Certain Investigations of Image Security Algorithms for Ad hoc Networks

S. Kumar
Research Scholar,
Bharathiar University,
Coimbatore, Tamilnadu,India.

P. Sivaprakasam Ph.D
Research Guide
Associate Professor of Computer Science
Sri Vasavi College, Erode, Tamilnadu

ABSTRACT

Ad hoc Networks allows for communicating users in communication without relying on a infrastructure. The model of communication depends on the topology of the network. The users rely on the security protocols and security algorithms that are part of the network standard. The information being exchanged could be text ,image, video based on the user's requirement. There is a need for algorithms to be robust to avoid information loss. The data to be transmitted has to be protected from the intruders as it could result in reduction of credibility. The paper performs a exhaustive study of different security algorithms in ad hoc network. It concentrates on understanding the difficulties in handling the information I,e image across users. The paper presents a complete survey of the different security algorithms available for handling images. The information to be transmitted along with the images also needs to be analyzed for its complexity,size and vulnerabity. The paper presents research directions for transmitting images in adhoc networks in a efficient manner considering the different performance parameters that needs to be managed.

Keywords : Ad hoc Network, security algorithm, key size, graph, complexity

1. INTRODUCTION

Adhoc network is a collection of nodes that communicates without a infrastructure.Encryption refers to algorithmic schemes that encode plain text into non-readable form or cipher text, providing privacy. The receiver of the encrypted text uses a "key" to decrypt the message, returning it to its original plain text form. The key is the trigger mechanism to the algorithm. Fig 1.1 shows the encryption process.

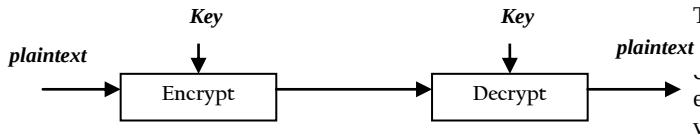

Fig 1.1: Encryption and Decryption process

A message is plaintext (sometimes called clear text). The process of disguising a message in such a way as to hide its substance is encryption. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption.

The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking ciphertext; that is, seeing through the disguise. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists. Modern cryptologists are generally trained in theoretical mathematics.

Plaintext is denoted by *M*, for message, or *P*, for plaintext. It can be a stream of bits, a text file, a bitmap, a stream of digitized voice, a digital video image...whatever. As far as a computer is concerned, *M* is simply binary data. (After this chapter, this book concerns itself with binary data and computer cryptography.) The plaintext can be intended for either transmission or storage. In any case, *M* is the message to be encrypted. Ciphertext is denoted by *C*. It is also binary data: sometimes the same size as *M*, sometimes larger. (By combining encryption with compression, *C* may be smaller than *M*. However, encryption does not accomplish this.) The encryption function *E*, operates on *M* to produce *C*. Or, in mathematical notation:

$$E(M) = C$$

In the reverse process, the decryption function *D* operates on *C* to produce *M*:

$$D(C) = M$$

Since the whole point of encrypting and then decrypting a message is to recover the original plaintext, the following identity must hold true:

$$D(E(M)) = M$$

They can be categorized into

1. Symmetric (private) key encryption.
2. Asymmetric (public) key encryption

(i) Symmetric Algorithms

There are two general types of key-based algorithms: symmetric and public-key. Symmetric algorithms, sometimes called conventional algorithms, are algorithms where the encryption key can be calculated from the decryption key and vice versa. In most symmetric algorithms, the encryption key and the decryption key are the same. These algorithms, also called secret-key algorithms, single key algorithms, or one-key algorithms, require that the sender and receiver agree on a key before they can communicate securely. The security of a symmetric algorithm rests in the key; divulging the key means that anyone could encrypt and decrypt messages .As long as the communication needs to remain secret, the key must remain secret. Encryption and decryption with a symmetric algorithm are denoted by:

$$E_K(M) = C$$
$$D_K(C) = M$$

Symmetric algorithms can be divided into two categories. Some operate on the plaintext a single bit (or sometimes byte) at a time; these are called stream algorithms or stream ciphers.

Others operate on the plaintext in groups of bits. The groups of bits are called blocks, and the algorithms are called block algorithms or block ciphers. For modern computer algorithms, a typical block size is 64 bits large enough to preclude analysis and small enough to be workable. (Before computers, algorithms generally operated on plaintext one character at a time. You can think of this as a stream algorithm operating on a stream of characters.)

(ii) Public-Key Algorithms

Public-key algorithms (also called asymmetric algorithms) are designed so that the key used for encryption is different from the key used for decryption. Furthermore, the decryption key cannot (at least in any reasonable amount of time) be calculated from the encryption key. The algorithms are called "public-key" because the encryption key can be made public: A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the public key, and the decryption key is often called the private key. The private key is sometimes also called the secret key, but to avoid confusion with symmetric algorithms, that tag won't be used here. Encryption using public key K is denoted by:

$$E_K(M) = C$$

Even though the public key and private key are different, decryption with the corresponding private key is denoted by:

$$D_K(C) = M$$

Sometimes, messages will be encrypted with the private key and decrypted with the public key; this is used in digital signatures (see Section 2.6). Despite the possible confusion, these operations are denoted by, respectively:

$$E_K(M) = C$$
$$D_K(C) = M$$

Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power.

2. RELATED WORK

Different Types of Image Encryption Schemes

In order to transmit secret images to other people, a variety of encryption schemes have been proposed. Current image encryption schemes are introduced briefly here.

2.1 Visual Cryptography for Color Images

Visual cryptography uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor complex computation. For security concerns, it also ensures that hackers cannot perceive any clues about a secret image from individual cover images. Young-Chang Hou [9] have proposed three methods for visual cryptography. Gray-level visual cryptography method first transforms the gray-level image into a halftone image and then generates two transparencies of visual cryptography. Obviously, we indeed cannot detect any information about the secret image from the two sharing transparencies individually, but when stacking them together, the result clearly shows the secret image. Method 1 uses four halftone images, cyan, magenta, yellow and black, to share the secret image. The codes of the four sharing images are fully disordered, and we cannot perceive any clue of the original secret image from any single sharing image. Method 2 reduces the inconvenience of Method 1 and requires only two sharing images to encrypt a secret image. However, after stacking the sharing images generated by Method 2, the range of color contrast will be 25% of that of the original image. Method 3 loses less image contrast, which is better than Method 2.

2.2 A New Chaotic Image Encryption Algorithm

Jui-Cheng Yen and Jiun-In Guo [8] have proposed a new image encryption scheme based on a chaotic system. In their method, an unpredictable chaotic sequence is generated. It is used to create a binary sequence again. According to the binary sequence, an image's pixels are rearranged. This algorithm has four steps. Step-1 determines a chaotic system and its initial point $x(0)$, row size M and column size N of the image f, iteration number no, and constants α, β, and μ used to determine the rotation number. Step-2 generates the chaotic sequence from the chaotic system. Step-3 generates the binary sequence. Step-4 includes special functions to rearrange image pixels. These functions are

$\boldsymbol{ROLR}_{l}^{i,p} : f \rightarrow f'$ is defined to rotate each pixel in the i^{th} row in f, $0 \leq i \leq M$ -1, in the left direction p pixels if l equals 0 or in the right direction p pixels if l equals1.

$\boldsymbol{ROUD}_{l}^{j,p} : f \rightarrow f'$ is defined to rotate each pixel in the jth column in f, $0 \leq i \leq N$ -1, in the up direction p pixels if l equals 0 or in the down direction p pixels if l equals 1.

$\boldsymbol{ROUR}_{l}^{k,p} : f \rightarrow f'$ is defined to rotate each pixel at position (x,y) in the image f such that $x + y = k$, $0 \leq k \leq M + N$-2, in the upper-right direction p pixels if l is equal to 1 or in the lower-left direction p pixels if l is equal to 0.

$\boldsymbol{ROUL}_{l}^{k,p} : f \rightarrow f'$ is defined to rotate each pixel at position (x,y) in the image f such that $x-y=k$, $-(N-1) \leq k \leq M$-1, in the upper-left direction p pixels if l is equal to 0 or in the lower-right direction p pixels if l is equal to 1.

2.3 Block Cipher Algorithms (using Image Encryption)

Many encryption algorithms[13] are widely available and used in information security. They can be categorized into Symmetric (private) and Asymmetric (public) keys encryption (Fig 3.1). In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. The key should be distributed before transmission between entities. If weak key is used in algorithm then every one may decrypt the data. Strength of Symmetric key [3] encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using smaller key.

Asymmetric key encryption or public key encryption is used to solve the problem of key distribution. In Asymmetric keys, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption .Because users tend to use two keys: public key, which is known to the public and private key which is known only to the user. There is no need for distributing them prior to transmission.

However, public key encryption is based on mathematical functions, computationally intensive

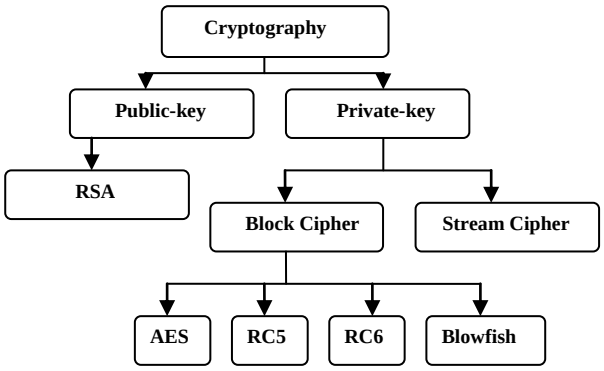

Fig 2.1: Overview of the field of cryptography

2.3.1 Image File Formats

They are standardized means of organizing and storing images. This entry is about digital image formats used to store photographic and other images; (for disk-image file formats see Disk image). Image files are composed of either pixel or vector (geometric) data that are rasterized to pixels when displayed (with few exceptions) in a vector graphic display. The pixels that compose an image are ordered as a grid (columns and rows); each pixel consists of numbers representing magnitudes of brightness and color.

Image file size—expressed as the number of bytes—increases with the number of pixels composing an image, and the colour depth of the pixels. The greater the number of rows and columns, the greater the image resolution, and the larger the file. Also, each pixel of an image increases in size when its colour depth increases—an 8-bit pixel (1 byte) stores 256 colours, a 24-bit pixel (3 bytes) stores 16 million colors, the latter known as true color.

Image compression uses algorithms to decrease the size of a file. High resolution cameras produce large image files, ranging from hundreds of kilobytes to megabytes, per the camera's resolution and the image-storage format capacity. High resolution digital cameras record 12 megapixel (1*MP* = 1,000,000 pixels / 1 million) images, or more, in truecolor. For example, an image recorded by a 12 *MP* camera; since each pixel uses 3 bytes to record truecolor, the uncompressed image would occupy 36,000,000 bytes of memory—a great amount of digital storage for one image, given that cameras must record and store many images to be practical. Faced with large file sizes, both within the camera and a storage disc, image file formats were developed to store such large images. An overview of the major graphic file formats follows below.

Major Graphic file formats- Including proprietary types, there are hundreds of image file types. The PNG, JPEG, and GIF formats are most often used to display images on the Internet. These graphic formats are listed and briefly described below, separated into the two main families of graphics: raster and vector.

2.3.1.1 JPEG

JPEG (Joint Photographic Experts Group) files are (in most cases) a lossy format; the DOS filename extension is JPG (other operating systems may use JPEG). Nearly every digital camera can save images in the JPEG format, which supports 8 bits per color (red, green, blue) for a 24-bit total, producing relatively small files. When not too great, the compression does not noticeably detract from the image's quality, but JPEG files suffer generational degradation when repeatedly edited and saved. Photographic images may be better stored in a lossless non-JPEG format if they will be re-edited, or if small "artifacts" (blemishes caused by the JPEG's compression algorithm) are unacceptable.

2.3.1.2 TIFF

The TIFF (Tagged Image File Format) is a flexible format that normally saves 8 bits or 16 bits per color (red, green, blue) for 24-bit and 48-bit totals, respectively, using either the TIFF or the TIF filenames. The TIFF's flexibility is both blessing and curse, because no single reader reads every type of TIFF file. TIFFs are lossy and lossless; some offer relatively good lossless compression for bi-level (black&white) images. Some digital cameras can save in TIFF format, using the LZWcompression algorithm for lossless storage. The TIFF image format is not widely supported by web browsers. TIFF remains widely accepted as a photograph file standard in the printing business. The TIFF can handle device-specific colour spaces, such as the CMYK defined by a particular set of printing press inks. OCR (Optical Character Recognition) software packages commonly generate some (often monochromatic) form of TIFF image for scanned text pages.

2.3.1.3 PNG

The PNG (Portable Network Graphics) file format was created as the free, open-source successor to the GIF. The PNG file format supports truecolor (16 million colors) while the GIF supports only 256 colors. The PNG file excels when the image has large, uniformly colored areas. The lossless PNG format is best suited for editing pictures, and the lossy formats, like JPG, are best for the final distribution of photographic images, because JPG files are smaller than PNG files. PNG, an extensible file format for the lossless, portable, well-compressed storage of raster images. PNG provides a patent-free replacement for GIF and can also replace many common uses of TIFF. Indexed-color, grayscale, and truecolor images are supported, plus an optional alpha channel. PNG is designed to work well in online viewing applications, such as the World Wide Web, so it is fully streamable with a progressive display option. PNG is robust, providing both full file integrity checking and simple detection of common transmission errors.

2.3.1.4 GIF

GIF (Graphics Interchange Format) is limited to an 8-bit palette, or 256 colors. This makes the GIF format suitable for storing graphics with relatively few colors such as simple diagrams, shapes, logos and cartoon style images. The GIF format supports animation and is still widely used to provide image animation effects. It also uses a lossless compression that is more effective when large areas have a single color, and ineffective for detailed images or dithered images.

2.3.1.5 BMP

The BMP file format (Windows bitmap) handles graphics files within the Microsoft Windows OS. Typically, BMP files are uncompressed, hence they are large; the advantage is their simplicity, wide acceptance, and use in Windows programs.

2.4 Gray Scale Image Encryption

Existing system contains symmetric block cipher algorithms for gray scale [4] Bitmap image encryption. Symmetric means the key used for encryption and decryption is the same, while block means the data (information) to be encrypted is divided into blocks of equal length.

Bitmap (BMP) image is a type of uncompressed image format which preserves all information about the image data. The encryption process has two inputs, the plaintext (data image) and the encryption key. To encrypt an image, its header is excluded and the start of the bitmap's pixels or array begins right after the header of the file. The bytes of the array are stored in row order from left to right with each row representing one scan line of the image. The rows of the image are encrypted from top to bottom. RC6, AES block ciphers used there. The key length for algorithms is 16 bytes (128 bits). In the decryption process, the encrypted image is divided into the same block length of each algorithm from top to bottom. The first block is entered to the decryption function of each algorithm and the same encryption key is used to decrypt the image but the application of sub-keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom. The bitmap image encryption will be done with three modes of operation, the Electronic Code Book (ECB) mode, the Cipher Block Chaining (CBC) mode, and the Output Feed Back (OFB) mode.

In image contains large amount of data, the ECB mode may not be secure. If the message is highly structured, it may be possible for a cryptanalyst to exploit these regularities. For example, if it is known that the message always starts out with certain predefined fields, then the cryptanalyst may have a number of known plaintext-ciphertext pairs to work with. If the message has repetitive elements, with a period of repetition a multiple of b bits, then these elements can be identified by the analyst. This may help in the analysis or may provide an opportunity for substituting or rearranging blocks.

2.5 Color Image Encryption

A pixel in a color image is represented in three values Red, Green, Blue. This preserves all information about the image data. The encryption process has two inputs, the plaintext (data image) and the encryption key. To encrypt an image, the color image pixels or array begins right the file. The bytes of the array are stored in row order from left to right with each row representing one scan line of the image. The rows of the image are encrypted from top to bottom. The key length for the four algorithms is 16 bytes (128 bits). In the decryption process, the encrypted image is divided into the same block length of each algorithm from top to bottom. The first block is entered to the decryption function of each algorithm and the same encryption key is used to decrypt the image but the application of sub-keys is reversed. The process of decryption is continued with other blocks of the image from top to bottom. The bitmap image encryption will be done with three modes of operation, the Electronic Code Book (ECB) mode, the Cipher Block Chaining (CBC) mode, and the Output Feed Back (OFB) mode. The color images, JPEG, PNG, TIF, and BMP. Image data can be either indexed or true color. An indexed image stores colors as an array of indices into the figure color map. A true color image does not use a color map; instead, the color values for each pixel are stored directly as RGB triplets.

2.6 Performance Parameters

One of the important factors in examining the encrypted image is the visual inspection where the highly disappeared features of the image the better the encryption algorithm. But depending on the visual inspection only is not enough in judging the complete hiding of the content of the data image. So, other measuring techniques are considered to evaluate the degree of encryption quantitatively. With the implementation of an encryption algorithm to an image, a change takes place in pixel values as compared to the values before encryption. Such change may be irregular. Apparently this means that the higher the change in pixel values, the more effective will be the image encryption and hence the quality of encryption. So, the quality of encryption may be expressed in terms of the total deviation (changes) in pixel values between the original image and the encrypted one [11].In addition to the visual inspection, three measuring quality factors will be considered to evaluate and compare between the three encryption algorithms RC6, RC5,Blowfish,AES. These factors are the maximum deviation, the correlation coefficient and irregular deviation [12].

2.6.1 The Maximum Deviation Measuring Factor

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original and the encrypted images [11]. The steps of this measure will be done as follows:

1) Count the number of pixels of each grayscale value in the range from 0 to 255 and present the results graphically (in the form of curves) for both original and encrypted images (i.e.; get their histogram distributions).
2) Compute the absolute difference or deviation between the two curves and present it graphically.
3) Count the area under the absolute difference curve, which is the sum of deviations (D) and this represents the encryption quality. D is given by the following equation:

$$D = \frac{h_0 + h_{255}}{2} + \sum_{i=1}^{254} hi$$

Where hi is the amplitude of the absolute difference curve at value i. Of course, the higher the value of D, the more the encrypted image is deviated from the original image.

2.6.2 The Correlation Coefficient Measuring Factor

Correlation is a measure of the relationship between two variables. If the two variables are the image and its encryption, then they are in perfect correlation (i.e.; the Correlation coefficient equals one) if they are highly dependent (identical). In this case the encrypted image is the same as the original image and the encryption process failed in hiding the details of the original image. If the correlation coefficient equals zero, then the original image and its encryption are totally different, i.e., the encrypted image has no features and highly independent on the original image. If the correlation coefficient (C.C) equals -1, this means the encrypted image is the negative of the original image. So, success of the encryption process means smaller values of the C.C. The C.C is measured by the following equation:

$$The\ Correlation\ Coefficient = \frac{cov(x,y)}{\sigma x\ \sigma y}$$

$$= \frac{\sum_{i=1}^{N}(xi - E(x))(yi - E(y))}{\sqrt{\sum_{i=1}^{N}(xi - E(x))^2}\sqrt{\sum_{i=1}^{N} yi - E(y))^2}}$$

Where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, and x and y are gray-scale pixel values of the original and encrypted images.

2.6.3 The Irregular Deviation Measuring Factor

This quality measuring factor is based on how much the deviation caused by encryption (on the encrypted image) is irregular [12]. It gives an attention to each individual pixel value and the deviation caused at every location of the input image before getting the histogram as described in [10] which does not preserve any information about the location of the pixels. This method can be summarized in the following steps:
1) Calculate the 'D' matrix which represents the absolute values of the difference between each pixel values before and after encryption. So, D can be represented as:

$$\mathbf{D = | I - J |}$$

Where I is the input image, and J is the encrypted image.
2) Construct the histogram distribution 'H' of the absolute deviation between the input image and the encrypted image. So, H = histogram (D).
3) Get the average value of how many pixels are deviated at every deviation value (i.e., the number of pixels at the histogram if the statistical distribution of the deviation matrix is a uniform distribution). This average (DC) value can be calculated as:

$$DC = \frac{1}{256}\sum_{i=0}^{255} h_i$$

Where hi is the amplitude of the absolute difference histogram at the value i.
4) Subtract this average from the deviation histogram, then take the absolute value of the result.

$$\mathbf{AC\ (i) = | H(i) - DC |}$$

5) Count the area under the absolute AC value curve, which is the sum of variations of the deviation histogram from the uniformly distributed histogram.

$$\boldsymbol{ID} = \sum_{i=0}^{255} AC(i)$$

The lower the ID value, the better the encryption algorithm.

3. CONCLUSION

This paper presents a set of approaches for handling image security. The different performance parameters that are part of the study are completed and presented. The paper could be extended by analyzing the computational part of the approaches in real domain. This can be extended in the following directions:

(i) A suitable application could be selected and the approach can be implemented an the feasibility of the image security algorithms can be completed.

(ii) The features can be extracted and the approach can be trained to minimize the error rate.

(iii) The approach can be extended with neural network and fuzzy approaches.

(iv) Varied Data set can be collected in real time and the camera characteristics can be analyzed.

(v) A complete performance estimation can be done based on Time Complexity ,Visual inspection, Quality measurements, Histogram Analysis

4. REFERENCES

[1] N. El-Fishawy, "*Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms*", International Journal of Network Security, Nov. 2007, PP.241–251

[2] Diaa Salama Abdul. Elminaam1, Hatem ohamed Abdul Kade and Mohie Mohamed Hadhoud, "*Performance Evaluation of Symmetric encryption Algorithms*", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008

[3] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, *"Encryption Efficiency Analysis and security Evaluation of RC6 Block Cipher for Digital Images",* International Conference on Electrical Engineering, April 2007

[4] Bruce Schneier, "*Applied Cryptography – Protocols, algorithms, and source code in C*", John Wiley & Sons, Inc., New York, second edition, 1996

[5] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah,"*Encryption Quality Analysis of RC5 Block Cipher Algorithm for Digital Images*", Journal of Optical Engineering, vol. 45, 2006.

[6] W. Stallings, "*Network and Internetwork Security: ice*",Prentice- Hall, New Jersey, 1995.

[7] Man Young Rhee, *"Internet Security Cryptographic Principles, Algorithms and Protocols*", John Wiley & Sons Ltd, 2003.

[8] T. Pevn´y and J. Fridrich. "*Merging Markov and DCT features for multi-class JPEG steganalysis*". In E. J. Delp and P. W. Wong, editors, Proceedings SPIE,Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents IX, volume 6505, pages 3 1–3 14, San Jose, CA, January 29 –February 1, 2007

[9] J. Fridrich. "*Feature-based steganalysis for JPEG images and its Implications for future design of steganographic scheme*". In J. Fridrich, editor, Information Hiding, 6th International Workshop, volume 3200 of Lecture Notes in Computer Science, pages 67–81, 2005.

[10] Avcibas, M. Kharrazi, N. Memon, and B. Sankur, "*Image steganalysis with binary similarity measures*," EURASIP J. Appl. Signal Process. 2005 (17), 2749–2757(2005).

[11] M. Kharrazi, H. T. Sencar, and N. Memon. "Benchmarking steganographic and steganalytic techniques". *In Proceedings of SPIE Electronic Imaging, Security,*Steganography and Watermarking of Multimedia Contents VII, San Jose, CA, 2005.

[12] D. C. Wu, and W. H. Tsai, "*A Steganographic Method for Images By Pixel Value Differencing*", Pattern Recognition Letters, Vol. 24, pp. 1613–1626, 2003

[13] Vajiheh Sabeti, Shadrokh Samavi, Mojtaba Mahdavi, Shahram Shirani, "*Steganalysis of Pixel-Value Differencing Steganographic Method*", IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, 2007, pp.292-295,22-24Aug.2007

[14] S.-L. Li, K.-C. Leung, L.-M. Cheng, and C.-K. Chan, "*Data Hiding In Images By Adaptive LSB Substitution Based On The Pixel-Value Differencing*", First International Conference on Innovative Computing, Information and Control (ICICIC'06), Vol. 3, pp. 58-61, 2006

[15] H. C. Wu, N. I. Wu, C. S. Tsai, and M.-S. Hwang, "*Image Steganographic Scheme Based On Pixel-Value Differencing and LSB Replacement Methods*", IEE Proceedings on Vision, Image and Signal Processing, Vol. 152, No. 5, pp. 611-615, 2005

[16] Ko-Chin Chang, Chien-Ping Chang, Ping S. Huang, and Te-Ming Tu, "*A Novel Image Steganographic Method Using Tri-Way Pixel-Value Differencing*", National Science Council, R.O.C, © 2008 Academy Publisher

[17] Cox I. J., Miller M. L., Boom J.A., Jessica Fridrich, "*Digital Watermarking And Steganography*", 2nd edition, Morgan Kaufmann publishers, 2008

[18] Y. K. Lee, L. H. Chen, "*High Capacity Image Steganographic Model*", IEE Proceedings on Vision, Image and Signal Processing, Vol. 147, No.3, pp. 288-294, 2000