VOL. 9, NO. 5, MAY 2014 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

ENCRYPTING AND DECRYPTING IMAGE USING COMPUTER VISUALIZATION TECHNIQUES

Gunasekaran G. and Bimal Kumar Ray
School of Information Technology and Engineering, VIT University, Vellore, India
E-Mail: ggunasekaran@vit.ac.in

ABSTRACT

Today's networks are essential to our modern world, and a thorough understanding of how they act is vital to their efficient operation. Fortunately, data on networks is plentiful; by visualizing this network data, it is possible to greatly improve our understanding and also should provide the security for network data. The motivation of this paper is on visualizing the network data associated with a network image or object that will be send in the format of image at the sender and at the receiver ends that image or object will be encrypted in the form of rich text format that will be decrypted form at the receiver end. The technique sending data in image format will provide a greatest security for World Wide Web data transmission on network. We can also visualize that what data is behind on image and rendering of the image. Finally, this proposal is trying to encrypt and decrypt image visualization using computer visualization techniques.

Keywords: encryption, decryption, image, rich text format, rendering, stegnography, secure data.

1. INTRODUCTION

Because of the increasing demand for information security, image encryption decryption has become an important research area and it has broad application prospects. The field of encryption is becoming very important in the present era. Image security is of utmost concern as web attacks have become more and more serious. Image encryption decryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Many image content encryption algorithms have been proposed [1, 2, 3]. To make the data secure from various attacks and for the integrity of data we must encrypt the data before it is transmitted or stored. Government, military, financial institution, hospitals and private business deals with confidential images about their patient (in Hospitals), geographical areas (in research), enemy positions (in defense), product, financial status. Most of this information is now collected and stored on electronic computers and transmitted across network to other computer. If these confidential images about enemy positions, patient and geographical areas fall into the wrong hands, than such a breach of security could lead to declination of war, wrong treatment etc. Protecting confidential images is an ethical and legal requirement.

Another use of network (World Wide Web) could be for sending secure data which may be very essential for a group of companies, which should not be viewed by others. Therefore sensitive data hiding becomes most important area in securing network data. The technique which is used for securing data is known as encrypting, after encrypting data, with the help of network it is forwarded to its destination. At its destination encrypted data is decoded with the help of provided algorithm and this whole process is known as decryption. The private or sensitive information will be hidden within an image, so it appears that no information is hidden at all, and then with the help of media it is transferred to its destination with the secure password which then decrypted and the main rich text format retrieved from the image. In past times, method used was humans, wax tablets and invisible ink, which in modern society totally changed. Now a day's images, pictures, videos and voices are used as a carrier, they transferred from one place to other with the help of telecommunication network [4]. In this paper, three methods are proposed for image encryption. First method is reversible data hiding method in which the image is encrypted by doing XOR operation bit by bit. The second method is cat map transform method in which the image is scrambled using periodicity. The third method is RSA encryption and decryption method [2]. By comparing all these methods, we are able to achieve a better image quality in cat map transform. The proposed algorithm is simulated in matlab and their PSNR values are calculated. The philosophy of proposal algorithm is to use the full menu of "Strong operations" supported in modern computers to achieve better security properties and provide high speed. The main aim behind the design of this proposal is to get the best security and performance tradeoff over existing networked Web Images.

The paper is organized as follows. In section-2, background for encryption and decryption algorithms. In section-3 gives existing techniques for image encryption. In section-4 describes proposed system design for visualizing networking data i.e. how the original image is encrypted and decrypted. It also explains the security provided by the steganography technique watermarking and its properties. In section-5 the implementation of steganography in encrypted images using cryptography scheme is explained. Section-6 gives the simulation results and discussion and section-7 gives the conclusion.

2. BACKGROUND

Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the internet and through wireless networks. Encryption is the process of transforming the information for its security. With the

huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. The security of images has become more and more important due to the rapid evolution of the internet in the world today. The security of images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images [2]. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types. In 1993, Bruce Schneier published the Blowfish block cipher. At this time, the current Data Encryption Standard (DES) was known to be vulnerable to crypto analysis and brute-force attacks. Schneier developed Blowfish to be a publicly available cryptographic algorithm with the potential to replace DES. Schneier also encouraged others to evaluate the performance and security of Blowfish. To date, the security of Blowfish has not been compromised. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors.

Blowfish is a symmetric block cipher that encrypts data in 8- byte (64-bit) blocks. The algorithm has two parts, key expansion and data encryption [1, 2, 3, 5]. Key expansion consists of generating the initial contents of one array (the P-array), namely, eighteen 32-bit sub keys, and four arrays (the S boxes), each of size 256 by 32 bits, from a key of at most 448 bits (56 bytes). Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. Blowfish can have a key that ranges from 32 to 448-bits. It is suitable and efficient for hardware implementation and no license is required. Blowfish is a cipher based on Feistel rounds. No attack is known to be successful against this. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryption. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one.

3. EXISTING TECHNIQUES

There are many image encryption algorithms which are available such as Baker's Transformation, in this Baker's map is used for image encryption; Magic cube transformation is used to scramble the image pixels etc. But all these have some disadvantages for that purpose new algorithm has been developed in recent years.

3.1. Data encryption standard (DES)

DES (Data Encryption Standard) was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It was developed by an IBM team around 1974 and adopted as a national standard in 1997. DES is a 64-bit block cipher under 56-bit key. The algorithm processes with an initial permutation, sixteen rounds block cipher and a final permutation. DES application is very popular in commercial, military, and other domains in the last decades. Although the DES standard is public, the design criteria used are classified. There has been considerable controversy over the design, particularly in the choice of a 56-bit key.

3.2. Triple des (TDES)

The triple DES (3DES) algorithm was needed as a replacement for DES due to advances in key searching. TDES uses three round message this provides TDES as a strongest encryption algorithm since it is extremely hard to break 2^168 possible combinations. Another option is to use two different keys for the encryption algorithm. This reduces the memory requirement of keys in TDES. The disadvantage of this algorithm is that it is too time consuming.

3.3. Advanced encryption standard (AES)

AES was developed by two scientists Joan and Vincent Rijmen in 2000. AES uses the Rijndael block cipher. Rijndael key and block length can be 128, 192 or 256-bits. If both the key-length and block length are 128-bit, Rijndael will perform 9 processing rounds. If the block or key is 192-bit, it performs 11 processing rounds. If either is 256-bit, Rijndael performs 13 processing rounds.

3.4. Blowfish

Bruce Schneier designed blowfish in 1993 as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. The Blowfish algorithm has many advantages. It is suitable and efficient for hardware implementation and no license is required. The elementary operators of Blowfish algorithm include table lookup, addition and XOR. The table includes four S-boxes and a P-array. Blowfish is a cipher based on Feistel rounds, and the design of the F-function used amounts to a simplification of the principles used in DES to provide the same security with greater speed and efficiency in software. Blowfish is a 64 bit block cipher and is suggested as a replacement for DES. Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors.

3.5. RSA algorithm

RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the

Web browsers from Microsoft and Netscape. It's also part of Lotus Notes, Intuit's Quicken, and many other products. The encryption system is owned by RSA Security. The technologies are part of existing or proposed Web, Internet, and computing standards.

4. PROPOSED SYSTEM DESIGN FOR ENCRYPTING AND DECRYPTING IMAGE VISUALIZATION

4.1. Image encryption

Due to the fast progression of data exchange in electronic way, information security is becoming more important in data storage and transmission. Because of widely using images in industrial process, it is important to protect the confidential image data from unauthorized access. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text. In order to transmit secret images to other people, a variety of image encryption schemes have been proposed.

4.2. Reversible data hiding method

Several proposals have dealt with data hiding in image encryption implementations. The reversible data hiding scheme is used for encrypting the images. It is mainly used to embed additional message into some distortion, with a reversible manner so that the original content can be perfectly restored after extraction of the hidden messages. The proposed scheme is the content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. The data hider embeds additional data into the encrypted image using a data hiding key though he does not know the original content. Within an encrypted image containing additional data, a receiver must first decrypt it using the encryption key and the decrypted version is similar to the original image. According to the data-hiding key, he can further extract the embedded data and recover the original image from the decrypted version. The detailed procedures are as follows:

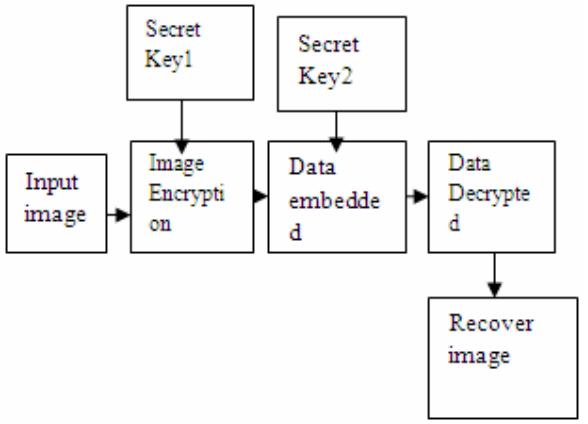

Figure-1. Proposed system design for encrypting and decrypting image visualization.

STEP-1: Consider an image, which is considered as a cover image.
STEP-2: Convert the cover image to binary.
STEP-3: Random bits are generated which act as the encryption key.
STEP-4: XOR operation is performed between the random bits generated and cover image.
STEP-5: Convert the above binary image to grayscale image. Thus, encrypted image is obtained.

4.3. LSB method

This method is used to hide the data in encrypted images. In 8-bit gray scale images are selected as the cover media. These images are called cover-images. Cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images [1, 3].

One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity. This allows a person to hide information in the cover image and make sure that no human could detect the change in the cover image. The LSB method usually does not increase the file size, but depending on the size of the information that is to be hidden inside the file, the file can become noticeably distorted. The detailed procedures as follows:

STEP-1: Consider an encrypted image (cover image).
STEP-2: Consider the message or data that should be hidden into the cover image.
STEP-3: Convert all the pixel values of the encrypted image from grayscale to binary (8-bit).
STEP-4: Embed the message or data into the cover image by hiding the data into the LSB bit of cover image.
STEP-5: The original image along with the data is recovered with less distortion and the PSNR value is calculated.

4.4. Cat map transform

This is the transform which stretches an image that is composed of n by n pixels and effectively wraps the stretched portions around to restore the original image. The proposed scheme is by using cat map transform and exclusive OR operation to produce scrambled images. The cat map transform is defined as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N$$

Where (x, y) is the image pixel location of an N *N image. a, b are positive integers.(x', y') is the new pixel location, y, (x ', y ') 1, 2,...*N* .The cat map transform above can efficiently scramble the 2D images [5]. The user can choose the number of iterations for applying the cat map transform to the image in order to achieve a higher level of security. The parameters a, b and iteration times N can act as security keys for the image scrambling process. The same procedure is used for data hiding using LSB method.

4.5. RSA encryption & decryption

RSA algorithm is currently accepted as the most mature and complete public key cryptosystem in both the theory and application [2, 3]. The first one can be used for both data encryption and digital signature, also, is the representative of public key cryptosystem. This paper applies the RSA algorithm in the pre-processing phase of information hiding to ensure the security of information. RSA algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent. The steps for RSA algorithm is as follows:

(1) Find two large primes p, q.
(2) n = p * q, z = (p - 1) * (q-1).
(3) Select a number e which is less than n and prime to z, so that e and z have no common factors.
(4) Select another number d, where (e*d-1) is divisible by z.
(5) The public key is (n, e) and the private key is (n, d).
(6) For a message m, if the cipher text is c, decryption and encryption process as follows:

Encryption:
c = m ^ e mod n.
Decryption:
m = c ^ d mod n.
Thus, the image encryption is obtained.

Algorithm to hide the data in encrypted image using LSB method:

STEP-1: Consider an encrypted image (cover image).
STEP-2: Consider the message or data that should be hidden into the cover image.
STEP-3: Convert all the pixel values of the encrypted image from grayscale to binary (8-bit).
STEP-4: Embed the message or data into the cover image by hiding the data into the LSB bit of cover image.
STEP-5: The original image along with the data is recovered with less distortion and the PSNR value is calculated.

5. RESULT

In this paper, we select the classical image of 256*256 for cameraman. tif with 256 gray levels as the original image and adopt the reversible data hiding method, Cat map transform and RSA algorithm for image encryption. We use MATLAB to simulate the experiment. Certainly not only static display could be used for embedding secure data, images, pictures, videos, voice and much more carrier could also be used for securing network data, only we can modify some changes required in above mentioned algorithm. Network stegnography helps in large amount in defiance system of any country to protect human resources. The major improvement in this field would be use of biometric protection system. For example; some annual reports show on High Technology Crime (HTC) lists nine common types of computer crime]: which are Criminal communications, Fraud Key fingerprint, Hacking, Electronic payments, Gambling and pornography, Harassment, Intellectual property offenses, Viruses, and Pedophilia. In India there is separate act based on cyber crime, which is easily available on World Wide Web. Cyber crime deals with all illegal use of Internet, and based on the crime their punishments also described. Terrorist uses Internet in such huge amount for their global communication, which to stop is almost impossible but government is doing its best to cut down their communication.

5.1. Reversible data hiding method

The test image Cameraman sized 256 *256 shown in Figure-2(a) was used as the original cover in the experiment. After image encryption, the 8 encrypted bits of each pixel are converted into a gray value to generate an encrypted image shown in Figure-2(b). Then, we embedded data into the encrypted image by using LSB method. The encrypted image with message is given as Figure-2(c), the decrypted image is given as Figure-2(d), and the values of PSNR caused by data embedding is 51.4 dB. At last, the embedded data were extracted and the original image was perfectly recovered from the decrypted image.

Figure-2. (a) Original image, (b) Scrambled images, (c) Encrypted images with message (d) decrypted version.

5.2. Cat map transform

The test image Cameraman sized 256 *256 shown in Figure-3(a) was used as the original cover in the experiment. Make the parameter in the Arnold cat secret, the images which are iterated 33 times and 21 times in a period are showed as Figure 3(b) and figure3(c) The decrypted image is given as Figure-3(d), and the values of PSNR caused by data embedding is 91.6 dB. The number of times may be selected according to visual effect. Through, the cat map, it realizes the scrambling and attain the purpose of encryption. It is safe to keep the secret of the parameters and the iteration times, but the attacker can also attract through the method of statistics analysis and exhaustion. So we still need to change the pixel value to encrypt further.

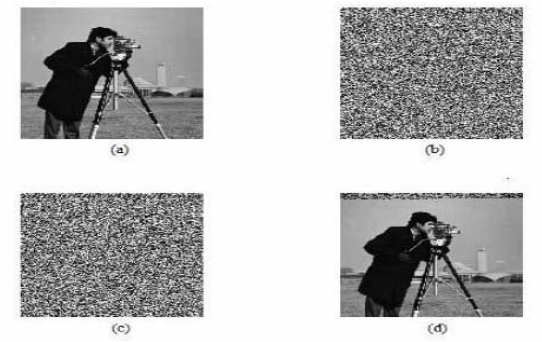

Figure-3. (a) Original image, (b) Scrambled images, (c) Encrypted images with message (d) decrypted version.

5.3 RSA encryption/decryption

The test image Cameraman sized 256 *256 shown in Figure-4(a) was used as the original cover in the experiment. Then, we embedded data into the encrypted image by using LSB method. The encrypted image with message is given Figure-4(c), is the encrypted file by public key. Figure-4(d) shows the extracted information that was decrypted by the private key. The test demonstrate that it is impossible to get the original information when input the wrong key which provides the protection to the hidden information.

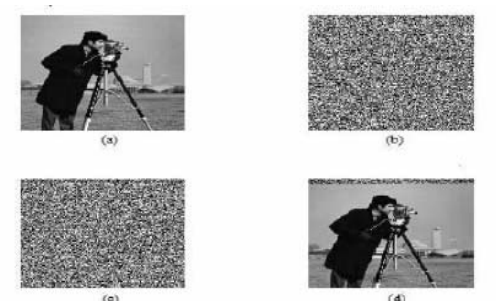

Figure-4. (a) Original image, (b) Scrambled image (c) Encrypted images with message (d) decrypted version.

6. CONCLUSIONS

In this paper, we demonstrate that the image encryption algorithm is efficient and highly secure. All parts of the proposed encryption system were simulated using MATLAB.The scheme can resist most known attacks, such as statistical analysis and brute-force attacks. All the experimental analysis shows that the proposed encryption algorithm has high level of security with less computation, it shows how to safe guard the sensitive data on network and it helps in securing the important information inside an image or picture.

ACKNOWLEDGEMENT

We would like to thank Min Wu and B. Liu for the valuable discussion on Data hiding in digital binary image, which was very useful for this work. We also thank Stalling, for the valuable discussion on Cryptographic and N/W security. We appreciate the help by Dr. Bimal Kumar Ray on proof reading of this paper.

REFERENCES

[1] Min Wu, and B. Liu. 2004. Data hiding in digital binary image. IEEE transactions on multimedia. 6(4).

[2] Cryptographic and N/W security: Principles and Practices by Stalling. Prentice Hall. 2nd Edition.

[3] Sos Agaian and Yicong Zhou. 2011. Image Encryption using the image steganography concept and PLIP model. IEEE International conference on System Science and Engineering. pp. 699-703.

[4] Richard A. Becker, Stephen G. Eick, and Allan R. Wilks. 1995. Visualizing Network Data. IEEE transaction on visualization and computer graphics. 1(1), March.

[5] V. Naveenkumar, Santosh Hariharan and Kumar Rajamani. 2011. Data hiding scheme for medical images using lossless code for mobile HIMS. IEEE International conference on Communication system and networks. pp.1-4.