ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Verifying the Reliability of Images with a Joint Encryption and Watermarking System

R.Harika
M.Tech Student
Department of ECE,
TPIST, Komatipalli, Bobbili,
Andhra Pradesh, India.

K.Kranthi Kumar
Assistant Professor
Department of ECE,
TPIST, Komatipalli, Bobbili,
Andhra Pradesh, India.

Abstract

Multimedia and communication technologies offer new means of sharing and remote access to data. In any information systems data confidentiality, authentication, integrity and non repudiation services are usually required. Here a joint encryption and watermarking system is used for the purpose of protecting images. It merges a chaotic mapping, an encryption algorithm which is a block cipher algorithm (e.g., AES) and substitutive blind and non-blind watermarking algorithms based on DWT & DCT.

This paper consists of dual encryption and dual watermark system, watermark embedding process consists of two stages. In first stage original watermark will be encrypted by using chaotic maps, after that the original image and encrypted output will be given as inputs to blind watermarking algorithm. In second stage the first stage output will be encrypted by using AES encryption and then the encrypted image and one false watermark will be given as inputs to non-blind watermarking algorithm.

Finally the watermarked image is decrypted version of non-blind algorithm output i.e. encrypted and watermarked image. Similarly watermark detection process also consists of two stages. Here the watermarked image is to be encrypted first and then in first stage the non-blind extraction algorithm is used for getting encrypted image, it is to be decrypted by using AES decryption. In second stage the watermark is to be extracted by using blind watermark extraction algorithm and finally extracted image is to be decrypted by chaotic decryption for getting original watermark.

Introduction

In the past several years there has been an explosive growth in digital imaging technology and applications. With this growth Digital images and video are now widely distributed on the Internet and via CD-ROM. Digital data, such as digital audio, images, and video, can be stored, copied, and distributed quickly, easily, and without any loss of fidelity. The success of the Internet, cost-effective and popular digital recording and storage devices, and the promise of higher bandwidth and quality of service for both wired and wireless networks have made it possible to create, replicate, transmit, and distribute digital content in an effortless way. This frequent use of the Internet has created a need for security. One problem with a digital image is that an unlimited number of copies of an "original" can be easily distributed and/or forged. This presents problems if the image is copyrighted. The protection and enforcement of intellectual property rights has become an important issue in the "digital world." As a consequence, to prevent information which belongs to rightful owners from being intentionally or unwittingly used by others, information protection is indispensable.

In the early days, encryption and control access techniques were employed to protect the ownership of media. However, to protect against unauthorized

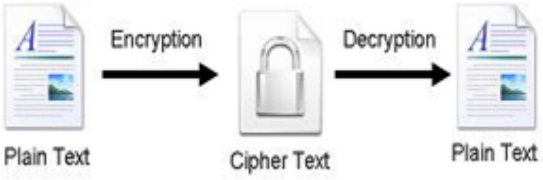
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

copying after the media have been successfully transmitted and decrypted, recently the watermarking techniques are utilized, because watermarking algorithms embed the watermark into digital data and the unauthorized copying can be prevented by using these watermark. In this project, a joint encryption and watermarking system is used for protecting and verifying the reliability of images.

Types of Watermarks

Encryption in Communications

Encryption is the process of converting a plaintext message into cipher text, which can be decoded back into the original message as shown in below. An encryption algorithm along with a key is used in the encryption and decryption of data. There are several types of data encryptions, which form the basis of network security. Encryption schemes are based on block or stream ciphers.



The type and length of the keys utilized depend upon the encryption algorithm and the amount of security needed. In conventional symmetric encryption a single key is used. With this key, the sender can encrypt a message and a recipient can decrypt the message but the security of the key becomes problematic. In asymmetric encryption, the encryption key and the decryption key are different. One is a public key by which the sender can encrypt the message and the other is a private key by which a recipient can decrypt the message. Algorithms play a significant role in ensuring the integrity of data. They provide necessary security when communications occur over insecure platforms, such as communications that involve the internet or outside network.

Encryption---terminology

The main purpose of encryption algorithms is to provide the following:

1. Authentication: Proving one's identity before granting access.
2. Confidentiality: Ensuring that outsiders cannot read data intended for specific parties.
3. Integrity: Ensuring that the message has not been modified in any way before it arrives the intended recipient.
4. Non-repudiation: Ensuring that the message is truly originated from sender.

A conventional encryption scheme has five major parts:

Plaintext - this is the text message to which an algorithm is applied.

Encryption Algorithm- it performs mathematical operations to conduct substitutions and transformations to the plaintext.

Secret Key - This is the input for the algorithm as the key dictates the encrypted outcome.

Cipher text - This is the encrypted or scrambled message produced by applying the algorithm to the plaintext message using the secret key.

Decryption Algorithm-This is the encryption algorithm in reverse. It uses the cipher text, and the secret key to derive the plaintext message.

When using this form of encryption, it is essential that the sender and receiver have away to exchange secret keys in a secure manner. If someone knows the secret key and can figure out the algorithm, communications will be insecure. There is also the need for a strong encryption algorithm. What this means is that if

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

someone were to have a cipher text and a corresponding plaintext message, they would be unable to determine the encryption algorithm.

As key lengths increase, the number of combinations that must be tried for a brute force attack increase exponentially. For example a 128-bit key would have 2^128 (3.402823669209e+38) total possible combinations

AES Encryption Algorithm

In cryptography, the Advanced Encryption Standard (AES) is an encryption standard Adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael.

AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. Assuming one byte equals 8 bits, the fixed block size of 128 bits is 128 ÷ 8 = 16 bytes. AES operates on a 4×4 array of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES

Final Round—

1)Sub bytes 2) Shift Rows 3) Add Round Key.

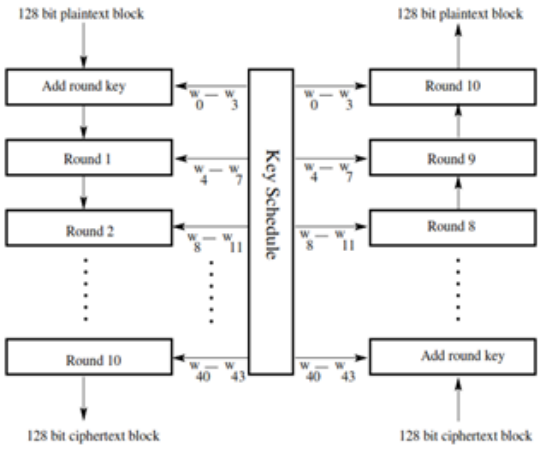
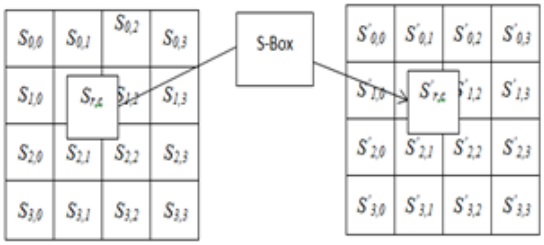


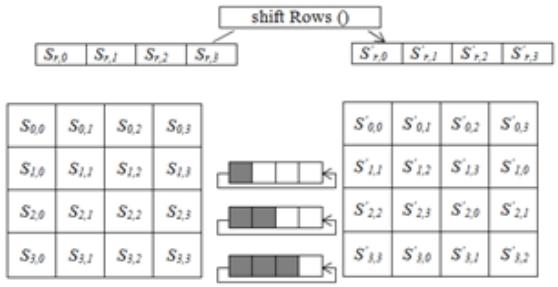
Diagram of AES encryption and decryption

The Sub Bytes step

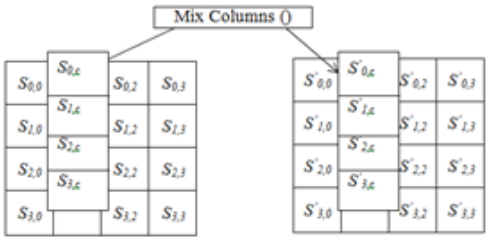
In the Sub Bytes step, each byte in the array is updated using an 8-bit Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF(28), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), and also any opposite fixed points.



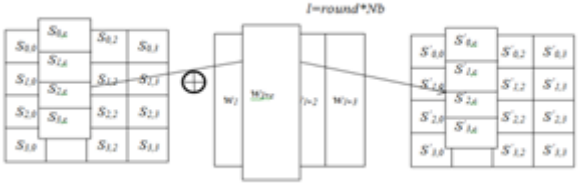
Step 2



Step 3



Step4



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Results:

Input image

Input water mark image

Chaotic encryption output

Blind watermarking output

Original watermark to be extracted

Conclusion

In this paper, a new joint watermarking and encryption system is proposed, which guarantees *a priori and a posteriori protection* of images. It merges a chaotic mapping, an encryption algorithm which is a block cipher algorithm (e.g., AES) and substitutive blind and non-blind watermarking algorithms based on DWT & DCT. Experimental results show that the image distortion is very low and that the achieved capacity is enough to embed a reliability proof as well as some other data.

Future Scope

Future works will focus on making our scheme more robust to attacks like lossy image compression (e.g., JPEG) and reducing the complexity of our algorithm. This scheme can be enhanced by combining with video watermarks. This project can also be extended by applying the scheme to specific environments or applications and examine its effectiveness.

References

[1] "A Joint Encryption/Watermarking System for Verifying the Reliability of Medical Images" Dalel Bouslimi, Member, IEEE, Gouenou Coatrieux, Member, IEEE, MichelCozic,-IEEE VOL. 16, NO. 5, SEPTEMBER 2012.

[2] Applications of toral automorphisms in image watermarking" G.Voyatzis and I.Pitas

[3] A Robust Digital Watermarking with Mixed Transform Technique for Digital Image"Chien-Pen Chuang , Cheng-Hung Liu , Yi-Tsai Liao , Huan-Wei Chi – Proceedings of the International multiConference of Engineers and Computer scientists 2012 vol I IMECS 2012 march 14-16 Hong Kong

[4] G. Caronni, "Assuring Ownership Rights for Digital Images". In H.H. Brueggemann and W. Gerhardt-Haeckl, editors, Reliable IT systems VIS 1995. Vieweg Publishing Company, Germany, 19956

[5] Jae S. Lim "Two dimensional Signal and Image Processing". Prentice-Hall International, 1990

[6] A.Z Tirkel, R.G. van Schyndel, and C.F. Osborne. "A two-dimensional digital watermark. In ACCV, Singapore, 1995.

[7] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," Proceedings of the IEEE, vol. 86, no. 6, pp. 1064–1087, 1998.