2010 Second International conference on Computing, Communication and Networking Technologies

VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES

Piyush Marwaha[1], Paresh Marwaha[2]

Infosys Technologies Limited, India

[1]piyushmarwaha@hotmail.com

[2]pareshmarwaha@hotmail.com

Abstract - **In today's information age, information sharing and transfer has increased exponentially. The threat of an intruder accessing secret information has been an ever existing concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat.**

Cryptography involves converting a message text into an unreadable cipher. On the other hand, steganography embeds message into a cover media and hides its existence. Both these techniques provide some security of data neither of them alone is secure enough for sharing information over an unsecure communication channel and are vulnerable to intruder attacks.

Although these techniques are often combined together to achieve higher levels of security but still there is a need of a highly secure system to transfer information over any communication media minimizing the threat of intrusion.

In this paper we propose an advanced system of encrypting data that combines the features of cryptography, steganography along with multimedia data hiding. This system will be more secure than any other these techniques alone and also as compared to steganography and cryptography combined systems

Visual steganography is one of the most secure forms of steganography available today. It is most commonly implemented in image files. However embedding data into image changes its color frequencies in a predictable way.

To overcome this predictability, we propose the concept of multiple cryptography where the data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. We shall use traditional cryptographic techniques to achieve data encryption and visual steganography algorithms will be used to hide the encrypted data.

978-1-4244-6589-7/10/$26.00 ©2010 IEEE

KEYWORDS: Cryptography, Steganography, Visual Steganography, Public Key Cryptography, Joint Key Cryptography, Asymmetric Key Cipher, Symmetric Key Cipher, Image Steganography.

I. BASIC OVERVIEW ON CRYPTOGRAPHY

A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers (an encrypted piece of text). We will discuss the two basic and most commonly used algorithms – The joint key cryptography and the public key cryptography.

THE JOINT KEY CRYPTOGRAPHY (Symmetric key cipher) uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. Joint key cipher algorithms are less complex and execute faster as compared to other forms of cryptography but have an additional need to securely share the key. In this type of cryptography the security of data is equal to the security of the key. In other words it serves the purpose of hiding a smaller key instead of the huge chunk of message data.

THE PUBLIC KEY CRYPTOGRAPHY (asymmetric key cipher) is a technique that uses a different key for encryption as the one used for decryption. Public key systems require each user to have two keys – a public key and a private key (secret key). The sender of the data encrypts the message using the receiver's public key. The receiver then decrypts this message using his private key. This technique eliminates the need to privately share a key as in case of symmetric key cipher. Asymmetric cryptography is comparatively slower but more secure than symmetric cryptography technique. The public key cryptography is a fundamental and most widely used technique, and is the approach which underlies Internet standards such as Transport Layer Security (TLS) (successor to SSL). The most common algorithm used for secret key systems is the Data Encryption Algorithm (DEA) defined by the Data Encryption Standard (DES) [3].

A *HYBRID CRYPTOSYSTEM* is a more complex cryptography system that combines the features of both joint and public key cryptography techniques.

We shall use traditional public key cryptography techniques to covert the message into a cipher. For embedding the cipher into images, a modified joint key technique will be used.

II. BASIC OVERVIEW ON STEGANOGRAPHY

Steganography is the art of hiding the existence of the communication message before sending it to the receiver. It has been practiced since 440 B.C. in many ways like writing information on the back of cattle in a herd, invisible ink etc. Some relatively modern ways include hiding the information in newspaper articles and magazines etc.

Multimedia steganography is one of the most recent and secure forms of steganography. It started in 1985 with the advent of the personal computer applied to classical steganography problems. Visual steganography is the most widely practiced form of steganography and is usually done using image files. It started with concealing messages within the lowest bits of noisy images or sound files. Images in various formats like jpeg have wide color spectrum and hence do not reflect much distortion on embedding data into them.

We shall perform steganography on image files and we shall hide the encrypted message into image files in an encrypted format thus achieving a multiple cryptographic system. The most commonly used technique for image steganography is bit insertion where the LSB of a pixel can be modified. Ref [4] explains various other techniques involve spread spectrum, patch work, JPEG compression etc. Instead of traditional LSB encoding, we will use a modified bit encoding technique to achieve image steganography in which each pixel will store one byte of data.

III. MULTIMEDIA IMAGE FILES

Multimedia content basically comprises of images, videos and audio files. Images form the basis of visual multimedia. Videos are streams of images displayed in sequence at a certain speed. We shall focus on image files to achieve visual steganography.

Images are visual data stored in a picture frame. Images basically are made up of various regions consisting of pixels. These pixels in turn consist of three basic colors R (red), G (green) and B (blue). The pixel values (R, G, B values) can be manipulated to hide data in the images. A marginal deviation in these pixel values does not alter the images as a whole but a slight shade difference occurs in the altered region that is not visible in normal conditions. The image can hence serve as a cover for the information so as to achieve steganography. The edited image can be transmitted to the receiver along with the original image. The receiver then can decode the data from the image by pixel based image comparison [6]. The process involved in encoding and decoding uses a blend of media cryptography and asymmetric cryptographic algorithms.

An image or a multimedia data has 5 + 1 properties which include the position of color pixel on the x-axis, the position of color pixel in the y-axis, the R component of color, the G component of color, the B component of color and the sixth is the image description properties like size, timestamp etc. These properties are stored in the first few lines of image property description. The number of bits per pixel is also a property that varies in different images. To achieve a more general bit encoding system we shall use 8-bits per pixel image.

IV. THE VISUAL CRYPTOGRAPHIC STEGANOGRAPHY SYSTEM

In the multimedia steganocryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Each color in the multimedia data when considered as an element in an arrangement of 3D matrix with R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. The method which we will use to map the data is a block or a grid cipher. This cipher will contain the data which will be mapped in a 3-D matrix form where the x-axis can be for R (red), y-axis can be for G (green) and z-axis can be for B (blue).

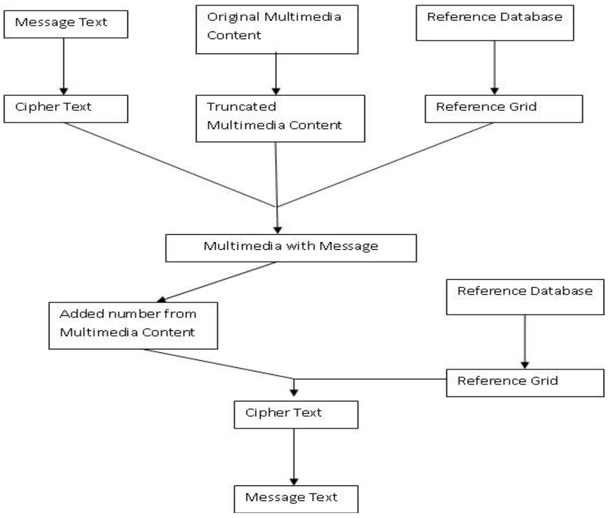

Fig. 1 System Flow Chart

Embedding data into an image often changes the color frequencies in a predictable way and also gives redundancy in formats like bmp. To remove this predictability, we will embed the cipher in the image in an encrypted form using a reference database instead of direct bit variations. Also only jpeg image will be used as it reflects the least impact of steganography.

V. PROPOSED METHOD

Cryptographic algorithms generally need a reference table which aids the conversion of a small block of data into another block (may not be a block of data in the original content).

- In order to provide higher security levels the algorithm is designed to use a reference database as shown in Fig. 2. The reference database will consist of various reference grids. Each of these grids will have a 3-d representation of the encoding schema which will be used to represent the characters in terms of specific numbers. (The same number may or may not represent a different character in a different grid)

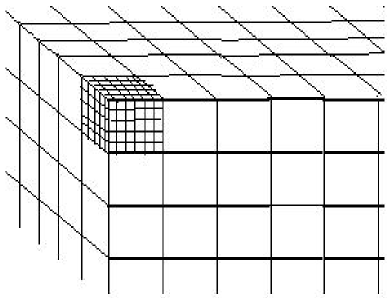

Fig. 2 Matrices in a Grid of the Reference database

1. *Encryption Algorithm*

- The message will first be encrypted using Asymmetric Key Cryptography technique. The data will be encrypted using basic DES algorithm [9]. This cipher will now be hidden into a multimedia file.
- The cipher will be saved in the image using a modified bit encoding technique by truncating the pixel values to the nearest zero digit (or a predefined digit) and then a specific number which defines the 3-D representation of the character in the cipher code sequence can be added to this number. For every character in the message a specific change will be made in the RGB values of a pixel. (This change

should be less than 5 for each of R,G and B values) This deviation from the original value will be unique for each character of the message. This deviation also depends on the specific data block (grid) selected from the reference database. For each byte in the data one pixel will be edited. Thus one byte of data will be stored per pixel in the image.

- In this method the cipher sequence can be decoded without the original image and only the edited image will be transmitted to the receiver.
- In the first few lines of image properties, the attributes of the image will be encrypted and saved so as to provide us the information if the image is edited or modified or the image extension has been changed like jpg to gif. These properties can be used in the decoding (identifying the correct block of data from the data grid). So only the correct encrypted image in the correct format will produce the sent message.
- For decryption, the receiver must know which image to decode and in which format as changing the image format changes the color distribution of the image. Every image gives a random data on decryption that has no meaning. But only the correct format decryption gives the original message.
- After hiding the data in the image, the image will be sent to the receiver. The receiver should have the decryption key (private key) which will be used to decode the data.

2. *Decryption Algorithm*

- The message can be decoded using an inverse function (as used in traditional techniques) using the receiver's private key. This key can be a part of the image or a text or any attribute of the image.
- The receiver's private key is used to identify the reference grid from the reference database.
- After selecting the correct grid, the x and y component of the image can define the block that has been used to encrypt the message and the RGB values can point to the data in the block identified by the x, y component as shown in Fig. 3.

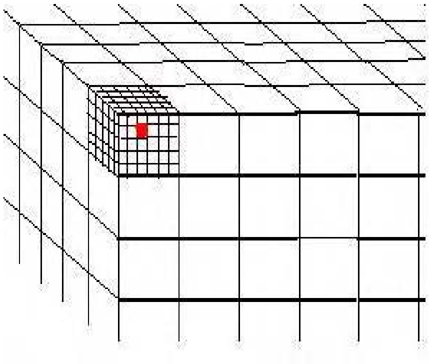

Fig. 3 Matrix in a grid of Reference database

- The cipher is retrieved by obtaining the difference in the pixel value from the closest predefined value (zero truncation). These numbers will now define the saved bit and will form the cipher text.
- This cipher can now be decrypted using an inverse function of the DEA algorithm to get the message text.

VI. EXPERIMRNTAL RESULTS AND ADVANTAGES OF THE ALGORITHM

The system was designed using an image of size 200x150 (30000) pixels. Initially, the pixel values were incremented to the next higher multiple of 5. The message text was converted into cipher text using DEA algorithm. The secret key used was 'This is the Secret Key'. Maximum possible size (29 Kb) of message data was taken considering one byte per pixel. The cipher text was then embedded into the jpeg image by pixel variation (decrement) of the selected value that was between 0-3 for R, 0-4 for G and 0-4 for B values of the pixel. The reference database consisted of 3 data grids. The data grid was selected on the basis of the number of pixels of the image. If the pixels were less than 1, 00,000 pixels the data grid 1 was selected, if they were between 1, 00,000 and 10, 00,000 then the data grid 2 was selected else the data grid 3 was selected. Each data grid had 20 matrices which were selected on the basis of the height to width ratio. The image containing message data was found to have no visible distortion.

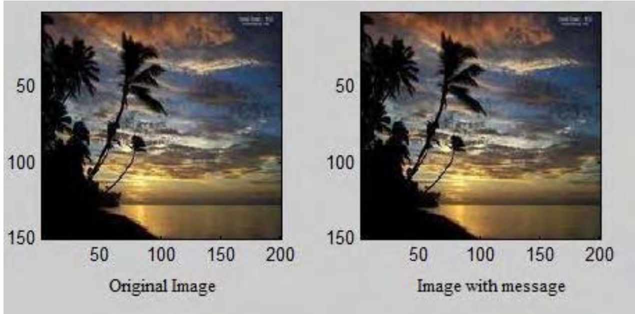

Fig. 4 Encryption result of the application.

For decryption the cipher was retrieved by checking the pixel variations and inverse DEA function was applied to retrieve the message. To retrieve the cipher from the image, the difference in the pixel value from the next higher multiple of 5 was calculated. The correct data grid from the reference database was selected on the basis of the number of pixels in the image. The correct matrix from the data grid was selected on the basis of the height to width ratio. After this the encrypted message was retrieved from the image. The inverse DEA function was applied to this encrypted message in order to retrieve the original message text.

The steganocryptic algorithm combines the features of cryptography and steganography and hence provides a higher level of security than either of the techniques alone.

The algorithm also is more secure than a normal cryptographic system as the encrypted data is hidden into a multimedia file and then transmitted. It is also more secure than a Steganography system as the data to be hidden is in an encrypted format. The algorithm scores over traditional visual steganography systems like LSB encoding as it implements multiple encryptions.

The image bits are used not to store the message but a slight deviation which correspond to a unique character. This deviation is then retrieved from the image and used to decrypt the original message. The image used for encryption is jpeg as it has the least deviation of embedding data.

VII. APPLICATION AREAS AND FUTURE SCOPE

This method can be used to increase the security on web based applications. The user will be asked to provide the secret key and the password can be compared from image files using the key. It can be used as advancement over the existing option to input the security phrase in various web based applications.

In the case of a secret message being transferred the information can be kept inside a multimedia data which will be the normal cipher which had to be transferred. This multimedia data can be transferred in the normal way. Video files and image streams can also be used to transmit data. In case of image streams part of message can be sent in each image. This will increase the security of the system, however the time consumption will increase in this case.

REFERENCES

[1]. Mizuho NAKAJIMA, “Extended use of Visual Cryptography for natural images, Department of Graphics and Computer Sciences”, Graduate School of Arts and Sciences, The University of Tokyo

[2]. Bart Preneel, “Cryptographic Algorithms: Basic concepts and application to multimedia security”, Katholieke University, Belgium

[3]. “Information Security”, National Institute of Standards and Technology, Special Publication, 2004

[4]. T. Morkel, “An Overview of Image Steganography”, Department of Computer Science, University of Pretoria, South Africa

[5]. Pradosh Kumar Mohapatra, “Public Key Crytography”, Crossroads: ACM Student Magazine, Sep 2000

[6] Paresh Marwaha, Piyush Marwaha, Shelly Sachdeva , “Content based Image Retrieval in Multimedia

Databases", International Journal of Recent Trends in Engineering, May 2009

[7]. Nameer N. EL-Emam, "Hiding a Large Amount of Data with High Security Using Steganography Algorithm", Applied Computer Science Department, Philadelphia University, Jordan,2007

[8]. Elvin M. Pastorfide and Giovanni A. Flores, "An Image Steganography Algorithm for 24-bit Color Images Using Edge-Detection Filter", Institute of Computer Science, 2007

[9]. "Data Encryption Standard (DES)", Federal Information Processing Standards Publication (FIPS PUB) 46-3, National Institute of Standards and Technology, Gaithersburg, 1999.

[10]. Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms", Department of Computer Sciences, Washington University, 2006 Publication

[11] Debashish Jena, "A Novel Visual Cryptography Scheme", IEEE International Conference on Advanced Computer Control, 2009