International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Improving Security for Digital Signature by Using Steganography

G. Pranitha[1], Ch. Suman Chakravarthy[2]

[1]Anil Neerukonda Institute of Technology and Sciences, Visakhapatnam

[2]Praveenya Institute of Marine Engineering and Maritime Studies

Abstract: ***In this paper, we enhance the security for the data by hiding the message using steganographic technique. Initially the given message is taken as input and we generate digital signature using MD5 algorithm. After generating the signature we conceal the given message using steganography .Now, the message which is hidden along with the digital signature is sent to the receiver.The receiver applies the steganographic technique to retrieve the message and then verifies the digital signature.***

Keywords: Encryption, MD5, image steganography, digital signature

1. Introduction

In today's data-centric world, much emphasis is placed on the security of information Every user has to know the importance of security .For example, in defence field like army security of data is a key aspect. Some of the important concepts in security are authentication and integrity of the data. Authentication is the process which allows a sender and receiver of information to validate and verify each other. When authentication is not performed properly then we cannot guarantee the communication which is performed is genuine. Integrity is the property which assures that modification is not performed on the data that is sent from source to destination.

2. Digital Signature

Signature verification is one of the techniques which is used by banks, intelligence agencies and high-profile institutions to validate the identity of an individual. Signature verification is used to match signatures in bank offices in order to find the identity. A digital signature is one a way to ensure that an electronic document such as e-mail, spreadsheet, text file, etc is authentic. Authentic means we are sure of the user who created it.

The digital equivalent of a hand written signature on a paper or a stamped document is equivalent to the digital signature concept. We have many algorithms to implement the concept of digital signature .A message digest is a cryptographic hash function containing a string of digits created by a one-way hashing formula.

Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message .In this paper we use, MD5 algorithm for generation.MD5 is a Message Digest algorithm that is a hash technique, which will produce 128-bit hash value .We need to convert the input data into bytes in order to convert it to hash value.

Digital signatures are based on public key cryptography which is known as asymmetric cryptography. Using a public key algorithm, RSA, one can generate two keys that are mathematically linked: one private and one public. The software application creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash value and other information like the hashing algorithm will form the digital signature. The reason for encrypting the hash value instead of the entire message or document is that a hash function has the capability to convert an arbitrary input into a fixed length value, which is usually much shorter.

The value of the hash is unique to the hashed data. If we change the data at least single character, will result in different result. This feature enables to validate the integrity of the data by using the signer's public key to decrypt the hash value. If the decrypted hash value matches a second calculated hash of the same data, it proves that the data was not changed since it was signed. If the two hashes don't match with each other, then we can assure that the data is being modified somewhere in the middle.

A digital signature can be used with any kind of message; whether it is encrypted or not, simply so the receiver can be sure of the sender's identity and that the message arrived will be genuine. Digital signatures make it difficult for the signer to deny that they have signed something which is termed as non-repudiation.

3. Algorithm

Message-Digest (Fingerprint) algorithms are special functions which transform input of arbitrary length into output of constant length which is called as message digest.. These conversion functions must satisfy the given requirements: no one should be able to produce two different inputs for which the transformation function returns the same output.MD5 algorithm takes input message of arbitrary length and generates 128-bit output hash value.

MD5 hash algorithm consists of 5 steps.

Step 1. Append Padding Bits
Step 2. Append Length
Step 3. Initialize MD Buffer
Step 4. Process Message in 16-Word Blocks
Step 5. Output

MD5 takes the input of a variable-length message and converts into a fixed-length output which will be of 128 bits. The input message is broken up to give chunks of 512-bit. The message is padded so that its length is divisible by 512.It should be multiple of 512 .The padding will be done as follows: first a single bit 1 is appended to the end of the message. This is followed by appending as many zeros as required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are used to hold the value of length of the original message.

The MD5 algorithm operates on a 128-bit block, which are divided into four 32-bit words that are denoted by constants *A*, *B*, *C*, and *D*. These are initialized with certain fixed constants which are hexadecimal values. The algorithm uses each 512-bit message block to modify the state. The processing of a message block consists of four similar stages called as rounds. Each round is composed of 16 similar operations based on a non-linear function *F*, modular addition, and left rotation.

The four-word buffer (A, B,C,D) is used to calculate the message digest from given message. Here each of A, B, C, D is a 32-bit register. These registers are initialized to the following values in hexadecimal form, low-order bytes first. The values are given below.

Word A: 01 23 45 67
Word B: 89 ab cd ef
Word C: fe dc ba 98
Word D: 76 54 32 10

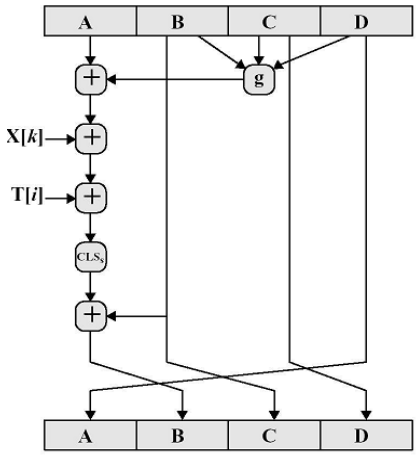

Figure 1

Figure1 illustrates one operation within a round. There are four functions *g* where different one is used in each round. We define four auxiliary functions where each one take as input three 32-bit words and produce as output one 32-bit word.

F(X, Y, Z) = XY v not(X) Z
G(X, Y, Z) = XZ v Y not (Z)
H(X, Y, Z) = X xor Y xor Z
I(X, Y, Z) = Y xor (X v not(Z))

It also uses a 64-element table T[1 ... 64] constructed from the sine function. Let T[i] will indicate the i-th element of the table, which is equal to the integer part of 4294967296 times abs(sin(i)), where i is in radians. The message digest produced as output is A, B, C, D. we begin with the low-order byte of A and end with the high-order byte of D.

4. Steganography

A. **Techniques of steganography**

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The following formula provides a very generic description of the pieces of the steganographic process:

cover medium + hidden data + stego_key = stego_medium

In this context, the cover_medium is the file in which we will hide the hidden data, which may also be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium). The cover_medium (and, thus, the stego_medium) are typically image or audio files. In this article, I will focus on image files and will, therefore, refer to the cover_image and stego_image.

There are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement.

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography.

Steganography is of four types.Text Steganography; image Steganography, audio Steganography, video Steganography.
Image Steganography

Using image files as hosts for steganographic messages takes advantage of the limited capabilities of the human visual system. Some of the more common method for embedding messages in image files can be categorized into two main groups, image domain methods and transform domain methods

B.LSB [Least Significant bit] Method

A digital image is described using a 2-D matrix of the colour intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the colour model, such as RGB model. The Steganography sys-tem which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques make the changes in the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.

The LSB is the lowest significant bit in the byte value of the image pixel.

The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image (CVR).

Least significant bit (LSB) insertion is a simple approach to embed the information in a cover image to provide security. The least significant bit that is the 8th bit of some or all of the bytes inside an image is changed to a bit of the secret message¨ When using a 24-bit image, a bit of each of the red, green and blue colour components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data¨ In its simplest form, LSB makes use of BMP images, since they use lossless compression

The simplest approach to hiding data within an image file is called least significant bit (LSB) insertion. In this method, we can take the binary representation of the hidden data and overwrite the LSB of each byte within the cover_image. If we are using 24-bit colour, the amount of change will be minimal and indiscernible to the human eye. As an example, suppose that we have three adjacent pixels (nine bytes) with the following RGB encoding:
10010101 00001101 11001001
10010110 00001111 11001010
10011111 00010000 11001011
Now suppose we want to "hide" the following 9 bits of data (the hidden data is usually compressed prior to being hidden): 101101101. If we overlay these 9 bits over the LSB of the 9 bytes above, we get the following (where bits in bold have been changed):

10010101 00001100 11001001
10010111 00001110 11001011
10011111 00010000 11001011
Note that we have successfully hidden 9 bits but at a cost of only changing 4, or roughly 50%, of the LSBs.

5. Architecture

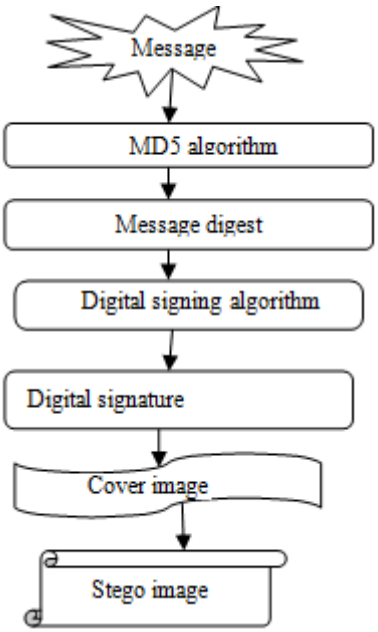

Figure 2

6. Procedure

In figure2 we can see the architecture of entire system. We apply cryptography to authenticate the user and check the integrity of the message and apply steganography to hide the message under transmission. The message is taken as input and the digital signature is generated using the MD-5 algorithm. The output that is produced is embedded under the cover image using image steganography..In this paper we use the LSB image steganography technique to perform the hiding of data. The result image which is generated is sent to the receiver.

The receiver receives the cover which contains the digital signature along with the message. Now, as both of them had already decided ,receiver extracts the message and digital signature from cover image. Then the receiver verifies the signature generated by performing the decryption using the public key of sender and authenticates the sender as well as checks the integrity of the data.

7. Conclusion

In this paper we have seen how to enhance the security for the digital signature that is generated using the MD5 algorithm. We have used the simple steganographic technique of LSB method to hide the data and digital signature. This algorithm would obscure the data. We can even extend this work by using more complex algorithms which would yield more security.

References

[1] N Akhtar, P Johri, S Khan ,**Enhancing the security and quality of LSB based image steganography**-Computational Intelligence and …, 2013 - ieeexplore.ieee.org
[2] RL Rivest, A Shamir, L Adleman, **A method for obtaining digital signatures and public-key cryptosystems**, Communications of the ACM, 1978 - dl.acm.org
[3] YJ Chanu, KM Singh, T Tuithung - **Image steganography and steganalysis**: A survey-International Journal of Computer science and research
[4] K Kant, F Iqbal, MI Alam,-**Digital Signature and Key Agreement,** International Journal of Science Engineering and Advance Technology,
[5] Min Wu, Member, IEEE, and Bede Liu, Fellow, IEEE, **Data Hiding in Binary Image for Authentication and Annotation**-IEEE TRANSACTIONS ON MULTIMEDIA, VOL. 6, NO. 4, AUGUST 2004
[6] R Ramachandaran, AES Vasagam- **DATA SECURITY USING APPLICATION HIDING CRYPTOSYSTEM AND STEGANOGRAPHY**-International journal of engineering researchand science and technology 2015 - ijerst.com

Author Profile

G. Pranitha is currently working as Assistant Professor, in Department of Computer Science and Engineering at Anil

Neerukonda Institute of Technology & Sciences, Bheemunipatnam (Municipality), Sangivalasa, Visakhapatnam. Her research interests include Networks Security & Information Security.

Ch. Suman chakravarthy is currently working as Assistant Professor, in Department of Computer Science and Engineering at Praveenya Institute of Marine Engineering and Maritime Studies, Vizianagaram. His research interests include Networks Security & Information Security and Computer Networks.