QUALITY ACCESS CONTROL OF IMAGE BY ENCRYPTION & DATA HIDING

Prof. Smita Desai(Guide)¹, Yashoda Tangadpalle², Trupti Pavshere³ Bhagyashri Kale⁴

Pad. Dr. D. Y. Patil Institute of Engineering & Technology, Pimpri, Pune-18

smita_rdesai@yahoo.co.in, yashodatangadpalle@gmail.com, trupti.pavshere@gmail.com, bkale2418@gmail.com

ABSTRACT- As the use digital techniques for transmitting and storing images are increasing; it is becoming an important issue how to protect the confidentiality, integrity and authenticity of images. This study paper extends to the performance parameters used in encryption processes and analyzing on their security issues which have been developed and are in practice today.

KEYWORDS- Digital rights management(DRM), Quality Of Services(QOS)

INTRODUCTION

With the availability of Internet and high quality scanner, digital images can be distributed and pirated easily without honoring the right of individuals. To alleviate this problem, digital rights management(DRM) systems rely on cryptography and watermarking in variety of ways [1]. One example is quality access control of images that allows all the receivers of the broadcast channel to display a low quality image with no or little commercial value. But at the same time, the scheme also enables authorized users to access the image at higher quality levels. Quality depends on each receiver’s access rights and is determined by the subscription agreement. This requirement arises as the manufacturers and the vendors have always two different objectives in their mind. They need to place their large volume of valuable works in the website for wide publicity and at the same time they like to restrict full quality access to the general users in order to maintain their commercial benefits. Access control may found an important application in future generation mobile communication system where billing is expected to be performed based on the fulfillment of degree of quality of services (QOS).

The combination of data hiding and encryption method are used in this paper for quality access control of digital image (s). The secret key is encrypted by public key encryption and is embedded in the cover image as a watermark using QIM. This principle reduces the risk of losing the information of the secret key during transmission through the channel corrupted by noise. Experimental results show that valid users having the full knowledge of the key enable to avail the ultimate quality of an image, and to disallow unauthorized users to avail the same with satisfactory quality. The results also show that even the channel is noisy the scheme extracts the decoding key correctly and avail better
quality of image. The scheme is simple, cost effective, secured, easy to implement. All these characteristics make the scheme a possible solution for digital rights management (DMR). Future work may be carried out to extend the proposed method for access control of color images, video and sound data.

BACKGROUND

Encryption, is the process of converting messages, information, or data into a form unreadable by anyone except the intended recipient. Encrypted data must be deciphered, or decrypted, before it can be read by the recipient. The root of the word encryption—crypt—comes from the Greek word kryptos, meaning hidden or secret. In its earliest form, people have been attempting to conceal certain information that they wanted to keep to their own possession by substituting parts of the information with symbols, numbers and pictures.

IMAGE ENCRYPTION

Fig. Block diagram.

General cryptography and encryption A technique in which secret messages are transferred from one person to another over the communication line called cryptography. The technique(s) used to convert the original data into secret code or data is called data encryption technique for all kinds of data such as textual data, Image data or multimedia data for secured communication over a network. In this paper we focus on Image encryption which has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication; etc. Images encryption is different from the simple data encryption. So in general the data hiding in image involves four steps. a. Selection of the secret media where the data will be hidden. b. The undisclosed message or information that is needed to be masked in the cover image. c. A function that will be used to hide the data in the cover media and its inverse to retrieve the hidden data. d. An optional key or the password to authenticate or to hide and unhide the data.

Based on above encryption standard a process of Non separable reversible data hiding in encrypted image is as shown in Fig.1.where A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. In the scheme, the data extraction is not separable from the content.

Now a days when more and more sensitive information is stored on computers and transmitted over the Internet for which security and safety of information need to be ensured as image is also an important part of that sensitive data. Therefore it’s very important to protect these images from legitimate users. There are many novel reversible data hiding scheme for encrypted image available which are made up of image encryption, data embedding and data-extraction/image-recovery phases. In which the
data of original cover are entirely encrypted and the additional message is embedded by modifying a part of encrypted data. At receiver side, with the aid of spatial correlation in natural image, the embedded data are successfully extracted while the original image is perfectly recovered.

RELATED WORK

1. Public-Key Cryptography:-
   - probably most significant advance in the 3000 year history of cryptography.
   - uses two keys – a public & a private key.
   - asymmetric since parties are not equal.
   - uses clever application of number theoretic concepts to function
   - complements rather than replaces private key crypto.
   - public-key/two-key/asymmetric cryptography involves the use of two keys:
     - a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures.
     - a private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures.
   - is asymmetric because.
   - those who encrypt messages or verify signatures cannot decrypt messages or create signatures.

Why Public-Key Cryptography?

   - developed to address two key issues:
     - key distribution – how to have secure communications in general without having to trust a KDC with your key.
     - digital signatures – how to verify a message comes intact from the claimed sender.

   - Public-Key Characteristics :-
     - Public-Key algorithms rely on two keys with the characteristics that it is:
     - computationally infeasible to find decryption key knowing only algorithm & encryption key.
     - computationally easy to en/decrypt messages when the relevant (en/decrypt) key is known.
     - either of the two related keys can be used for encryption, with the other used for decryption (in some schemes).

2. Private-Key Cryptography:
   1. traditional private/secret/ single key cryptography uses one key.
   2. shared by both sender and receiver.
   3. if this key is disclosed communications are compromised.
   4. also is symmetric, parties are equal.
   5. hence does not protect sender from receiver forging a message & claiming is sent by sender.

RSA ALGORITHM:-
1 Introduction

This algorithm is based on the difficulty of factorizing large numbers that have 2 and only 2 factors (Prime numbers). The system works on a public and private key system. The public key is made available to everyone. With this key a user can encrypt data but cannot decrypt it, the only person who can decrypt it is the one who possesses the private key. It is theoretically possible but extremely difficult to generate the private key from the public key, this makes the RSA algorithm a very popular choice in data encryption.
1.1 Algorithm
First of all, two large distinct prime numbers p and q must be generated. The product of these, we call n is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it - 512 bits at least i.e. numbers greater than 10154. We then generate the encryption key e which must be co-prime to the number m = \'(n) = (p - 1)(q - 1). We then create the decryption key d such that de \equiv 1 \pmod{m} = 1. We now have both the public and private keys.

1.2 Encryption

We let y = E(x) be the encryption function where x is an integer and y is the encrypted form of x

\[ y = xe \mod n \]

1.3 Decryption:
We let X = D(y) be the decryption function where y is an encrypted integer and X is the decrypted form of y

\[ X = yd \mod n \]

3. RSA Algorithm Example:-
· Choose p = 3 and q = 11
· Compute n = p \times q = 3 \times 11 = 33
· Compute \( \varphi(n) = (p - 1)(q - 1) = 2 \times 10 = 20 \)
· Choose e such that 1 < e < \( \varphi(n) \) and e and n are co-prime. Let e = 7
· Compute a value for d such that \( (d \times e) \mod \varphi(n) = 1 \). One solution is d = 3 \[ (3 \times 7) \mod 20 = 1 \]
· Public key is (e, n) = (7, 33)
· Private key is (d, n) = (3, 33)
· The encryption of m = 2 is c = 27 \% 33 = 29
· The decryption of c = 29 is m = 293 \% 33 = 2

RESULT

The combination of data hiding and encryption method are used in this paper for quality access control of digital image(s). The secret key is encrypted by public key encryption and is embedded in the cover image as a watermark using QIM. This principle reduces the risk of losing the information of the secret key during transmission through the channel corrupted by noise. Experimental results show that valid users having the full knowledge of the key enable to avail the ultimate quality of an image, and to disallow unauthorized users to avail the same with satisfactory quality. The results also show that even the channel is noisy the scheme extracts the decoding key correctly and avail better quality of image. The scheme is simple, cost effective, secured, easy to implement. All these characteristics make the scheme a possible solution for digital rights management (DMR).

CONCLUSION
Future work may be carried out to extend the proposed method for access control of video and sound data.

REFERENCES


