Secure Multilayer Database System for Digital Image Archiving

Sos S. Agaian and Okan Caglayan
Nonlinear Signal Processing Laboratory,
Univ. of Texas at San Antonio, Texas, USA

Natalie Granado
Center for Infrastructure Assurance and Security,
Univ. of Texas at San Antonio, Texas, USA

Abstract

The focus of this paper is to have a secure digital media storage technology for creating, preserving, cataloging, indexing and retrieving images, documents and different types of signals in digital media format. The most secure multilayer database system exists with encrypted data files so that an outside source cannot easily access the classified information. The problem with this technique is when an unauthorized client has the knowledge regarding the existence of the secured data in a system; this can make the system vulnerable to alterations, extraction or destroying of the secured data.

This paper presents a new conceptual framework of a secure multilayer database system for archiving digital images by using steganographic techniques.

The key components of the proposed multilayer system are:

1. Integration of security techniques; steganography and cryptography.
2. Enhancement of the storage capacity.

1. Introduction

A large database is likely to be multilayer – that is, composed of several different schemas, with physical (source) schemas at the bottom and virtual (view) schemas layered on top. The multilayer database system has security classification (access control) where users with low-level clearance can only access the cover database. Users with higher levels of security clearances can access the information that contains classified embedded messages within the layers of the classified database and the cover database. Multilayer databases take many forms. For example, a set of view tables can be used to insulate applications from stored tables that have been partitioned or denormalized, and which change as the workload changes. A federated database provides a virtual schema above multiple sources. A data warehouse gathers and transforms data and stores it in a separate server; this can be seen as computing a materialized view (subject to delays in propagating source updates).[12]

Classical database security relies on many different mechanisms and techniques.[3,4] The operating system, network security, access control, data and user authentication are among the few of these. The advantage is to develop a systematic understanding of database security problems and their solutions and to come up with an outline. Ideally, this kind of an outline should give some assurance that all relevant security problems have been addressed, and it can possibly point out new security issues.[5] The concern for security arises when the database contains vital information with a variety of classification levels. The most database systems exist with encrypted data files so that an outside source cannot easily access the classified information. Encryption is the key element and implemented in the innermost layer of the multilayer database systems. While there are many good reasons to encrypt data, there are many bad reasons to encrypt data. Once an unauthorized client becomes aware of the secured data, the system becomes vulnerable and can potentially be compromised. Encryption does not solve all the security problems, and may even make some problems worse. For example:

1. Encryption does not solve access control problems.
2. Encrypt everything does not make data secure-encrypted data can be deleted or modified.[10,11]

The fundamental goal of any security system is to increase their safety measures. Recently, steganography has become very popular. Steganography (literally, covered writing) is the hiding of secret messages within another seemingly innocuous message, or carrier. Steganography, like cryptography, is a means of providing secrecy.[9] The difference between the steganography and cryptography is that in cryptography, the user can tell that a message has been encrypted, but the user cannot decode the message without knowing the proper key. On the other hand, in steganography, the message itself may not be difficult to decode, but it is invisible to an outside source. In general, a

database must release information to support legitimate activities; at the same time, it must secure sensitive information from unauthorized users in the event an unauthorized user gains access into the database. One of possible approach for increasing safety measures of a database is to use the art of steganography. It is adventitious to use the steganographical and cryptographical techniques simultaneously to get higher security and to have more flexibility.

This paper attempts to strengthen the weakness of many secure databases and to increase the security measures by hiding second database inside the existing database. The key element of building a secure multilayer database is to be able to prevent outside access from hackers intruding into the database. In addition to the security, we may enhance the storage capacity of the database by dilating the non-informative data and by embedding vital information.

2. Background

Our focus was to address the database security issues in a general level in which an outside source could become a threat to the vital information. First, we addressed the unilateral and multilateral security. Secondly we defined the first level of the database security of the proposed system, before the level of the application of steganographic technique. In many security-relevant applications, security is seen as a unilateral problem: Some system (or entity, or collection of entities) must be protected against a malicious outsider, often called an attacker. The system is secure if no attacker can cause any significant difference of the system from the specified behavior.[2] This includes, for example, that the attacker cannot extract classified information. Typical examples of unilateral security problems are the protection of a computer system by security mechanisms of the operating system, as well as the protection of an organization's internal network against hackers, for instance by firewalls and intrusion detection technology. Database security is often seen as a unilateral security problem: The database system must be protected against the outside sources and possibly also against potentially malicious users.[2] In contrast to unilateral security, many security-relevant applications require the protection of several parties, each against the potential misbehavior of some other parties, possibly against all other parties. A simple example of bilateral security is on-line transactions where both the customer and the vendor want to be protected against malicious behavior by the other. In practice, such bilateral security issues are often not really addressed and instead solved by assuming that one of the parties, for example the vendor, is trustworthy.[2]

The example of multilateral security, involving three entities, is on-line auctions. The auctioneer, the bidder, and the party ordering an object need to be protected against possible fraud by another party (and, of course, also against external attackers). An even higher level of security is achieved if each party is protected against the other two parties cheating collectively with a joint strategy.[2] As we discussed unilateral and multilateral securities in the database, we wanted to address the security measures that we took in our database design for the initial level of security.

Authentication and Authorization

Initial security mandated the user to pass through two stages of security: authentication and authorization.[7] The authentication identified the user using the login information and verified only the permissions to connect to the instance of the database. If authentication was successful, the user would have to be authorized. Then, the user needed the authorization from the database administrator who monitored the user accounts. Without appropriate authorization, the authenticated users could not do anything towards the database. After the authorization procedure, the user had to pass through the access control, which we briefly discussed in the next section. The authorizations in the database were set on the basis of the security policy of the Nonlinear Signal Processing Laboratory.

Access Control

After the authentication and authorization levels, the user had to pass through the access control. The purpose of the access control was to limit the actions or operations that a legitimate user of a computer system could perform. In access control systems a distinction was made between policies and mechanisms. Policies were the high level guidelines that determined how accesses were controlled and access decisions determined. Mechanisms were the low-level software and hardware functions that could be configured to implement a policy.[6] Figure 1 shows the database security diagram.

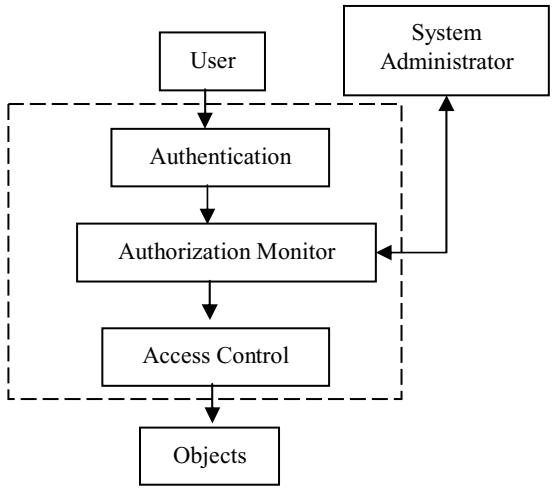

Figure 1. Database Security (DB Security) structure diagram

3. Steganography in Multilayer Database

Figure 2 shows the basic blocks diagram of a steganographic system[9]:

In the conventional application of steganographic techniques, the message retrieval algorithm does not consider

the recovery of the cover media hundred percent. In contrast, in our proposed method, we will reconstruct the cover media and the secret message, so that functionality of the database will be fully accomplished.

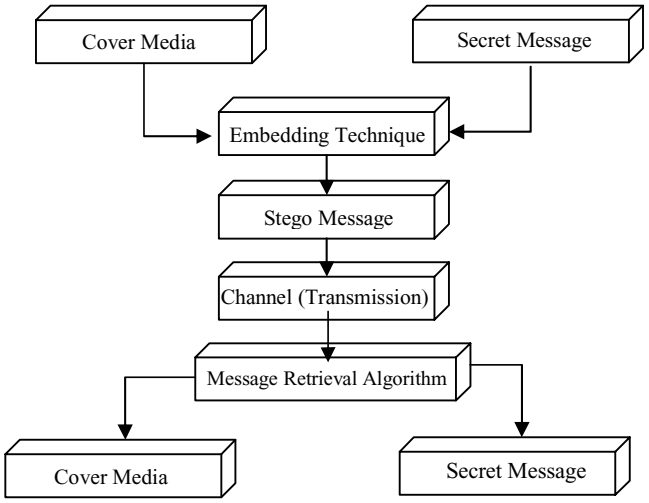

Figure 2. A Structure Diagram of a steganographic system

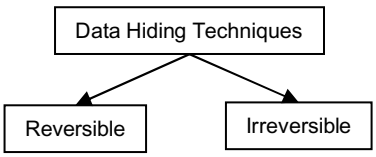

Figure 3. Steganographic Techniques

The two types of steganographic techniques are lossy (irreversible) and lossless (reversible) data hiding.[8] Data hiding is referred to as a process to embed useful data (representing some information) into a cover media. In these techniques invisibility is the major requirement.

In lossy data hiding, the cover media will experience some distortion and cannot be inverted back to the original media. That is, some permanent distortion exists even after the hidden data has been extracted. On the other hand, in lossless data hiding, it is desired to reverse the marked media back to the original cover media after the hidden data is retrieved. As a numerical example, given a *2048 x 1296* cover image in the size of *7.59 MB* has the embedded data capacity of *2 MB* by using several Least Significant Bits, without having any distortion to the cover image.[14]

In applying the steganographic technique, we employed the lossless (reversible) data hiding in the classified layer of the database. In the algorithm, we modified Least Significant Bits (LSB) of the cover image in order to embed the vital information.[8] Every color image could be represented by the sum of red, green and blue components. This procedure was referred to as the color image decomposition. Therefore, we took an image and decomposed it into its three components. Within each component, the bit plane images were generated. We took the LSB plane of the given layer, calculated the redundancy defined as the difference between the numbers of pixels, and proceeded to higher bit-planes until the redundancy became greater or equal to the size of the information that needed to be embedded.[13] The pixels, which were close to zero or the minimum point of the bit plane, were scanned and slightly modified to embed the data (information). Extraction of the embedded information proceeded in the reverse order. The bit-plane was first decomposed, the information was decoded, and the compressed bit-plane was decompressed. The encoded bit-plane was replaced with the decompressed original. The embedded information was reconstructed from the color image. By utilizing the lossless data hiding technique, the vital information became invisible and more secure than the conventional database systems. In general the size of a secure data is not big, so the embedding large data (information) comparable to the image size can cause detection of the secret data.

Multilayer Database System

In the multilayer database system, we stored the unclassified digital media (original images) in the cover database as low-level security necessary for users to access the data pertained to the original image sets. Within the subsequent layers of the database, we stored the steganographic images that contain vital information. The common user may request the information related to the cover database. This information along with the invisible classified information is obtained simultaneously. The authorized user is the only personnel with the highest level of security privileges and therefore obtains the right of entry. The authorized user will have prior knowledge of the classified database and can request the vital information accordingly. Once the authorized client has accessed the classified database, each of the entities will also have the access control. This allows the classified database to have the highest level of security. Even if an unauthorized user (hacker) is aware of the classified database and has passed the authentication, authorizations and access control, the Steganographic technique will prevent the hacker from obtaining the vital information.

Figure 4 shows a multilayer design of the database system where hidden images are un-viewable to any outside source. An example of the cover database (the images that are open to public for information) contains the cultural images provided by the Institute of Texan Cultures.[1] The embedded database has different types of files, such as text, color images and various signals, all of which contain embedded information. In Figure 4, both the cover and the classified database have three entities and various numbers of attributes. The structure of this system is based on the relation of their attributes.

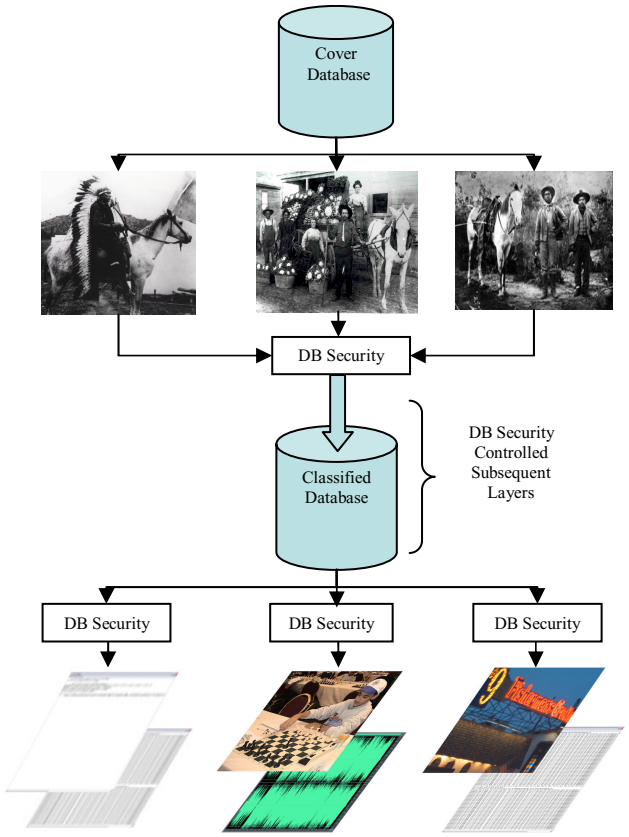

Figure 4. Users with secret clearance level or higher will have the access to the both layers of the database. Higher levels of security clearances or personnel on a need to know basis will have access to other database layers.

The Nonlinear Signal Processing Laboratory is providing a Dell Poweredge 4600 Server that will allow us to implement the proposed database system with the application of Microsoft SQL Server 2000 software. We will be using SQL to tie the information stored in the cover database to the classified database. By linking at least one of the attributes in each of the databases, the Database Management System (DBMS) will obtain the requested information simultaneously. An example of similar attributes between the two databases is the number of pixels of the image. By linking the number of pixels in each of the databases, we will be able to return the requested information to the user. However, as previously stated, the classified information will be invisible to all except those who have the appropriate clearance and the need to know.

The main advantage of the steganographic techniques is that the embedded information (data) within the cover image is invisible to an outside source. The Secure Multilayer Database System allows the user to consolidate an unclassified and classified database. This consolidation will save the consumer time, energy, and the money it costs to operate and maintain two separate systems.

4. Conclusions and Future Work

In this paper we have presented a steganographic technique based, a secure multilayer database system for archiving digital media (texts, images, audio and video) with highest level of security. The key components of the proposed multilayer system are: integration of two data hiding techniques; steganography and cryptography; double security towards the database systems; enhancement of the storage capacity. The main advantage of the steganographic techniques is that the embedded information (data) within the cover image is invisible to an outside source. We use the both types of steganographic techniques lossy and lossless. The lossy steganographic techniques are used when the original digital data is distorted by some small amount information, in which lossless data hiding case we reserve the digital media.

Acknowledgement

This research was partially funded by the Center for Infrastructure Assurance and Security under contract with the US Air Force (Air Force Research Laboratory), and Air Force Information Warfare Center. We would additionally like to express our appreciation to June Rodriguez for the contribution of a multitude of digital images for analytical support.

References

1. John L. Davis, “Texans One and All”, Institute of Texan Cultures,
2. URL:http://www.texancultures.utsa.edu/publications/ texansoneandall/texans.htm
3. Ueli Maurer; “The Role of Crytography in Database Security”, *SIGMOD 2004*, June 13-18 2004, Paris, France
4. Dan Thomsen, Mary Denz, “Incremental Assurance for Multilevel Applications”, *Computer Security Applications Conference, 1997. Proceedings.*, *13th Annual* , pp. 81-88, 8-12 Dec. 1997
5. Bhavani Thuraisingham, William Ford, “Security Constraint Processing in a Multilevel Secure Distributed Database Management System”, *Knowledge and Data Engineering, IEEE Transactions on*, pp. 274-293 Volume: 7, Issue: 2, April 1995
6. S.H. Son, “Real-Time Database Systems: Present and Future”, *Real-Time Computing Systems and Applications, 1995. Proceedings., Second International Workshop on* , pp. 50-52, 25-27 Oct. 1995
7. Raghu Ramakrishnan, “Database Management Systems”, The McGraw Hill Companies Inc., 1998
8. P. Ponniah, “Database Design and Development”, IEEE Press, Wiley-Interscience, 2003
9. Zhicheng Ni, Yun Shi, Nirwan Ansari, and Wei Su, “Reversible data hiding”, *IEEE Proceedings of ISCAS’03*, vol.2, pp.II-912-II-915, May 2003.
10. Neil Johnson, Zoran Duric, Sushil Jajodia; “Information Hiding: Steganography and Watermarking – Attacks and

Countermeasures", Kluwer Academic Publishers, Second Printing 2001.
11. "Oracle9i Application Developer's Guide-Fundamentals, Release2 (9.2)", Part Number A965990-01, Oracle, http://download-west.oracle.com/docs/cd/B10501_01/appdev.920/a96590/adgsec01.htm#1004586
12. Qiang Lin; "Defense In-Depth to Achieve "Unbreakable" Database Security", *Proceedings of the 2nd International Conference on Information Technology For Application (ICITA)*, 2004
13. Arnon Rosenthal, Edward Sciore; "Administering Propagated Metadata in Large, Multi-Layer Database Systems", *IEEE Workshop on Knowledge and Data Exchange*, 1999
14. Sos Agaian, Benjamin Rodriguez; "Steganographic Capacity used for Steganalysis Cluster Classification" Gsteg Pacific Rim Workshop on Digital Steganography, November 2004
15. Sos Agaian, Juan Perez; "New Pixel Sorting Method for Palette Steganography and Steganographic Capacity Measure", Gsteg Pacific Rim Workshop on Digital Steganography, November 2004

Biographies

Sos S. Agaian is Full Professor, College of Engineering, The University of Texas at San Antonio and an Adjunct Professor in the Dept. of Electrical Engineering, Tufts Univ., Medford, Massachusetts. He has authored more than 275 scientific papers, three books, and holds 13 patents. He is an associate editor of the Journal of Real-Time Imaging, the Journal of Electronic Imaging, and an editorial board member of the Journal Pattern Recognition and Image Analysis. His current research interests lie in the broad area of Signal/image processing and transmission, Information security, and Quantum signal processing, and communication.

Okan Caglayan holds a Bachelor's degree in Electrical Engineering from the University of Texas at San Antonio and is currently pursuing Master's degree in Electrical Engineering at Univ. of Texas at San Antonio. He is currently affiliated with the Nonlinear Signal Processing laboratory research team. His research is in the areas of digital signal/image and video processing with hardware implementations, fast algorithms, steganography and steganalysis.