ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

PREVENTION OF WATERMARKING ATTACKS USING CRYPTOGRAPHY METHOD

S. S. Sudha[1] , K. K. Rahini [2]

Assistant Professor, Department of Computer Science, PSG College of Arts & Science, Coimbatore, India[1]

Research Scholar, Department of Computer Science, PSG College of Arts & Science, Coimbatore, India[2]

Abstract: As the need for information over network is high the security for such information is necessary when the information is shared over network or retrieved from network. Media files which are shared in networking sites and other areas must be highly protected to prevent files from hackers. Watermarking is a prevention technique used for preventing media files like images, audio & video files etc. The paper shows the detailed information about providing authentication or security for media data which are shared over internet. This research provides the information about the file encryption using AES algorithm and watermarking using DCT Algorithm. The image is taken for testing and the study shows the idea of using combination of cryptographic algorithm and watermarking algorithm in securing media informations. The image is encrypted and then the enciphered or encrypted image embedded into cover file and finally covered image is watermarked. The result of the process is watermarked image.

Keywords: Watermarking, Types of Watermarking, Digital Watermarking, Watermarking Attacks, Discrete Cosine Transform technique (DCT), AES Algorithm and its operations.

I. INTRODUCTION

Digital watermarking is one of the best solutions to prevent illegal copying, modifying and redistributing multimedia data. Encryption of multimedia products prevents an intruder from accessing the contents without a proper decryption key. But once the data is decrypted, it can be duplicated and distributed illegally. Copyright protection, data authentication, covert communication and content identification can be achieved by digital watermarking. Digital watermarking is a technique to embed copyright or other information into the underlying data. The embedded data should maintain the quality of the host signal. A digital watermark is a pattern of bits inserted into a digital image, audio and video file that identifies the file's copyright information. The bits representing the watermark must be scattered throughout the file in such a way that they cannot be identified and manipulated.

And finally, a digital watermark must be robust enough to survive changes to the file its embedded in, such as being saved using a lossy compression algorithm e.g.: JPEG. Watermarking techniques is to provide a proof of ownership of digital data by embedding copyright statements into a video or into a digital image. Watermarking bring a variety of techniques how to hide important information, in an undetectable and/or irremovable way, in an image audio and video data. Watermarking are main parts of the fast developing area of information hiding**.**

Watermarking is a totally different technique from cryptography. Cryptography only provides security by encryption and decryption. Unlike Cryptography, watermarks can protect content even after they are decoded. Digital watermarking has received considerable attention as a complement to cryptography for the protection of digital content such as music, video, and images. Cryptography provides a means for secure delivery of content to the consumer. Legitimate consumers are explicitly or implicitly provided with a key to decrypt the content in order to view or listen to it.

The original image is given to AES algorithm for encryption. AES, using 128 bit key it encrypts the original image and gives the output as enciphered image for watermarking. The algorithm takes 10 rounds for such encryption process. The output of AES that is enciphered image is then embedded into cover image. Again the embedded image is watermarked using DCT algorithm with its blocks. Finally the process produces the watermarked image as a result at sender side.

Fig 1: Process of Encryption using AES Algorithm

Fig 2: Process of Watermarking using DCT Algorithm

II. TYPES OF WATERMARKS

The watermarking techniques are of two types. They are as follows:

A) VISIBLE WATERMARK

The visible watermarks are viewable to the normal eye such as bills, company and television channel logos, etc. In visible watermarking, Watermark perceptibility is visibly meaningful pattern and the nature of robustness is user-intervention based watermark removal. The protection in visible watermarking is active and the extraction is by direct viewing.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014


B) INVISIBLE WATERMARKING

In the case of invisible watermarking, the locations in which the watermark is embedded are secret, and then only authorized persons extract the watermark. In invisible watermarking, intentional attacks and common signal processing is robustness in nature. The protection in invisible watermarking is passive and the extraction is in explicit module. Information is added as digital data to audio, picture or video, but it cannot be perceived because it may be in a form of Steganography.

III. DIGITAL WATERMARKING APPLICATIONS

A) Ownership Assertion

Watermarking is used to detect the actual owner of a digital content. 'A' uses a private key to generate a watermark and embeds it**.** 'A' makes the watermarked images publicly available**.** 'B' claims that he owns the images derived from the public image. 'A' produces the unmarked original image and establishes the presence of 'A's watermark.

B) Fingerprinting

It is used to avoid unauthorized duplication and distribution. A distinct watermark (a fingerprint) is embedded in each copy of data. If the unauthorized copies are found, origin of the copy can be determined by retrieving the fingerprint.

C) Authentication & Integrity verification

Watermarks should be able to detect even the slightest change in the document. A unique key is associated with the source and it is used to create the watermark and then embed in the document. This key is used to extract the watermark and the integrity of the document verified on the basis of the integrity of the watermark.

D) Content labeling

Bits embedded in the data, comprise an annotation, by giving some more information about the data. Digital cameras annotate images with the time and date, when the photographs were taken. Medical imaging machines annotate images (X-Rays) with patient name, ID.

E) Usage control & Copy protection

Digital watermark inserted to indicate the number of copies permitted. Every time a copy is made, hardware modifies the watermark and at the same time it would not create any more copies of the data. It is commonly used in DVD technology.

F) Content Protection

Content owner might want to publicly and freely provide a preview of multimedia content is to being sold. To make the preview commercially useless, content is being stamped with visible watermarks.

IV. WATERMARKING ATTACKS

By using watermarking alone for file safeguard will not be a best solution for attacking problems. It can be hacked by the attacker. If the file is encrypted before watermarking using cryptographic technique then it is tough for hacker to gain the file and use. The file which is encrypted by the sender can be decrypted by the receiver by sharing the keys used by the sender. One categorization of the wide class of existing attacks contains four classes of attacks: removal attacks, geometric attacks, cryptographic attacks, and protocol attacks.

A) Removal attacks

Removal attacks aims at the complete removal of the watermark information from the watermarked data without cracking the security of the watermarking algorithm, e.g., without the key used for watermark embedding. That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data.

B) Geometric attacks

In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark itself, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained.

C) Cryptographic attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks. One such technique is the brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a non-watermarked signal when a watermark detector device is available.

D) Protocol attacks

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks. The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data. It has been shown that for copyright protection applications, watermarks need to be non-invertible.

Another protocol attack is the copy attack. In this case, the goal is not to destroy the watermark or impair its

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. The copy attack is applicable when a valid watermark in the target data can be produced with neither algorithmic knowledge of the watermarking technology nor the knowledge of the watermarking key. Again, signal-dependent watermarks might be resistant against the copy attack.

V. WATERMARKING USING DCT

Discrete Cosine Transform technique (DCT)

The discrete cosine transforms (DCT) are mathematical function that transforms digital image data from the spatial to the frequency domain. In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components and is specified for lossy compression. DCT coefficients are used for JPEG compression. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components. In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band, so that the visibility of the image will not be affected. The general equation for a 1D (N data items) DCT is defined by the following equation:

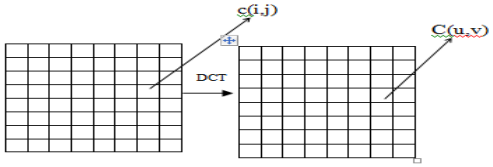

Fig 3: Discrete Cosine Transform of an Image

$$C(u) = a(u) \sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where u= 0, 1, 2….. N-1

The general equation for a 2D (*N* by *M* image) DCT is defined by the following equation:

$$C(u,v) = a(v) \sum_{i=0}^{N-1} [a(u) \sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)] \times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

Where u, v = 0,1,2….N-1. Here, the input image is of size N X M. c (i, j) is the intensity of the pixel in row i and column j; C(u,v) is the DCT coefficient in row u and column v of the DCT matrix.

DCT is used in steganography. Image is broken into 8×8 blocks of pixels. Working from left to right, top to bottom, DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

VI. AES ALGORITHM

(Advanced Encryption Standard)

The advanced Encryption Standard (AES) is an Encryption algorithm for securing sensitive data established by U.S National Institute of Standards and Technology (NIST) in January of 1997. This technique is developed by the Belgian cryptographers Joan Daemen and Vincent Tijmen.

The algorithm described by AES is a Symmetric-Key algorithm, which is the same key is used for both encrypting and decrypting the data. AES is an iterated block cipher with a fixed block size of 128 and a variable key length. The different transformations operate on the intermediate results, called states.

AES uses a variable number of rounds, which are fixed:

- A key of size 128 has 10 rounds.
- A key of size 192 has 12 rounds.
- A key of size 256 has 14 rounds.

During each round, the following operations are applied on the state.

- *SubBytes:* Every byte in the state is replaced by another one, using the Rijndael S-Box.
- *ShiftRow:* Every row in the 4×4 array is shifted a certain amount to the left.
- *MixColumn:* A linear transformation on the columns of the state.
- *AddRoundKey:* Each byte of the state is combined with a round key, which is a different key for each round and derived from the Rijndael key schedule.

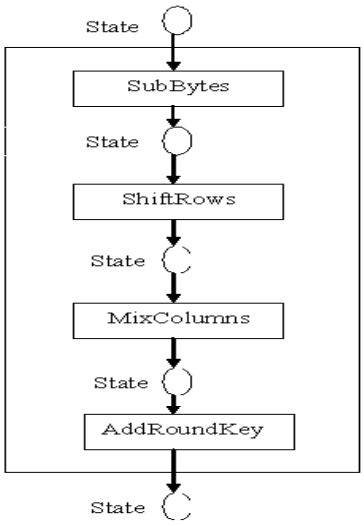

Fig 4: Structure of each round at the encryption side.

AES Operations:

1) SubBytes Operation:

The SubBytes operation is a non-linear byte substitution, operating on each byte of the state independently. The substitution table(S-Box) is invertible and is constructed by the composition of two transformations:

- Taking the multiplicative inverse in Rijndael's finite field.
- Then applying an affine transformation which is documented in the Rijndael documentation.

Since the S-Box is independent of any input, pre-calculated forms are used, if enough memory (256 bytes for one S-Box) is available. Each byte of the state is then substituted by the value in the S-Box whose index corresponds to the value in the state

a (i, j) = SBox [a (i,j)]

1) ShiftRow Operation:

In this operation, each row of the state in cyclically shifted to the left, depending on the row index.

- The first row is shifted 0 positions to the left.
- The second row is shifted 1 position to the left.
- The third row is shifted 2 positions to the left.
- The fourth row is shifted 3 positions to the left.

2) MicxColumns Operation:

The MixColumns transformation operates at the column level it transforms each column of the state to a new column. The four bytes of each column of the state are combined using an invertible linear transformation.

3) The AddRoundKey Operation:

In this operation, a Round key is applied to the state by a simple bitwise XOR. The Round Key is derived from the Cipher key by the means of the key schedule. The Round Key length is equal to the block key length (=16 bytes.)

VII. CONCLUSION

Thus the paper contains the information about the watermarking and the applications used in watermarking. It shows the detailed expansion about watermarking, its techniques, attacks and types of attacks in watermarking. Related work focuses on watermarking using DCT Algorithm and encryption using AES cryptographic algorithm.

REFERENCES

[1] S. Voloshynovskiy, S. Pereira, T. Pun, J.J. Eggers and J.K. Su, "Attacks on Digital Watermarks: Classification, Estimation-based Attacks and Benchmarks".
[2] Stuti Goel, Arun Rana, Manpreet Kaur, "Comparison of Image Steganography Techniques" International Journal of Computers and Distributed Systems www.ijcdsonline.com Vol. No.3, Issue I, April-May 2013.
[3] Doug Tygar, "Watermarking and its types".
[4] A.Joseph Raphael,Dr.V Sundaram, "Cryptography and Steganography – A Survey", ISSN:2229-6093, Int. J. Comp. Tech. Appl., Vol 2 (3), 626-630.
[5] Parameshachari B D, K M Sunjiv Soyjaudah, Chaitanyakumar M V, "A Study on Different Techniques for Security of an Image", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-6, January 2013.
[6] Ahmed H. Omari, Basil M. Al-Kasasbeh, Rafa E. Al-Qutaish, Mohammad I. Muhairat, "A New Cryptographic Algorithm for the Real Time Applications", 7th WSEAS International Conference on Information Security and Privacy (ISP '08).
[7] Douglas Selent, "Advanced Encryption Standard", Rivier Academic Journal, Vol 6, Number 2, Fall 2010.

BIOGRAPHIES

Mrs. S. S. Sudha received her M.Sc., (Computer Science) degree from Madurai Kamarajar University, and M.Phil., degree in Computer Science from Madurai Kamarajar University. She has Presented Papers in National Conferences. She has 6 and a Half years of Teaching Experience and she is currently working in PSG College of Arts & Science, Coimbatore. Her Research interests include Digital Watermarking and Image Data Hiding.

K. K. Rahini received her B.Sc., (Computer Science) degree in 2011, M.Sc., (Computer Science) in 2013 from Bharathiar University, Coimbatore. At present she is pursuing her M.Phil (Computer Science) at PSG College of Arts & Science, Coimbatore. She has presented papers in National Conferences. Her research interest is Digital Image Processing.