Upward Compatibility of Temporal Query Languages," *Business Informatics (Wirtschafts Informatik)* 39(1):25–34, February 1997.

[4] D. Barbará, R. Goel, and S. Jajodia, "Using Checksums to Detect Data Corruption," in *Proceedings of the International Conference on Extending Database Technology*, Springer Lecture Notes in Computer Science, vol. 1777, Germany, March 2000.

[5] H. Carvey and D. Kleiman, **Windows Forensics and Incident Recovery**, Syngres, 2007.

[6] C. C. Chan, H. Lam, Y. C. Lee, X. Zhang, **Analytical method validation and instrument performance verification**, Wiley-IEEE 2004.

[7] CSI/FBI Tenth Annual Computer Crime and Security Survey, July 2005, `http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf` (accessed April 25, 2008).

[8] Department of Defense, "Trusted Computer System Evaluation Criteria," DOD-5200.28-STD, December 1985, `http://www.dynamoo.com/orange` (accessed April 25, 2008).

[9] F.D.A., "Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures," 2003, `http://www.fda.gov/ora/compliance_ref/part11/` (accessed April 28, 2008).

[10] K. Fu, M. F. Kaashoek and D. Mazières, "Fast and secure distributed read-only file system," in *Proceedings of the USENIX Symposium on Operating Systems Design and Implementation*, pp. 181–196, October 2000.

[11] P. A. Gerr, B. Babineau, and P. C. Gordon, "Compliance: the effect on information management and the storage industry," Enterprise Storage Group Technical Report, May 2003, `http://www.enterprisestrategygroup.com/ESGPublications/ReportDetail.asp?ReportID=201` (accessed May 4, 2008).

[12] M. T. Goodrich, M. J. Atallah, and R. Tamassia, "Indexing Information for Data Forensics," in *Proceedings of the Conference on Applied Cryptography and Network Security*, Springer Lecture Notes in Computer Science 3531, pp. 206–221, 2005.

[13] R. L. Graham, D. E. Knuth, and O. Patashnik, **Concrete Mathematics**, Second Edition, Addison–Wesley, September 2004.

[14] S. Haber and W. S. Stornetta, "How To Time-Stamp a Digital Document," *Journal of Cryptology* 3:99–111, 1999.

[15] W. W. Hsu and S. Ong, "Fossilization: A process for establishing truly trustworthy records," IBM Research report RJ 10331, 2004.

[16] C. S. Jensen and C. E. Dyreson (eds), "A Consensus Glossary of Temporal Database Concepts—February 1998 Version," in **Temporal Databases: Research and Practice**, O. Etzion, S. Jajodia, and S. Sripada (eds.), Springer-Verlag, pp. 367–405, 1998.

[17] C. S. Jensen and R. T. Snodgrass, "Temporal Specialization and Generalization," *IEEE Transactions on Knowledge and Data Engineering*, 6(6):954–974, December 1994.

[18] R. G. Jonson, "Tamper-indicating seals," *American Scientist* 94(6):515–524, Nov–Dec 2006.

[19] D. Lomet, R. Barga, M. F. Mokbel, G. Shegalov, R. Wang, and Y. Zhu, "Immortal DB: transaction time support for SQL server," in *Proceedings of the International ACM Conference on Management of Data (SIGMOD)*, pp. 939–941, June 2005. See also `http://research.microsoft.com/research/db/immortaldb/` (accessed April 25, 2008).

[20] D. Mazières, M. Kaminsky, M. F. Kaashoek and E. Witchel, "Separating key management from file system security," in *Proceedings of the ACM Symposium on Operating Systems Principles*, pp. 124–139, December 1999.

[21] J. Mena, **Investigative Data Mining for Security and Criminal Detection**, Butterworth Heinemann, 2003.

[22] A. Muthitacharoen, R. Morris, T. M. Gil and B. Chen, "Ivy: A Read/Write Peer-to-Peer File System," in *Proceedings of USENIX Operating Systems Design and Implementation*, 2002.

[23] Oracle Corporation, "Oracle Database 11g Workspace Manager Overview," Oracle White Paper, June 2007, `http://www.oracle.com/technology/products/database/workspace_manager/pdf/twp_AppDev_Workspace_Manager_11gR1.pdf` (accessed April 28, 2008).

[24] K. E. Pavlou and R. T. Snodgrass, "Forensic Analysis of Database Tampering," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, pp. 109–120, Chicago, June 2006.

[25] K. E. Pavlou and R. T. Snodgrass, "The Pre-images of Bitwise *AND* Functions in Forensic Analysis," TimeCenter Technical Report, October 10, 2006.

[26] B. Schneier and J. Kelsey, "Secure Audit Logs to Support Computer Forensics," ACM *Transactions on Information and System Security* 2(2):159–196, May 1999.

[27] R. T. Snodgrass, S. S. Yao, and C. Collberg, "Tamper Detection in Audit Logs," in *Proceedings of the International Conference on Very Large Databases*, pp. 504–515, Toronto, Canada, September 2004.

[28] P. Stahlberg, G. Miklau, and B. N. Levine, "Threats to privacy in the forensic analysis of database systems," in *Proceedings of the ACM SIGMOD International Conference on Management of Data*, Beijing, 2007.

[29] U.S. Dept. of Health & Human Services, The Health Insurance Portability and Accountability Act (HIPAA), 1996, `http://www.cms.hhs.gov/HIPAAGenInfo/` (accessed April 25, 2008).

[30] U.S. Public Law No. 107-204, 116 Stat. 745, The Public Company Accounting Reform and Investor Protection Act, 2002.

[31] G. Wingate, ed., **Computer systems validation: Quality Assurance, Risk Management, and Regulatory Compliance for Pharmaceutical and Healthcare, Companies**, Informa Health Care, 2003.

[32] Q. Zhu and W. W. Hsu, "Fossilized Index: The Linchpin of Trustworthy Non-Alterable Electronic Records," in *Proceedings of the ACM International Conference on Management of Data*, pp. 395–406, Baltimore, Maryland, June 2005.

...

THIS DOCUMENT IS THE ONLINE-ONLY APPENDIX TO:

Forensic Analysis of Database Tampering

Kyriacos E. Pavlou
and
Richard T. Snodgrass
University of Arizona

ACM Transactions on Database Systems, Vol. V, No. N, September 2008, Pages 1–45.

This appendix has six sections. Appendix A discusses the subtleties involved in the forensic analysis of introactive corruption events, while Appendix B demonstrates how false positives arise in the RGBY algorithm. Appendix C describes the Tiled Bitmap algorithm (pseudocode provided), discusses the notion of a candidate set, and gives the running time of the algorithm. A more thorough exposition of the use of candidate sets in forensic analysis may be found elsewhere [25]. The remaining Appendices D, E, and F provide the forensic cost for the algorithms, using worst-case, best-case, and average-case assumptions, respectively, on the distribution of corruption sites.

A. INTROACTIVE CORRUPTION EVENTS

Introactive corruption events were introduced in Section 5. However, subsequent examples and algorithms do not deal explicitly with the particular challenges raised by these CEs in forensic analysis. The main challenge stems from the fact that the partial chains computed during the validation event scan terminating at t_{FVF} cannot be used to identify introactive CEs. (This holds for all algorithms utilizing partial hash chains.) The reason is that an introactive CE occurs *before* these latest partial hash chains are notarized. Recall that we deferred the partial chain hashing and notarization during a validation scan in order to decrease the read overhead. This results in the latest partial chains hashing the corrupted values. Hence, the validation of the rehashed value corresponding to the entire database must happen first, and if and only if it returns true are the partial hash chains notarized. Moreover, because the cumulative black chains perform hashing in real-time it is impossible for an introactive CE to occur before their creation. This implies that a single introactive CE *can* be detected by all algorithms because in this case we can locate the corruption using only the cumulative black chains. The problem described above only arises if there are multiple CEs, as in the example shown in Figure 7 on page 20. In this example partial chains B_6 and G_6 cannot be trusted. The analysis and implementation of the algorithms do not deal with this explicitly. The working assumption in the presentation of the algorithms in this paper is that all partial chains can be used in forensic analysis. One way to accommodate introactive CEs is for each algorithm to treat the entire region where introactive CEs can occur as suspect when dealing with multiple corruptions.

B. FALSE POSITIVES IN THE RGBY ALGORITHM

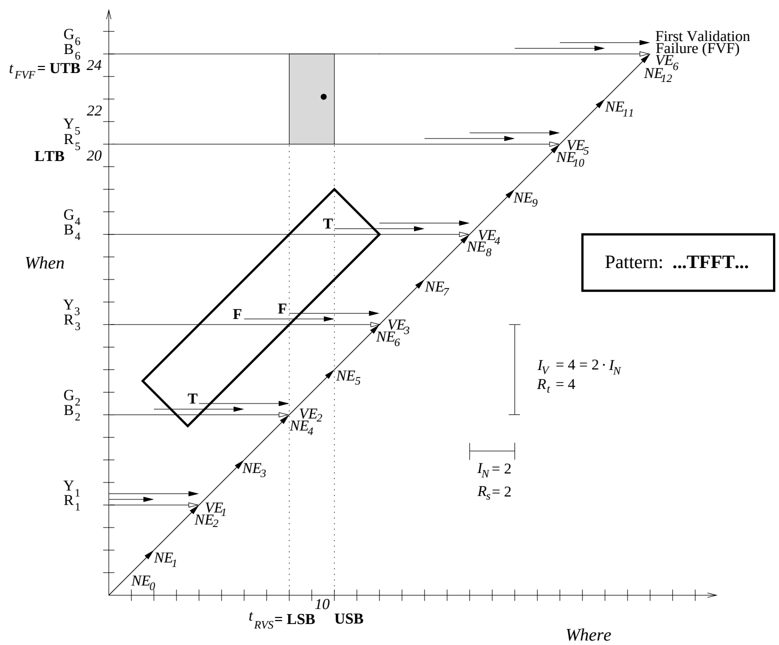
In this section we discuss the nature of the linear search of the RGBY Algorithm and show how false positives inevitably arise. Figure 18**(a)** shows the basic pattern of truth values encountered over a single corruption during the linear scan of the forensic analysis, namely ...TFFT.... Similarly, if we look at Figure 18**(d)** we observe that two corruption sites sufficiently-spaced (i.e., distance two or more I_N apart in the spatial dimension) produce a succession of the same basic pattern observed in the case where $\kappa = 1$, i.e., ...TFFTFFT.... In other words, sufficiently spaced multiple corruption sites can be definitively identified by the RGBY Algorithm just by seeking the pattern ...FF... during the linear scan.

If however, two corruption sites are less than two I_N apart (in the spatial dimension) then the situation is more complex. Figure 18**(b)** depicts two *contiguous* corruption sites. The pattern observed here is ...TFFFT.... It is important to realize that since the linear scan involves a look-ahead of size one (i.e., it needs to examine the results of two chains at a time to locate ...FF...) and between each iteration the frame shift is again one, the pattern ...FFF... will be correctly interpreted by the algorithm as two ...FF... patterns overlapping in the middle, hence correctly identifying the two contiguous corruption sites.

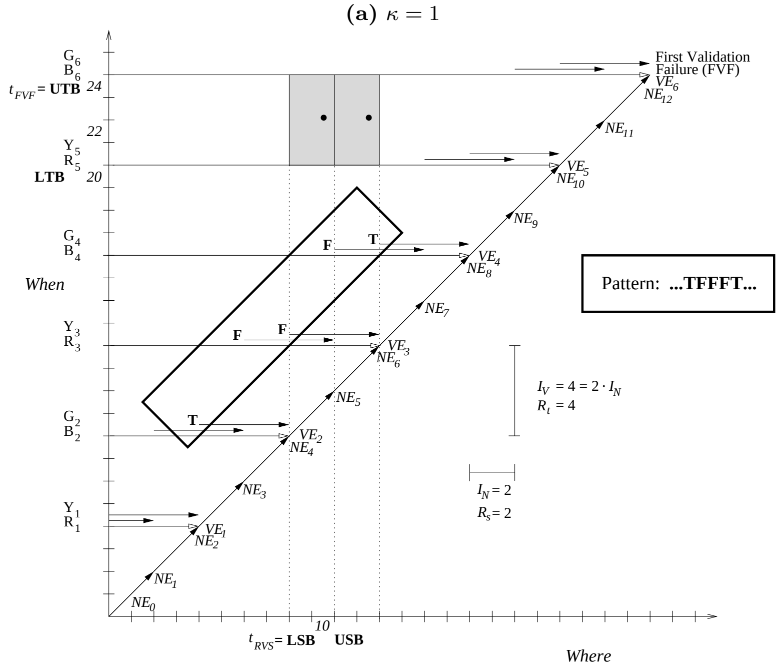
This does not happen in the the case shown in Figure 18**(c)** where two corruption sites are distance I_N apart. Here the pattern observed is ...TFFFFT.... Parsing this string as before, i.e., two values at a time will result in the algorithm identifying *three contiguous* corruption sites instead of the correct two. Thus, the corruption is overestimated and the middle $I_N \times I_V$ rectangle is a false positive. Any attempt to circumvent this problem by increasing the look-ahead to three chains (i.e. parse four values at a time) is doomed because the case where there are indeed three contiguous corruption sites produces the same pattern as the case shown in Figure 18**(c)**, making the two indistinguishable. For this reason, occurrence of false positives is inevitable in the RGBY algorithm, and moreover, in the worst case scenario where corruption sites alternate with corruption-free areas of width I_N, RGBY can produce up to 50% false positives.

C. THE TILED BITMAP ALGORITHM

Here we present an improved version of the Polychromatic Algorithm [24] called the Tiled Bitmap Algorithm. The original Polychromatic Algorithm utilized multiple *Red* and *Blue* chains while retaining the *Green* chain from the RGB Algorithm. These two kinds of chains and their asymmetry complicated this algorithm. The Tiled Bitmap Algorithm relocates these chains to be more symmetric, resulting in a simpler pattern.

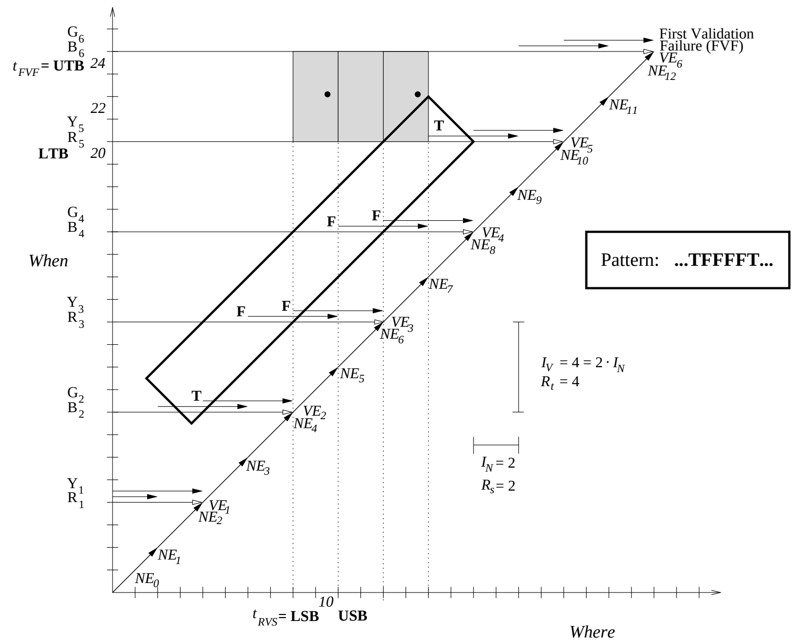


(a) $\kappa = 1$

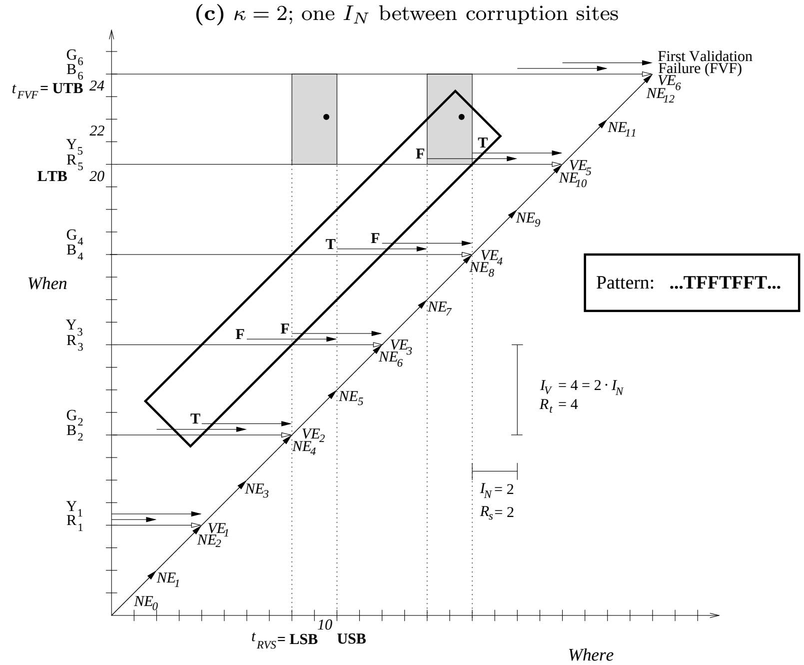


(b) $\kappa = 2$; contiguous corruption sites

Fig. 18. The chain patterns and corresponding corruption regions of the RGBY algorithm for one or two contiguous corruption sites.



(c) $\kappa = 2$; one I_N between corruption sites



(d) $\kappa = 2$; two I_Ns between corruption sites

Fig. 18. (continued) The chain patterns and corresponding corruption regions of the RGBY algorithm for two corruption sites with one or two I_Ns between the sites. The middle corruption region rectangle in **(c)** is a false positive.

We proceed to modify the Polychromatic Algorithm by:

—Removing the *Green* chain altogether.

—Adding two new subchains in the *Red* and *Blue* chain groups. For odd i, the algorithm computes the main red hash chain from $NE_{2\cdot i-3}$ to $NE_{2\cdot i-1}$, while for even i the blue and green chains are computed over the intervals $NE_{2\cdot i-3}$ to $NE_{2\cdot i-1}$ and $NE_{2\cdot i-2}$ to $NE_{2\cdot i}$ respectively.

—Shifting the first group of Red_1 to the right.

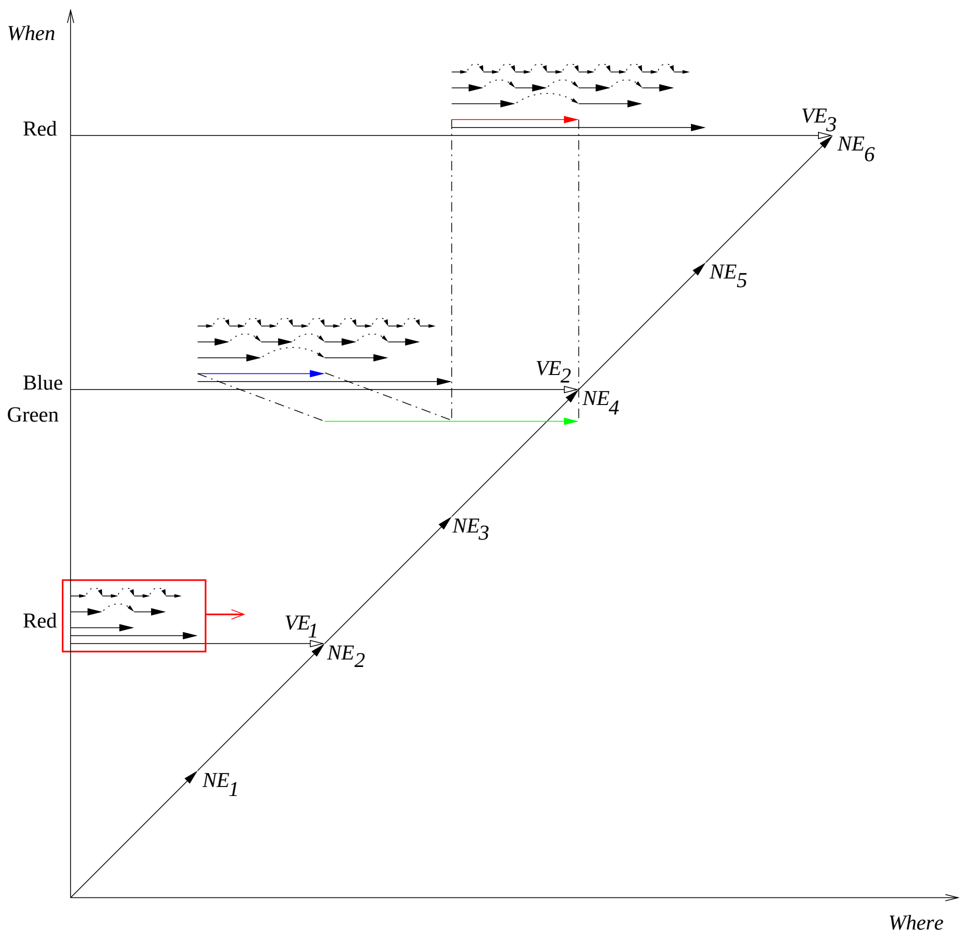


Fig. 19. Improvements introduced to the Polychromatic Algorithm.

As Figure 19 shows the main green chain $Green_i^0$ is "broken" in half and is substituted by Red_{i+1}^1 and $Blue_i^1$. The second half of the $Green_i^0$ chain becomes the "missing" Red_{i+1}^1 chain in the next group of red chains in order to complete the logarithmic number of chains defined in an I_V. The first half of the $Green_i^0$ chain, however, covers the complimentary interval of what is missing in the group of blue chains. Hence, we first take the complement of this first half and then add it as the missing $Blue_i^1$ chain. This leads to an increase in the number of hash chains by one per I_V. This is the price paid in order to have each group of chains function as a bitmap and to have the ability to perform the combinatorial bit pattern analysis suggested below.

Next, in a completely independent step, we shift to the right the Red_1 group of hash chains (which was shorter than the rest). In this way all the remaining hash chain groups are also shifted to the right by $I_V/2$ days. This has the result of aligning the hash chain groups, with the actual validation intervals and thus making the structure of the algorithm more regular. Each hash chain group is repeated and thus "tiles" the action line and will serve later as a bitmap. Hence the name of this algorithm: *Tiled Bitmap Algorithm*.

Finally, we make this algorithm more general by fixing the length of the tile to cover an I_N and have V number of tiles between successive validations as shown in Figure 9 in Section 8.3.

If the CE is data-only, the result of validating the entire tile of hash chains (marked with a "$\rightsquigarrow$" in Figure 9) and concatenating the result of each subchain creates a binary string whose numerical value is the relative position of the compromised granule within the tile. In this way we can easily establish a mapping between the binary string representation of the truth value pattern (1 = Success, 0 = Failure) within each hash chain group and the desired time (granule) down to R_s.

Let us turn to an example involving a corruption. Consider CE_1 in Figure 9. We find the first tile in which a corruption has occurred via binary search in order to locate t_{RVS}. In this figure CE_1 has $t_l = 19$ and a relative position within the second I_N of 2. If we validate the hash chains of the tile in which the CE transpired then we get the string 00010 (most significant bit corresponds to the chain which covers all the days in I_N), termed the *target bit pattern*. The numerical value of the target string 00010 is 2 which is exactly the relative position of the granule within the second I_N.

Now, let's see what happens if a timestamp corruption occurs and both t_l and t_p are within the same tile. Figure 9 also shows a postdating CE_2 with $t_l = 20$ and $t_p = 27$ which are both in the second tile ($I_N = 16$). If each of these were to appear on their own the target bit patterns produced by the tile validation would be 0011 (3^{rd} granule within N) and 1010 (10^{th} granule within N). However, since both occur at the same time within the same I_N and the hash chains are linked together, then the bit patterns given above are *AND*ed and the target 0010 is the actual result of the validation, as shown in Figure 20. This target corresponds to the existence of the two suspect days t_l and t_p, without being able to distinguish between the two. (NB: if g is a specific granule while r is its relative position within I_N, then $(g - 1) \bmod N = r$.)

In reality the situation is more involved: when dealing with multiple CEs there might be many combinations of bit patterns which when *AND* ed can yield the target bit pattern computed during forensic analysis. Thus even in the simple case where a single post/backdating CE *does not* have its endpoints in different tiles can introduce ambiguity. For example, we cannot distinguish between the two scenarios

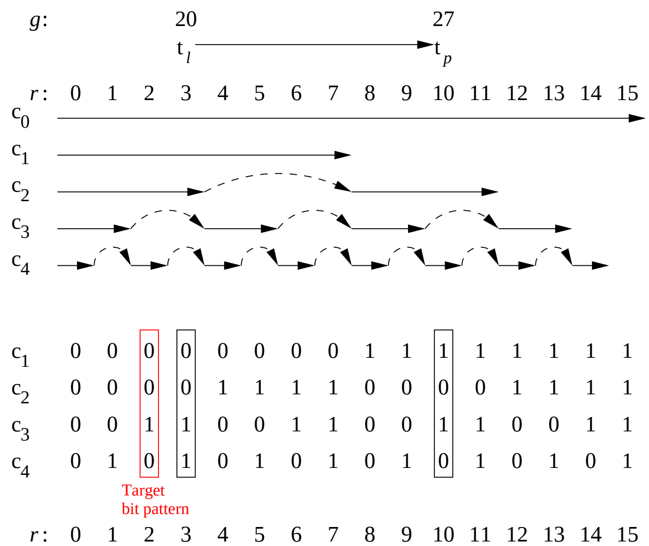


Fig. 20. The bitmap of a single tile.

shown in Figure 21 because in both cases the target bit pattern is the same. In the first case, both CE_2 and CE_3 produce the target bit pattern 0010 because the *AND* operation is commutative: $0011 \wedge 1010 = 1010 \wedge 0011$. For this reason we cannot distinguish between CE_2 and CE_3. Moreover, distinguishing between CE_2, CE_3 and CE_4, CE_5 is also impossible because CE_4 and CE_5 also produce the same target bit pattern as before. More specifically, CE_4 produces the bit pattern $0010 \wedge 0111 = 0010$ and CE_5 produces again $0110 \wedge 1010 = 0010$.

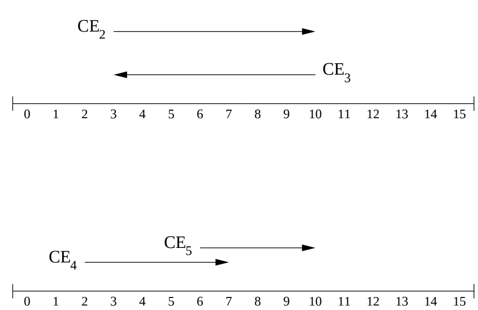


Fig. 21. Examples of CEs resulting in the same target bit pattern.

Hence we introduce the notion of a candidate set [25], because the pre-image of the target bit pattern under the bit-wise *AND* function is not unique. More formally, we define the length l of a binary number b, denoted by $|b| = l$, as the number of its digits. We seek to find the pre-images of all the binary numbers of length l, $\mathbb{B} = \{b : |b| = l\}$, under a family of bit-wise *AND* functions whose domain

```
// input:     t_FVF is the time of first validation failure
//            I_N is the notarization interval
//            V is the validation factor
//            k is a parameter of the C_set to be created
// output:    C_set, an array of binary numbers
//            UTB, LTB are the temporal bounds on t_c
procedure Tiled_Bitmap(t_FVF, I_N, V, k ):
    I_V ← V · I_N
    t_RVS ← find_t_RVS(t_FVF, I_N)
    UTB ← t_FVF
    LTB ← max(t_FVF − I_V, t_RVS)
    target ← 0
    C_set ← C_temp ← ∅
    if t_RVS mod I_V = 0 then t ← t_RVS    // t must coincide with the start of a tile
    else t ← t_RVS − I_N
    while t < t_FVF do
        if ¬ val_check(c_0(t)) then
            n ← lg I_V
            for i ← n to 1 do
                target ← target + 2^(n−i)·val_check(c_i(t))
            C_temp ← candidateSet(target, n, k)
            for each r ∈ C_temp do
                g ← (r · t)/I_V + 1
                C_set ← C_set ∪ {g}
        t ← t + I_V
    return C_set, LTB < t_c ≤ UTB
```

Fig. 22. The Tiled Bitmap Algorithm.

is a finite Cartesian product.

$$AND_k : \mathbb{B}^k \longrightarrow \mathbb{B}$$

$$AND_k((b_1, b_2, \ldots, b_k)) = b_1 \wedge b_2 \wedge \ldots \wedge b_k$$

Observe that the maximum number k of sets participating in the Cartesian product is 2^l, since if k is allowed to take a value beyond that, it will force a repetition of one of the binary numbers. This is not informative or useful in any way since repeated ANDing operations with the *same* binary number leave the result invariant (the operation is *idempotent*). In other words, repetition is not allowed and hence for a given k-tuple all its components are distinct. Also note that the value of k uniquely identifies a specific AND_k function in the above family. The *candidate set* is the set of all binary numbers that appear as components in at least one of the pre-images (i.e., k-tuples) of a specific binary number termed the *target*.

$$C_{target,k} = \{b \in \mathbb{B} \,|\, \exists\, b_1, b_2, \ldots, b_{k-1} \in \mathbb{B}\ (AND_k((b, b_1, \ldots, b_{k-1})) = target)\}\ .$$

This candidate set captures all potential sites of corruption. In the example given above the candidate set obtained for CE_2, CE_3 and CE_4, CE_5 will be the same in both cases and is equal to

$$C_{0010,2} = \{0010, 0011, 0110, 0111, 1010, 1011, 1110, 1111\}\ .$$

The pseudocode for the Tiled Bitmap Algorithm is provided in Figure 22. In this algorithm, the partial hash chains within a tile are denoted by $c_0(t), c_1(t), \ldots, c_{\lg N}(t)$, with $c_i(t)$ denoting the i^{th} hash chain of the tile which starts at time instant t. The algorithm begins looking at the black chains as the Polychromatic Algorithm does. This bounds t_c: $LTB < t_c \leq UTB$ as before. The binary search on the black chains also finds the value of t_{RVS}. Lines 7 and 8 adjust the start of the iteration to coincide with the beginning of a tile. On line 9 the algorithm iterates through the different tiles and checks (line 10) if the longest partial chain $c_0(t)$ evaluates to false. If not, it moves on to the next tile. If the chain evaluates to false (line 10), the algorithm iterates through the rest of the partial chains in the tile (line 12) and concatenates the result of each validation to form the target number (line 13). Then the candidateSet function is called to compute all the preimages of the target number according to the user-specified parameter k discussed above and in more detail elsewhere [25].

On lines 15–16 the candidate granules are renumbered to reflect their global position. The call to find_t_{RVS} takes $2 \cdot \lg(D/N)$ time because it performs a binary search on the cumulative black hash chains in order to locate t_{RVS}. The "while" loop on line 9 takes $\lceil D/N \rceil$ in the worst case. In reality, because of the "if" statement on line 10 the body of the loop gets executed only if corruption is initially detected by using $c_0(t)$. Hence, the actual running time of the loop is $\Theta(F)$ where F is the number of times the validation of a $c_0(t)$ chain fails. The "for" loop on line 12 takes $\lg(I_N/R_s)$ while the candidateSet function takes $\Omega(\lg(I_N/R_s) + 2^z)$. The loop on line 15 takes $\Theta(2^z)$, where z is the number of zeros in the target binary number. Hence the run time of this algorithm is as follows.

$$\begin{aligned}
&\Omega(\lg(D/N) + F \cdot (\lg(I_N/R_s) + (\lg(I_N/R_s) + 2^z) + 2^z)) \\
&\quad = \Omega(\lg(D/N) + F \cdot (\lg N + 2^z)) \\
&\quad = O(\lg(D/N) + (D/N) \cdot (\lg N + N)) \\
&\quad = O(D)
\end{aligned}$$

The upper bound is obtained as follows. F in the worst case is $O(D/N)$, that is, the total number of tiles. 2^z in the worst case is N because that is the total number of granules (R_s units) within a tile.

D. FORENSIC COST FOR WORST-CASE DISTRIBUTION OF CORRUPTION SITES

In Section 9.1 we analyzed the worst-case forensic cost for the Monochromatic Algorithm. Here we proceed with a similar analysis for the RGBY, Tiled Bitmap, and a3D forensic analysis algorithms.

D.1 The RGBY Algorithm

As with the previous algorithm, in the RGBY Algorithm, the spatial detection resolution (R_s) is I_N, so after normalizing by R_s, $N = 1$. Also recall that $V = 2$ for this algorithm. In this algorithm, during normal processing at each validation event we validate one chain and notarize two partial chains; hence we have $(D/2) \cdot 3$ interactions with the digital notarization service during validation.

During forensic analysis we have to perform a linear search which could involve all partial hash chains previously notarized, i.e., two at each validation event and hence $2 \cdot (D/2)$.

$$\begin{aligned} \mathit{NormalProcessing}_{RGBY} &= \mathit{Number\ of\ Notarizations} \\ &\quad + \mathit{Number\ of\ Validations} \\ &= D \\ &\quad + 3 \cdot (D/2) \end{aligned}$$

$$\begin{aligned} \mathit{ForensicAnalysis}_{RGBY} &= \mathit{Binary\ search\ for\ finding}\ t_{\mathrm{RVS}} \\ &\quad + \mathit{Linear\ scan\ of\ partial\ chains} \\ &= 2 \cdot \lg(D) \\ &\quad + 2 \cdot (D/2) \end{aligned}$$

The RGBY Algorithm can detect multiple corruption sites which if sufficiently apart can produce distinct $Area_P$, each equal to $V \cdot N^2 = 2$. In the worst case, however, if corruptions alternate with corruption-free areas of spatial dimension I_N then the RGBY algorithm produces false positives by identifying the intervening corruption-free area as part of $Area_P$ as shown in Figure 23. This makes $Area_P = 4$ for all $\kappa > 1$, and $Area_U = 0$.

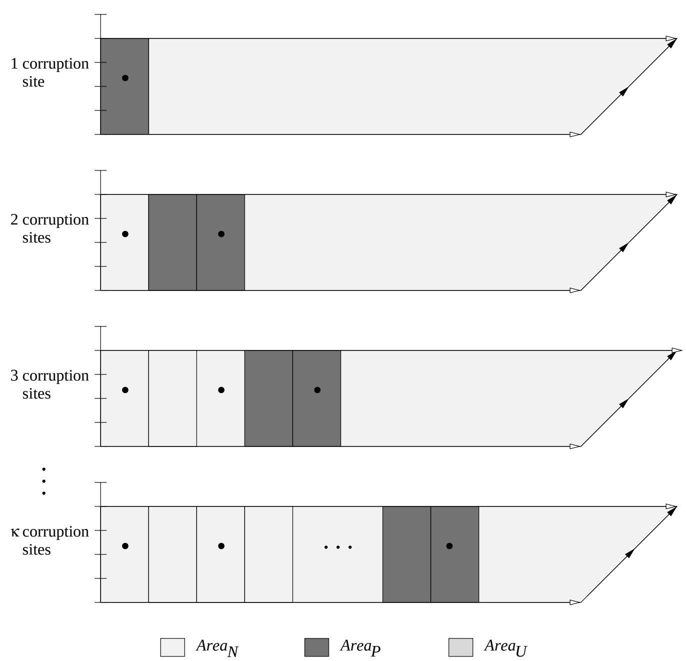


Fig. 23. Three types of forensic area for RGBY and κ corruption sites.

Table XI. **Forensic areas for $1 \leq \kappa \leq D$ corruption sites (RGBY).**

# Corruption Sites ($1 \leq \kappa \leq D$)	$Area_P$	$Area_U$	$Area_N$
1	2	0	$TotalArea - 2$
2	4	0	$TotalArea - 4$
3	4	0	$TotalArea - 4$
⋮	⋮	⋮	⋮
κ	4	0	$TotalArea - 4$

$$FC_{RGBY}(D,1,2,\kappa) = (D + 3 \cdot (D/2) + 2 \cdot \lg D + 2 \cdot (D/2)) + (2 + \sum_{i=2}^{\kappa} 4)$$

For $\kappa = 1$, the last term is an empty sum, and thus is equal to zero. Hence:

$$\begin{aligned} FC_{RGBY}(D,1,2,1) &= (D + 3 \cdot (D/2) + 2 \cdot (D/2) + 2 \cdot \lg D) + 2 \\ &= O(D) \\ FC_{RGBY}(D,1,2,\kappa \geq 2) &= (D + 3 \cdot (D/2) + 2 \cdot (D/2) + 2 \cdot \lg D) \\ &\quad + (2 + (\kappa - 1) \cdot 4) \\ &= O(\kappa + D) \end{aligned} \tag{3}$$

D.2 The Tiled Bitmap Algorithm

Unlike the previous two algorithms, the Tiled Bitmap Algorithm effects a spatial resolution (R_s) that is *smaller* than the notarization interval. Also V and N are both set by the DBA, and hence appear as variables.

The normal processing component is made up of the number of notarizations required for the black chains, the number of notarizations for the partial chains that make up each tile, and the number of validations performed.

$$\begin{aligned} NormalProcessing_{tiled\_bitmap} &= \textit{Number of black chain notarizations} \\ &\quad + \textit{Number of within-tile notarizations} \\ &\quad + \textit{Number of validations} \end{aligned}$$

For each validation event, during normal processing the Tiled Bitmap Algorithm contacts the notarization service once to validate the database and then notarizes all the chains within a tile, which are $1 + \lg N$ in number.

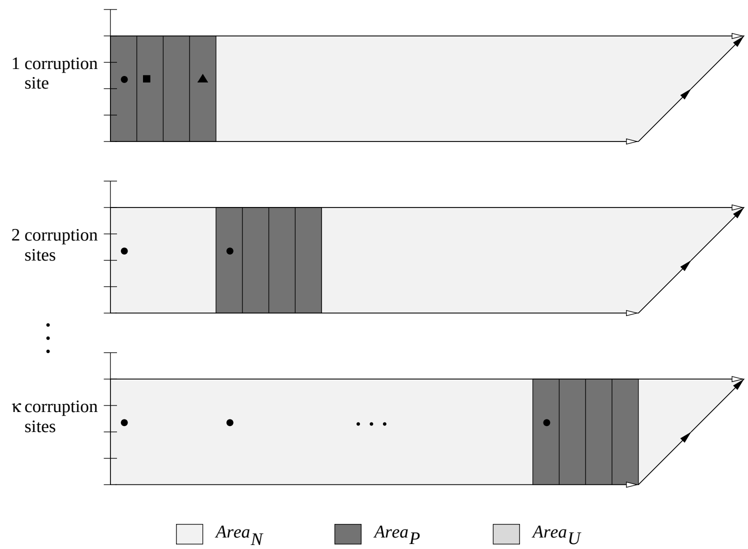


Fig. 24. Three types of forensic area for Tiled Bitmap and κ corruption sites.

$$\begin{aligned} \mathit{NormalProcessing}_{\mathit{tiled\_bitmap}} &= D/N \\ &+ (1 + \lg N) \cdot (D/N) \\ &+ D/(V \cdot N) \end{aligned}$$

For forensic analysis we have to perform a binary search to find t_{RVS} and then a linear search to locate corruptions for each tile. The linear search could involve κ tiles in the worst case.

$$\begin{aligned} \mathit{ForensicAnalysis}_{\mathit{tiled\_bitmap}} &= \mathit{Binary\ search\ for\ finding}\ t_{\text{RVS}} \\ &+ \mathit{Number\ of\ chains\ validated\ within\ tiles} \\ &= 2 \cdot \lg(D/N) \\ &+ (1 + \lg N) \cdot \kappa \end{aligned}$$

The algorithm returns a candidate set $C_{target,2}$ each element of which corresponds to a distinct corruption region of area $V \cdot N^2$. The cardinality of the candidate set is equal to 2 raised to the number of zeros z in the target [25] and thus $|C_{target,2}| = 2^z$. The maximum value z can take is the length l of the *target* which is $\lg N$. This implies that $|C_{target,2}| = O(2^{\lg N}) = O(N)$, as it should be (!).

Note that the worst case scenario for the Tiled Bitmap Algorithm occurs when each of the κ corruption sites occurs in the first granule of *each tile* as shown with a • in Figure 24. Subsequent corruption sites (shown with ■ and ▲) *within the same tile* as the ones in the first tile do not alter the cardinality of the candidate set and thus do not cause an increase in $Area_P$. Note that $Area_P$ is the entire tile in this (improbable) worst case. We still normalize I_N and I_V by R_s, which implies that N is larger than 1 (actually, it must be a power of 2).

Table XII. **Forensic areas for $1 \leq \kappa \leq D$ corruption sites (Tiled Bitmap).**

# Corruption Sites ($1 \leq \kappa \leq D$)	$Area_P$	$Area_U$	$Area_N$
1	$V \cdot N^2$	0	$TotalArea - V \cdot N^2$
2	$V \cdot N^2$	0	$TotalArea - V \cdot N^2$
3	$V \cdot N^2$	0	$TotalArea - V \cdot N^2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
κ	$V \cdot N^2$	0	$TotalArea - V \cdot N^2$

$$
\begin{aligned}
FC_{tiled\_bitmap}(D,N,V,\kappa) &= ((D/N) + (1+\lg N)\cdot(D/N) + D/(V\cdot N) \\
&\qquad + 2\cdot\lg(D/N) + (1+\lg N)\cdot\kappa) \\
&\quad + (\kappa\cdot V\cdot N^2) \qquad (4)\\
&= O(\kappa\cdot V\cdot N^2 + (D\cdot\lg N)/N + \lg D)
\end{aligned}
$$

In this case, even though the cost of normal processing and forensic analysis have increased because of the increased number of notarizations and validations that need to be performed, the area has shrunk considerably. The entire $Area_U$ is zero while $Area_P$ has seen a modest increase.

It is worth noting here that there exists a case when the candidate set will find the corruption site with perfect precision. This happens when the corruption only occurs inside the last granule of the tile (shown with ▲ and disregarding the other corruption sites in that tile). In this case the resulting *target* bit string uniquely identifies the corrupted granule so we know that there exists only one corruption site in the tile, along with its exact location.

D.3 The a3D Algorithm

In the a3D Algorithm, during normal processing, for every validation event we notarize one cumulative black chain, we validate once the entire database, and we notarize a number of partial hash chains depending on the R_s unit. The total number of notarizations performed in D units was calculated in Section 8.4; see equation (1) in that section. (Recall that we normalize I_N and t_{FVF} by R_s, the spatial detection resolution. Recall also that in the a3D Algorithm $V = 1$.) There we proved that the total number of notarizations is equal to $O(D)$.

$$\begin{aligned} \mathit{NormalProcessing}_{\,a3D} &= \mathit{Total\ Number\ of\ Validations} \\ &\quad + \mathit{Total\ Number\ of\ Notarizations} \\ &= D/N \\ &\quad + \mathcal{N}(D) + D/N - (1 + \lfloor \lg(D/N) \rfloor) \\ &= O(D) \end{aligned}$$

The forensic analysis cost depends on the actual distribution of the κ corruption sites. A worst case scenario arises when each successive corruption site that is added causes the maximum possible number of validations in the algorithm. To explain this we utilize the binary tree representation of the hash chains in the algorithm. The algorithm is forced to perform the maximum number of validations whenever a new site corrupts a leaf which belongs to a subtree rooted at a node whose previous validation has yielded a true result and this subtree has maximal height. Figure 25 shows a tree of height four and the validation results after the addition of $\kappa = 8$ corruptions sites. A (non-unique) sequence of adding corruption sites which satisfies the condition for worst-case scenario stated above, is given with numbers underneath the leaves. For example, the first site in Figure 25 is a corruption on the data covered by hash chain $P_{1,0,0}$, the second site corrupts data covered by hash chain $P_{5,0,8}$, and so on. It's easy to see that the existence of $\kappa = D/2$ properly distributed corruption sites can force the validation of *all the hash chains* covering the first D units.

The number of validations in forensic analysis with each successive addition of a corruption site satisfies the following recursive formula,

$$\mathcal{V}(\kappa) \;=\; \mathcal{V}(\kappa - 1) + 2 \cdot (H - \mathit{depth}(\kappa)) \;, \tag{5}$$

where $\mathcal{V}(\kappa)$ is the number of hash chains validated by the algorithm when κ corruption sites exist under a worst-case distribution, the height of the tree H is $\lg N + \lceil \lg(D/N) \rceil = \lceil \lg D \rceil$, and $\mathit{depth}(\kappa)$ is the depth of the root of the maximal-height subtree in which the new corruption site occurs. For $\kappa \geq D/2$, $\mathit{depth}(k) = H$. The validation of the hash chain corresponding to this root evaluates to true before the κ^{th} corruption occurs and false afterwards.

The base case for this recursion is $\mathcal{V}(0) = 1$ and corresponds to the case when the result of the validation of the root of the entire tree (B_8 in this case) was true implying that no corruption has occurred ($\kappa = 0$). For $\mathcal{V}(1)$ there exists a single corruption site in the subtree of maximal height which in this case is the entire complete binary tree. This first corruption site corresponds to the number '1' in Figure 25. The corruption site will thus force the validation of the following sequence of hash chains: $B_8, B_4, B_2, B_1, P_{1,0,0}, P_{1,0,1}, P_{2,1,1}, P_{4,2,1}, P_{8,3,1}$. The number of chains validated (for a specific κ) is by definition $\mathcal{V}(\kappa)$, hence, $\mathcal{V}(1) = 9$. Alternatively, $\mathcal{V}(1) = \mathcal{V}(0) + 2 \cdot (4 - \lg 1) = 1 + 2 \cdot 4 = 9$. We now solve this recursion.

Theorem D.1. *The solution to the recursion* $\mathcal{V}(\kappa) = \mathcal{V}(\kappa - 1) + 2 \cdot (H - \mathit{depth})$ *is* $\mathcal{V}(\kappa) = 2 \cdot \kappa \cdot (H - \lceil \lg \kappa \rceil) + (1 + [\kappa \neq 2^i]) \cdot 2^{\lfloor \lg \kappa \rfloor + 1} - 1$, *for some* $i \in \mathbb{N} \cup \{0\}$.

Proof.
The variable *depth* denotes the depth of the root of the maximal-height subtree in

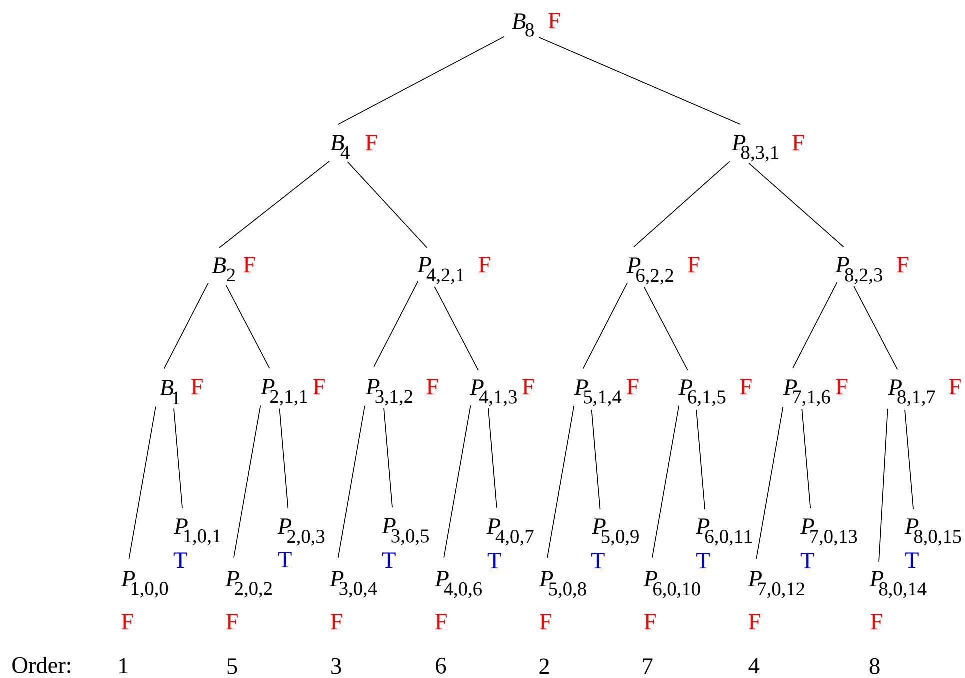


Fig. 25. Worst-case scenario for corruption site distribution (a3D).

which the new corruption occurs. This depth is a function of κ, namely, $depth = \lceil \lg \kappa \rceil$.

$$\begin{aligned}
\mathcal{V}(\kappa) &= \mathcal{V}(\kappa-1) + 2 \cdot (H - depth) \\
&= \mathcal{V}(\kappa-1) + 2 \cdot (H - \lceil \lg \kappa \rceil) \\
&= \mathcal{V}(\kappa-2) + 2 \cdot (H - \lceil \lg(\kappa-1) \rceil) + 2 \cdot (H - \lceil \lg \kappa \rceil) \\
&\vdots \\
&= \mathcal{V}(\kappa-i) + 2 \cdot (H - \lceil \lg(\kappa-(i-1)) \rceil) + \ldots + 2 \cdot (H - \lceil \lg \kappa \rceil)
\end{aligned}$$

So, in order to get a closed form, we unfold the recursion until $\mathcal{V}(\kappa - i) = \mathcal{V}(0)$, which implies $\kappa = i$. We substitute $i = \kappa$ in our recursive formula and get

$$\begin{aligned}
\mathcal{V}(\kappa) &= \mathcal{V}(0) + 2 \cdot (H - \lceil \lg 1 \rceil) + \ldots + 2 \cdot (H - \lceil \lg \kappa \rceil) \\
&= \mathcal{V}(0) + 2 \cdot \sum_{j=1}^{\kappa} (H - \lceil \lg j \rceil) \\
&= \mathcal{V}(0) + 2 \cdot \sum_{j=1}^{\kappa} H - 2 \cdot \sum_{j=1}^{\kappa} \lceil \lg j \rceil \\
&= 1 + 2 \cdot \kappa \cdot H - 2 \cdot \sum_{j=1}^{\kappa} \lceil \lg j \rceil \; .
\end{aligned}$$

If we expand the last term we find that $\sum_{j=1}^{\kappa}\lceil\lg j\rceil = 0+1+2+2+3+3+3+3+4+4+4+4+4+4+4+4+\ldots+\lceil\lg\kappa\rceil$. We observe that the terms of the sum can be divided into "groups," each group having the same number repeated a power of 2 number of times. The numbers repeated are 1, 2, 3, up to $\lceil\lg j\rceil$. Thus, we can evaluate the original sum by summing the sums of each group, e.g, $1\cdot 1+2\cdot 2^2+3\cdot 2^2+4\cdot 2^3+\ldots+j\cdot 2^{j-1}$. If κ is a power of 2 then the last "group" of numbers will be complete, otherwise we will a partial final "group." For this reason, we first add up all the complete "groups" in the sum, i.e., $\sum_{j=1}^{\lfloor\lg\kappa\rfloor} j\cdot 2^{j-1}$. Then we add what is left over, i.e., $\kappa-2^{\lfloor\lg\kappa\rfloor}$ times the last summand which is $\lceil\lg\kappa\rceil$. If we put all the terms together we get

$$\sum_{j=1}^{\kappa}\lceil\lg j\rceil = \sum_{j=1}^{\lfloor\lg\kappa\rfloor} j\cdot 2^{j-1} + (\kappa-2^{\lfloor\lg\kappa\rfloor})\cdot\lceil\lg\kappa\rceil\ .$$

We then substitute this sum evaluation into $\mathcal{V}(\kappa)$ and get the following.

$$\begin{aligned}\mathcal{V}(\kappa) &= 1+2\cdot\kappa\cdot H-2\cdot(\sum_{j=1}^{\lfloor\lg\kappa\rfloor} j\cdot 2^{j-1}+(\kappa-2^{\lfloor\lg\kappa\rfloor})\cdot\lceil\lg\kappa\rceil)\\ &= 1+2\cdot\kappa\cdot H-\sum_{j=0}^{\lfloor\lg\kappa\rfloor} j\cdot 2^{j}-2\cdot\kappa\cdot\lceil\lg\kappa\rceil+2^{\lfloor\lg\kappa\rfloor+1}\cdot\lceil\lg\kappa\rceil\end{aligned}$$

The sum $\sum_{j=0}^{\lfloor\lg\kappa\rfloor} j\cdot 2^{j}$ is evaluated using a known formula,

$$\sum_{k=0}^{n} k\cdot x^k = \frac{x-(n+1)\cdot x^{n+1}+n\cdot x^{n+2}}{(1-x)^2}, \qquad \text{for } x\neq 1\ .$$

$$\begin{aligned}\mathcal{V}(\kappa) &= 1+2\cdot\kappa\cdot H-\frac{2-(\lfloor\lg\kappa\rfloor+1)\cdot 2^{\lfloor\lg\kappa\rfloor+1}+\lfloor\lg\kappa\rfloor\cdot 2^{\lfloor\lg\kappa\rfloor+2}}{(1-2)^2}\\ &\quad -2\cdot\kappa\cdot\lceil\lg\kappa\rceil+2^{\lfloor\lg\kappa\rfloor+1}\cdot\lceil\lg\kappa\rceil\\ &= 1+2\cdot\kappa\cdot H-2+\lfloor\lg\kappa\rfloor\cdot 2^{\lfloor\lg\kappa\rfloor+1}+2^{\lfloor\lg\kappa\rfloor+1}-\lfloor\lg\kappa\rfloor\cdot 2^{\lfloor\lg\kappa\rfloor+2}\\ &\quad -2\cdot\kappa\cdot\lceil\lg\kappa\rceil+2^{\lfloor\lg\kappa\rfloor+1}\cdot\lceil\lg\kappa\rceil\\ &= 2\cdot\kappa\cdot H-1+2^{\lfloor\lg\kappa\rfloor+1}\cdot(\lfloor\lg\kappa\rfloor+1-2\cdot\lfloor\lg\kappa\rfloor+\lceil\lg\kappa\rceil)-2\cdot\kappa\cdot\lceil\lg\kappa\rceil\\ &= 2\cdot\kappa\cdot H-1+2^{\lfloor\lg\kappa\rfloor+1}\cdot(\lceil\lg\kappa\rceil-\lfloor\lg\kappa\rfloor+1)-2\cdot\kappa\cdot\lceil\lg\kappa\rceil\\ &= 2\cdot\kappa\cdot(H-\lceil\lg\kappa\rceil)+(\lceil\lg\kappa\rceil-\lfloor\lg\kappa\rfloor+1)\cdot 2^{\lfloor\lg\kappa\rfloor+1}-1\\ &= 2\cdot\kappa\cdot(H-\lceil\lg\kappa\rceil)+([\kappa\neq 2^i]+1)\cdot 2^{\lfloor\lg\kappa\rfloor+1}-1\,, \qquad \text{for some } i\in\mathbb{N}\cup\{0\}\end{aligned}$$

Here we use Iverson brackets [13, p. 24]. □

Note that for values of κ between $D/2$ and D the value of $\mathcal{V}(\kappa)$ is unchanged at $\mathcal{V}(D/2)=2\cdot D-1$. This is because, as we have seen above, when κ is equal or exceeds $D/2$ all the hash chains covering the first D days will have to be validated.

Thus we can calculate the cost during forensic analysis quite simply.

$$\mathit{ForensicAnalysis}_{a3D} = \mathcal{V}(\kappa)$$

Table XIII. **Forensic areas for $1 \leq \kappa \leq D$ corruption sites (a3D).**

# Corruption Sites ($1 \leq \kappa \leq D$)	$Area_P$	$Area_U$	$Area_N$
1	N	0	$TotalArea - N$
2	N	0	$TotalArea - N$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
κ	N	0	$TotalArea - N$

We now examine the breakdown of the three types of areas in the a3D Algorithm. Each granule corresponds to a distinct region of area of height $V \cdot N = N$ (normalized) and width 1 (!) and thus, total $Area_P = \kappa \cdot V \cdot N = \kappa \cdot N$. Moreover, since this algorithm will detect all κ corruption sites this implies that $Area_U = 0$. The breakdown of the different areas is given in Table XIII.

$$
\begin{aligned}
FC_{a3D}(D, N, 1, \kappa) &= (D/N + \mathcal{N}(D) + D/N - (1 + \lfloor \lg(D/N) \rfloor) \\
&\qquad\quad + \mathcal{V}(\kappa)) \\
&\quad + Area_P \\
&= (D/N + 2 \cdot D - 1 + D/N - (1 + \lfloor \lg(D/N) \rfloor) \\
&\qquad\quad + 2 \cdot \kappa \cdot (\lceil \lg D \rceil - \lceil \lg \kappa \rceil) + (1 + [\kappa \neq 2^i]) \cdot 2^{\lfloor \lg \kappa \rfloor + 1} - 1) \\
&\quad + (\kappa \cdot N) \qquad\qquad (6) \\
&= O(\kappa \cdot N + D + \kappa \cdot \lg D)
\end{aligned}
$$

In the case of the a3D Algorithm we see an increase in the cost of normal processing and forensic analysis, but the area produced by this algorithm is optimal. $Area_U$ is zero while $Area_P$ achieves its minimum because, by definition, each granule cannot be shrunk below the spatial resolution R_s (as discussed in Section 8.4). For a reason why the *temporal* dimension of the area, i.e., the uncertainty of t_c, cannot be shrunk further, see Section 10.

Finally, when $\kappa > D/2$, rather than doing κ binary searches, we can simply scan the R_r units, reducing the forensic cost to $O(\kappa \cdot N + D + D) = O(\kappa \cdot N)$.

E. FORENSIC COST FOR BEST-CASE DISTRIBUTION OF CORRUPTION SITES

We perform an analysis of the forensic cost of the four algorithms assuming a *best-case* distribution of κ corruption sites.

E.1 Monochromatic Algorithm

A best-case distribution for the Monochromatic algorithm occurs when each of the κ corruption sites appears in a different notarization interval at the rightmost end of the trapezoid in the corruption diagram. This means that the sites occur starting from the most recent I_N and go back to older notarization intervals in a contiguous manner, as shown in Figure 26. As in Section 9 we examine how each corruption site partitions the trapezoid—bound by the last validation event—into the three types of forensic area, i.e., $Area_P$, $Area_U$, and $Area_N$. Observe that unlike in the worst-case distribution the corruption sites are examined from right to left. This, in conjunction with the fact that only one corruption site occurs within each notarization interval, allows each site to be positively identified. Hence, Table XIV shows that each site is associated with an $Area_P$ but not with an $Area_U$.

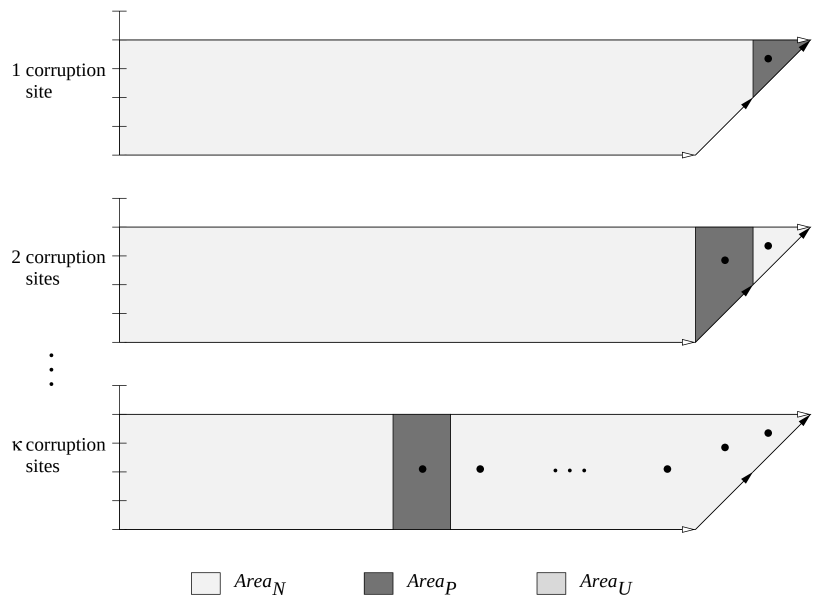


Fig. 26. Three types of forensic area for best-case distribution of κ corruption sites (Monochromatic).

All the terms in the forensic cost formula remain the same as in the worst case except for the forensic areas. Summing $Area_P$ over all corruption sites we can compute the forensic cost for the Monochromatic Algorithm.

$$\begin{aligned} FC_{mono}(D, 1, V, \kappa) &= (D + D/V + 2 \cdot \lg D) \\ &\quad + (V + \sum_{i=2}^{\kappa} V) \\ &= D + D/V + 2 \cdot \lg D + V + (\kappa - 1) \cdot V \\ &= O(\kappa \cdot V + D) \end{aligned}$$

The forensic cost of the Monochromatic Algorithm for best-case distribution is asymptotically smaller than cost for worst-case distribution which is $O(\kappa \cdot V \cdot D)$.

Table XIV. **Forensic areas for best-case distribution of κ corruption sites (Monochromatic).**

# Corruption Sites $(1 \leq \kappa \leq D)$	$Area_P$	$Area_U$	$Area_N$
1	V	0	$TotalArea - V$
2	V	0	$TotalArea - V$
3	V	0	$TotalArea - V$
⋮	⋮	⋮	⋮
κ	V	0	$TotalArea - V$

E.2 RGBY Algorithm

In the case of the RGBY Algorithm the *best* case distribution of corruption sites is exactly the same as in the Monochromatic Algorithm. The sites occur starting from the most recent I_N and go back to older notarization intervals in a contiguous manner, as shown in Figure 27. Once again because of the assumption of only one site per I_N we have only positive areas associated with each site.

Table XV. **Forensic areas for best-case distribution of κ corruption sites (RGBY).**

# Corruption Sites $(1 \leq \kappa \leq D)$	$Area_P$	$Area_U$	$Area_N$
1	2	0	$TotalArea - 2$
2	2	0	$TotalArea - 2$
3	2	0	$TotalArea - 2$
⋮	⋮	⋮	⋮
κ	2	0	$TotalArea - 2$

Table XV shows the breakdown of the three types of the forensic areas for each of the κ corruption sites. All the terms in the forensic cost formula remain the same as in the worst case except for the forensic areas. Summing $Area_P$ over all corruption sites we can compute the forensic cost for the RGBY Algorithm.

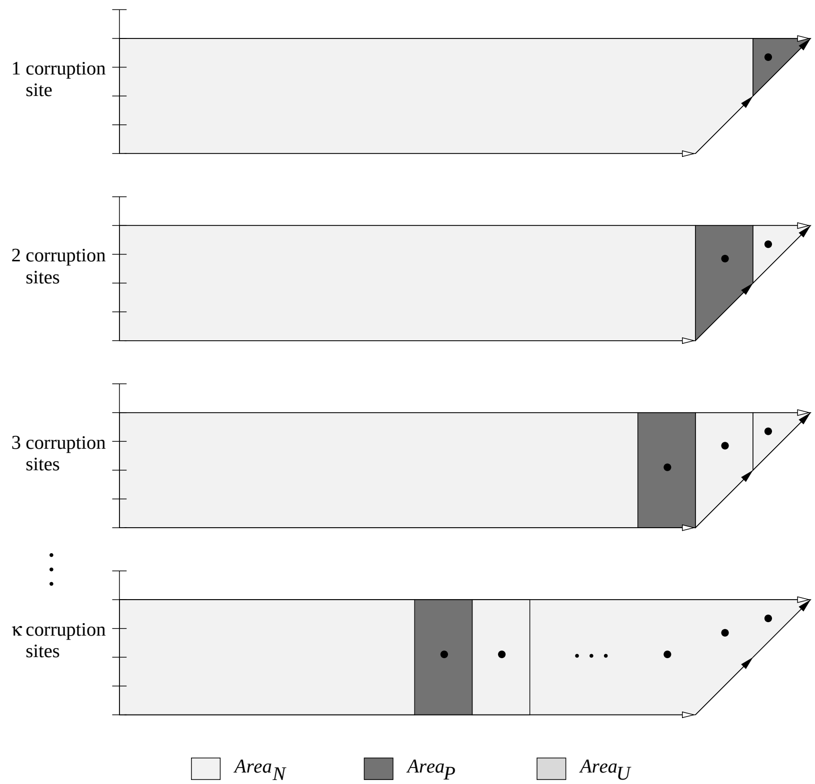


Fig. 27. Three types of forensic area for best-case distribution of κ corruption sites (RGBY).

$$\begin{aligned} FC_{RGBY}(D,1,2,\kappa) &= (D + 3\cdot(D/2) + 2\cdot(D/2) + 2\cdot \lg D) \\ &\quad + (\sum_{i=1}^{\kappa} 2) \\ &= O(\kappa + D) \end{aligned}$$

The forensic cost of the RGBY Algorithm for best-case distribution is asymptotically the same as the cost for worst-case distribution which is also $O(\kappa + D)$.

E.3 Tiled Bitmap Algorithm

The best-case distribution for the Tiled Bitmap Algorithm happens when the corruption sites occur one in each tile, tampering the last granule in the tile as shown in Figure 28. The resulting bit string uniquely identifies the corrupted granule so we can positively identify the corruption site in the tile with no false positives.

Table XVI shows that each $Area_P$ has area $V \cdot N$, and thus summing over all corruption sites yields the new forensic cost.

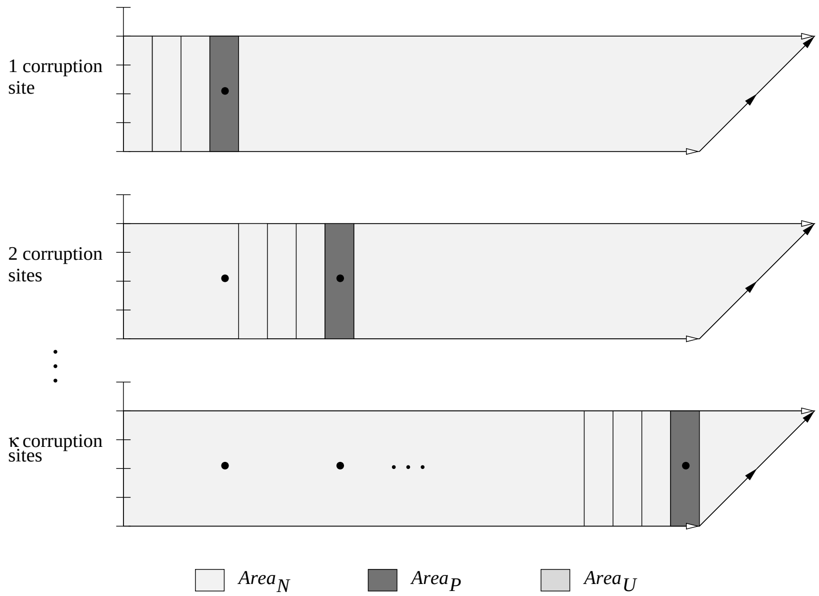


Fig. 28. Three types of forensic area for best-case distribution of κ corruption sites (Tiled Bitmap).

Table XVI. **Forensic areas for best-case distribution of κ corruption sites (Tiled Bitmap).**

# Corruption Sites $(1 \leq \kappa \leq D)$	$Area_P$	$Area_U$	$Area_N$
1	$V \cdot N$	0	$TotalArea - V \cdot N$
2	$V \cdot N$	0	$TotalArea - V \cdot N$
3	$V \cdot N$	0	$TotalArea - V \cdot N$
⋮	⋮	⋮	⋮
κ	$V \cdot N$	0	$TotalArea - V \cdot N$

$$
\begin{aligned}
FC_{tiled\_bitmap}(D, N, V, \kappa) &= ((D/N) + (1 + \lg N) \cdot (D/N) + D/(V \cdot N) \\
&\qquad + 2 \cdot \lg(D/N) + (1 + \lg N) \cdot \kappa) \\
&\quad + (\kappa \cdot V \cdot N) \\
&= O(\kappa \cdot V \cdot N + (D \cdot \lg N)/N + \lg D)
\end{aligned}
$$

The new cost is asymptotically lower than the corresponding cost for worst-case distribution. In particular, the $\kappa \cdot V \cdot N^2$ term in the worst-case cost has lost a factor of N.

E.4 a3D Algorithm

The best-case distribution of corruption sites for the a3D Algorithm is one in which the sites occur consecutively in leaves of the tree as shown in Figure 29. The numbers labeled with "Order of κ" show the order with which the sites are examined. This order is such that moving from one site to the next incurs a minimum increase in the number of chains validated in the tree. This defers the validation of the entire tree until the last (16^{th}) site has been examined.

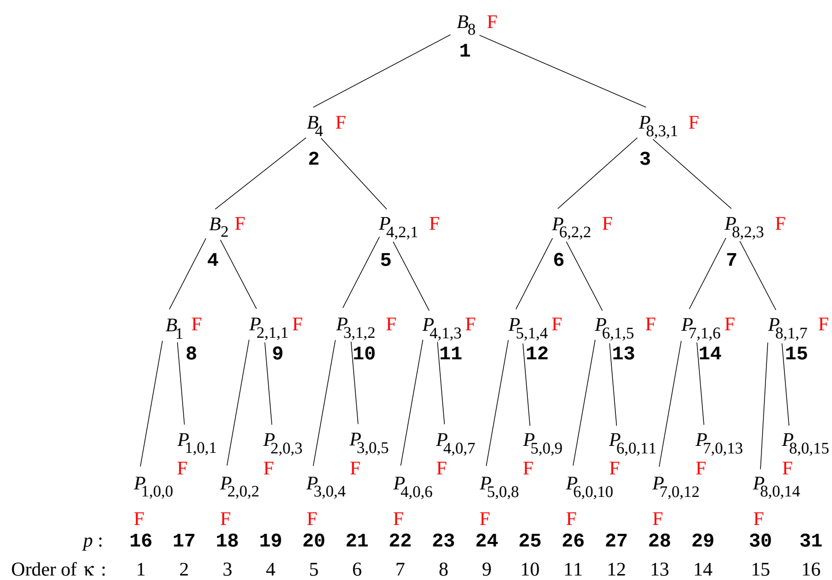


Fig. 29. Three types of forensic area for best-case distribution of κ corruption sites (a3D).

The number of validations in the forensic analysis with each successive corruption site satisfies the following recursive formula,

$$\mathcal{V}_b(\kappa) \; = \; \mathcal{V}_b(\kappa - 1) + 2 \cdot (H - depth_b(\kappa)) \qquad \text{for } 1 \le \kappa \le D \; , \tag{7}$$

where $\mathcal{V}_b(\kappa)$ is the number of hash chains validated by the algorithm when κ corruption sites exist under a *best*-case distribution, the height of the tree H is $\lg N + \lceil \lg(D/N) \rceil = \lceil \lg D \rceil$, and $depth_b(\kappa)$ is the depth of the root of the maximal-height subtree in which the new corruption site occurs, again, under a best-case distribution. The validation of the hash chain corresponding to this root evaluates to true before the κ^{th} corruption occurs and false afterwards.

To find how $depth_b$ depends on κ we first number the nodes of the tree in a breadth-first manner. The numbers are shown in `courier` font in Figure 29. Observe that the leaves under this numbering scheme are labeled by p and the correspondence between p and κ is $p = \kappa + D - 1$. Observe also that we only need to deal with leftmost paths of subtrees since any site occurring in a leaf of a rightmost path contributes zero to $\mathcal{V}_b$. Recall that for all nodes in a binary tree if the parent has index i its children have indices $2 \cdot i$ and $2 \cdot i + 1$. Hence, in order to find the number of the root (inner node) of the subtree given a p number of a leftmost leaf we must divide p by 2^x where x is the maximum integer such that $2^x \mid p$ but $2^{x+1} \nmid p$. In other words, x is the zero-based index, counting from the right end, of the leftmost "1" in the binary representation of p. We can use Iverson brackets [13, p. 24] to express x as the sum $x = \sum_{1 \le l \le \lfloor \lg p \rfloor} [p \bmod 2^l = 0]$. Given the position of the root we can find its depth by the following formula:

$$depth_b(\kappa) \;=\; \lfloor \lg(\frac{p}{2^x}) \rfloor \tag{8}$$

where $p = \kappa + D - 1$ and $x = \sum_{1 \le l \le \lfloor \lg p \rfloor} [p \bmod 2^l = 0]$.

We can now substitute (8) in the recursion, unfold it, and get a closed form:

$$\mathcal{V}_b(\kappa) = 1 + 2 \cdot \kappa \cdot \lg D - 2 \cdot \sum_{i=1}^{\kappa} \lfloor \lg \left((p-i)/(2^{\sum_{1 \le l \le \lfloor \lg (p-i) \rfloor} [(p-i) \bmod 2^l = 0]}) \right) \rfloor$$

We do not attempt to evaluate the sum but we rather try to find the asymptotic upper bound for $\mathcal{V}_b$. The idea is to minimize the value of the sum so that the entire expression can be bounded from above. The minimum value the numerator in the summand can take is $D-1$ when $i = \kappa$, while the maximum value the denominator can take is $2^H = D$, i.e., when we are considering the root of the entire tree. This makes the sum easy to bound as shown in equation (9).

$$\begin{aligned}
\mathcal{V}_b(\kappa) \;&=\; 1 + 2 \cdot \kappa \cdot \lg D - 2 \cdot \sum_{i=1}^{\kappa} \lfloor \lg \left((p-i)/(2^{\sum_{1 \le l \le \lfloor \lg (p-i) \rfloor} [(p-i) \bmod 2^l = 0]}) \right) \rfloor \\
&\le\; 1 + 2 \cdot \kappa \cdot \lg D - 2 \cdot \sum_{i=1}^{\kappa} \lg((D-1)/D) \\
&\le\; 1 + 2 \cdot \kappa \cdot \lg D - 2 \cdot \kappa \lg((D-1)/D) \\
&\le\; 1 + 2 \cdot \kappa \cdot \lg D + 2 \cdot \kappa \lg(D/(D-1)) \\
&\le\; 1 + 2 \cdot \kappa \cdot \lg D + 2 \cdot \kappa \cdot \lg D \Rightarrow \\
\mathcal{V}_b(\kappa) \;&=\; O(\kappa \cdot \lg D)
\end{aligned} \tag{9}$$

Putting everything together we can now evaluate the best-case forensic cost of the a3D Algorithm.

$$\begin{aligned}
FC_{a3D}(D, N, 1, \kappa) \;&=\; (D/N + \mathcal{N}(D) + D/N - (1 + \lfloor \lg(D/N) \rfloor) \\
&\qquad\quad + \mathcal{V}(\kappa)) \\
&\quad + Area_P \\
&=\; (D/N + 2 \cdot D - 1 + D/N - (1 + \lfloor \lg(D/N) \rfloor) \\
&\qquad\quad + \kappa \cdot \lg D) \\
&\quad + (\kappa \cdot N) \\
&=\; O(\kappa \cdot N + D + \kappa \cdot \lg D)
\end{aligned}$$

Table XVII. **Forensic areas for average-case distribution of κ corruption sites (Monochromatic).**

# Corruption Sites $(1 \leq \kappa \leq D)$	$Area_P$	$Area_U$	$Area_N$
1	V	0	$TotalArea - V$
2	0	$(2 \cdot TotalArea - V)/3$	$(TotalArea + V)/3$
3	0	$(3 \cdot TotalArea - V)/4$	$(TotalArea + V)/4$
⋮	⋮	⋮	⋮
κ	0	$(\kappa \cdot TotalArea - V) \cdot \frac{1}{\kappa+1}$	$(TotalArea + V) \cdot \frac{1}{\kappa+1}$

The asymptotic forensic cost for the worst-case distribution is thus identical to that for the best-case distribution of a large number of corruption sites, namely, $O(\kappa \cdot N + D + \kappa \cdot \lg D)$.

F. FORENSIC COST FOR AVERAGE-CASE DISTRIBUTION OF CORRUPTION SITES

In this section we give an analysis of the forensic cost of the four algorithms assuming an average distribution of κ corruption sites. The analysis for the Monochromatic and RGBY Algorithms are similar in approach and detail, i.e., for each corruption site we examine how it partitions the trapezoid bound below by the last validation event, into the three types of forensic area $Area_P$, $Area_U$, and $Area_N$. However, to obtain an estimate of the forensic cost of the Tiled Bitmap Algorithm we employ the average size of the candidate set instead of considering the distribution of the corruption sites. In the case of the a3D Algorithm the analysis is much simpler since we have shown that the forensic cost is the same for best and worst case distributions of corruption sites.

F.1 Monochromatic Algorithm

In order to obtain a bound on the forensic cost of the Monochromatic Algorithm we assume that the κ corruption sites are evenly distributed in the trapezoid as shown in Figure 30. Each successive “addition” of a corruption site splits the area evenly and hence if there are κ sites then each intervening area between them has size $(TotalArea - \kappa \cdot V)/(\kappa + 1)$.

Figure 30 shows that only the first corruption site can be positively identified as was true in the worst-case distribution. We consider the forensic cost of a single corruption site ($\kappa = 1$) separately from the cases where $\kappa > 1$, the reason being the area breakdown is different in the two cases. Notice that for $\kappa \geq 2$, the last term in the cost formula (10) is a partial sum of a harmonic series. It is an established result [13, p. 276] that a partial sum of the harmonic series H_n is bounded above by $\lfloor \lg n \rfloor + 1$.

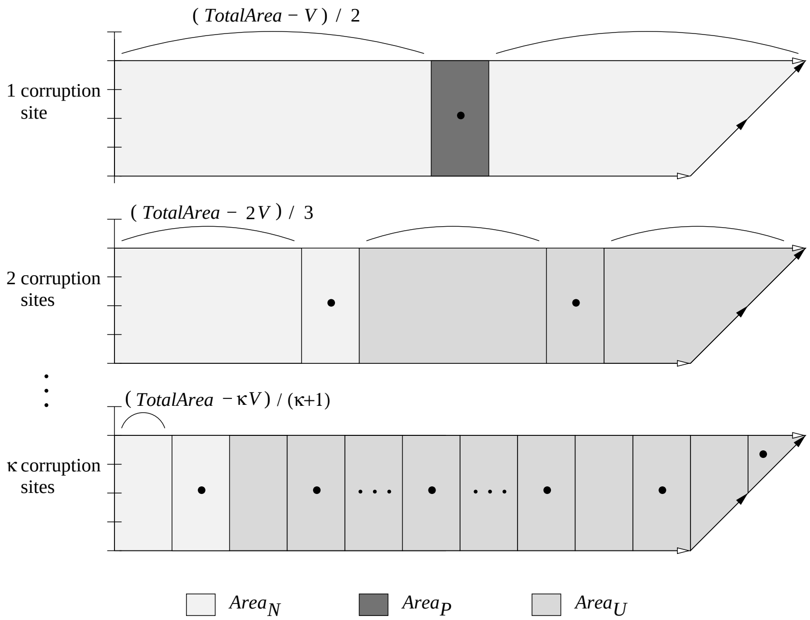


Fig. 30. Three types of forensic area for average-case distribution of κ corruption sites (Monochromatic).

$$
\begin{aligned}
FC_{mono}(D,1,V,1) &= (D + D/V + 2\cdot \lg D) + V \\
&= O(V + D) \\
FC_{mono}(D,1,V,\kappa \geq 2) &= (D + D/V + 2\cdot \lg D) \\
&\quad + (V + \sum_{i=2}^{\kappa}(i \cdot \mathit{TotalArea} - V)/(i+1)) \\
&\leq D + D/V + 2\cdot \lg D + V + (\kappa - 1)\cdot \mathit{TotalArea} \\
&\quad - V \cdot \sum_{i=2}^{\kappa} 1/(i+1) \qquad (10) \\
&\leq D + D/V + 2\cdot \lg D + V + (\kappa - 1)\cdot \mathit{TotalArea} \\
&\quad - V\cdot(\lfloor \lg(\kappa+1)\rfloor - 1/2) \\
&= O(\kappa \cdot V \cdot D)
\end{aligned}
$$

The forensic cost of the Monochromatic Algorithm for the average case distribution is asymptotically the same as the cost for worst-case distribution.

F.2 RGBY Algorithm

The forensic cost of the RGBY Algorithm for the worst-case distribution of κ corruption sites is asymptotically the same as the one for best-case distribution: $O(\kappa + D)$. This implies that the forensic cost for the average case distribution of corruption site is the same.

F.3 Tiled Bitmap Algorithm

To obtain an estimate of the forensic cost of the Tiled Bitmap Algorithm, we do not consider the distribution of the κ corruption sites. Rather, for each site we must deduce its relative position within a tile so that the size of the candidate set can be computed. Furthermore, given a uniform distribution of κ, we have no way of enforcing that each site will belong to a different tile. For these reasons we consider the average size of the candidate set instead.

LEMMA 1. *The average cardinality of the candidate sets for* $k = 2$ *and for a given* $l = \lg N$ *is* $\overline{|C|} = \frac{3^l - 1}{2^l}$.

PROOF. The average is $\overline{|C|} = \frac{1}{2^l} \cdot \left((\sum_{z=0}^{l} \binom{l}{z} \cdot 2^z) - 1 \right)$. $\sum_{z=0}^{l} \binom{l}{z} \cdot 2^z$ is the binomial expansion of $(2+1)^l = 3^l$. So $\overline{|C|} = \frac{3^l - 1}{2^l}$. □

Note that $\overline{|C|} = \frac{3^l - 1}{2^l} < 1.5^l = O(1.5^l)$. For $l = 10$ a candidate set will contain on average about 5% of the possible binary numbers of length l. For $l > 20$ a candidate set will contain on average only about 0.3% of the possible strings. This is expected since the fraction $\frac{1.5^l}{2^l}$ decreases as l increases.

This decrease in candidate set cardinality as l increases has implications for forensic analysis. Recall that the goal is to determine the set of possible corruption events implied by a provided target binary number. While the number of possibilities grows as l gets larger, the *percentage* of possible granules declines.

We have showed that the average cardinality of all possible candidate sets for a fixed-length *target* is $\overline{|C|} = (3^l - 1)/2^l$. Recall that $l = \lg N$.

$$\begin{aligned} Area_P &= \sum_{i=1}^{\kappa} \overline{|C|} \cdot V \cdot N = \kappa \cdot \frac{3^{\lg(N)} - 1}{2^{\lg(N)}} \cdot V \cdot N = \kappa \cdot \frac{3^{\lg_3(N)/\lg_3 2} - 1}{N} \cdot V \cdot N \\ &= \kappa \cdot V \cdot (N^{\lg 3} - 1) \end{aligned}$$

Thus the forensic cost of the algorithm, taking the average cardinality of the candidate set, is

$$\begin{aligned} FC_{tiled\_bitmap}(D, N, V, \kappa) &= ((D/N) + (1 + \lg N) \cdot (D/N) + D/(V \cdot N) \\ &\qquad + 2 \cdot \lg(D/N) + (1 + \lg N) \cdot \kappa) \\ &\quad + (\kappa \cdot V \cdot (N^{\lg 3} - 1)) \\ &= O(\kappa \cdot V \cdot N^{\lg 3} + (D \cdot \lg N)/N + \lg D) \ . \end{aligned}$$

This replaces a factor of N^2 with $N^{\lg 3}$ making the average cost asymptotically lower than in the worst case.

F.4 a3D Algorithm

The forensic cost of the a3D Algorithm for the worst-case distribution of κ corruption sites is asymptotically the same as the one for best-case distribution: $O(\kappa \cdot N + D + \kappa \cdot \lg D)$. This implies that the forensic cost for the average case distribution of corruption site is the same.