Securing Data Using Jpeg Image over Mobile Phone

Roopesh Kumar [1], Yogendra Kumar Jain[2] and Pankaj Agarwal[3]

[1] Samrat Ashok Technological Institute , Vidisha (M.P.) 464001 India

Received: 13 May 2011 Accepted: 6 June 2011 Published: 21 June 2011

Abstract

In recent past years, Internet and Mobile is widely used for communication. Multimedia messaging (MMS) and Short Service Messaging (SMS) are the popular services provided by the telecommunication companies. In MMS we can easily send picture with text message. In SMS we can send text only. These techniques make the communication so fast. As well as the communication became easy attention toward information security increased. Data Security is the main concern for research. Mostly used techniques for secure communication are Cryptography and Steganography. There are so many techniques for steganography and cryptography. Mostly used techniques are image steganography and there are so many algorithms for this. For the cryptography mainly AES techniques is being used. In this paper we are presenting a technique using cryptography and steganography for securing information over mobile in MMS. It is very common practice to hide data in LSB of pixel. Spatial and frequency domains are generally used for image processing. Spatial domain have so many computations comparatively frequency domain. There different transform techniques are used for transformation e.g. DCT, FFT and wavelets. Here we are using Discrete Cosine transform (DCT) for image steganography and tiny encryption algorithm for cryptography. Tiny encryption algorithm (TEA) is block cipher algorithm.It is simple and fast but best for mobile application.

Index terms— Steganography, DCT, Messaging.

1 INTRODUCTION

he most important characteristics of (digital) information are that it is very easy to create and distribute unlimited number of its copies. There may be different type of areas like music, film, book and software which requires protection or security. It is a very big problem dealing with the protection of the intellectual and production rights. The fact that an unlimited number of perfect copies of text, audio and video data can be illegally produced and distributed requires studying ways of embedding copyright information and serial numbers in audio and video data. Steganography and watermarking bring a variety of very important techniques how to hide important information in an undetectable and irremovable way in audio and video data.Steganography and watermarking are main parts of the fast developing area of information hiding. Steganography emphasize on hiding of existence of message. Watermarking emphasize on protection in such way that no one can remove or change the information. Other way of information security is cryptography. Cryptography hides the message from attacker not the existence of that message. The word steganography originally derived from Greek word which means ”covered writing” [2].

2 II. RELATED WORK

Most of the work has been carried out in the steganography field. Mainly steganography has been done on bit map pictures, gif pictures and on gray scale pictures. Researchers have given so many methods for image steganography as follows The purpose of steganography is hiding of data in to another data. As defined by Cachin [1], steganography is the art and science of communicating in such a way that the presence of a message cannot be detected. Steganography refers to the science of ”invisible” communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer [3]. In recent years mobile phones are widely useful devices for communication. MMS (Multimedia Messaging Service) is a technology that allows a user of a properly enabled mobile phone to create, send, receive and store messages that include text, images, audio and video clips [6]. Now a day's people are using cell phones and wireless technology too much. It is very convenient way for communication by sending SMS or MMS. We can also send MMS while we are talking over phone. There is not such application have been developed for mobile phone to hide the data. Hiding data in text message has implemented. In this paper mms technologies are used for sending message and data hiding technique for jpeg images is used as well as text hiding technique is used for steganography. Moreover, there are some constraints for the size of media text cannot exceed 30kB, an image must be below 100kB and a video must be smaller than 300kB [4].So many research have already been done in the field of image steganography but till now not any technique implemented for mobile jpeg steganography, in this paper Steganography has implemented for jpeg image on mobile.

3 August

, a) Ancient steganography

The first recorded use of steganography found from 440 BC back when Herodotus informed to Greece about forthcoming attack by writing a message on the wooden and covered it by wax. Another example of ancient steganography is Histiaeus who shaved the head of his slave and tattooed the message on it after hair grown message was hidden **??**13].

Several steganography methods were used during II world war. Microdots developed by the Nazis are essentially microfilm chips created at highly magnification. These dots could contain pages of information and drawing etc. The Nazis also employed invisible ink and null ciphers [14].

Later on steganography came in the form of digital steganography .Digital steganography has been performed by various methods some of commonly used methods are as follows.

4 b) Jsteg Algorithm

This algorithm made by Derek Upham. It was the first publicly available steganography system for JPEG. Its embedding algorithm sequentially replaces the least significant bit of DCT coefficient with message's data.

Jsteg algorithm: Input : message, cover images Output: stego image While data left to embed do Get next DCT coefficient from cover image if DCT ? 0 and DCT?1 then get next lsb from message replace DCT LSB with message LSB end if insert DCT into stego image end while [12] c) F3 Algorithm It differs in double respect from jsteg: 1. Instead of overwriting bits it decrement the coefficient's absolute values in case their LSB does not match-except coefficient with the value zero, where we cannot decrement the absolute value. 2. Some embedded bits fall victim to shrinkage. due to receiver could not distinguish a zero coefficient, it skips all zero coefficients. Hence sender repeatedly embed the affected bits since he notice when he produces a zero [5].

5 d) F4 Algorithm

It uses invert steganography and removes the drawback of F3 algorithm. Even positive coefficient shows zero and odd shows positive one. Even negative coefficient shows one and odd negative zero. [5] e) F5 Algorithm This is developed by Andreas Westfield researcher specialized in steganography. Provably one of the most advance program publicly available. It uses matrix encoding technique. The best suitable technique for jpeg steganography is considered F5 algorithm [5].

6 ALGORITHM:

1. JPEG compression. Stop after quantization. 2. Using password key initialize random number generator 3. Instantiate permutation 4. Determine the parameter k from the capacity of carrier medium and the length of secret message 5. Calculate the code word length n=2 k -1 6. Embed the secret message with (I, N, K) matrix encoding. 7. Continue JPEG compression [5].

In the mobile computation very less work has been done for steganography. Some research are as follows:

1. Text Steganography : In 2007 Mohammad Shirali Shahreza and M.Hassan Hasan Shirali Shahreza have given the new method for text steganography in SMS (Short Messaging Service). The purpose of this project is to hide information in SMS by abbreviations text steganography and with the use of SMS texting language [15]. 2. Steganography in MMS : This work is also carried out by M. Shirali Shareza. He has given the algorithm for steganography in MMS using PNG format. He has described the new method of steganography using both text and images. First the data is broken into two parts. Each part size is proportionate to the capacity of the text and the image for hiding data. For example if the text has 10 bits capacity and the image has more than 200 bits capacity for hiding data, and the data which we want to hide is 60 bits, then we hide the data as follows: First we save the size of information which is stored in the MMS in the image, because knowing the size of the information is necessary for decoding correctly the information. Then we hide the first bit in the text. After

that we hide 5 next bits in the image. Then we hide the 7th bit in the text. After that we hide 5 next bits in the image again. We do this loop until reach the end of data. For hiding data in the text part of MMS message, the mentioned text steganography method is used; and for hiding the data in image part of MMS message, the image steganography method is used [6].

7 Steganography in SMS by Sudoku puzzle :

This technique also presented by Shahreza and Shahreza [16]. In this paper, they proposed a method of hiding data in Sudoku puzzle and arranged number in each row and column of Sudoku by permutations of 9!. For hiding the data, they place the numbers accordance with the desired permutations in a row or column of 9 x 9 sudoku puzzle. In view of this, we solve the Sudoku puzzle in which we want to hide the data. Then we replace certain row or column of this Sudoku puzzle in accordance with the permutation 1 through 9 which created [16].

8 III. PEAK TO SIGNAL RATIO

Signal to noise (SNR) measures are estimates of the quality of a reconstructed image compared with an original image. The basic idea is to compute a single number that reflect the quality of the reconstructed image. The actual metric we compute is the peak signal to noise ratio of reconstructed image measure which is called PSNR [10].The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec. The signal in this case is original data and the noise is the error introduced by the compression. When comparing compression codec it is used as an approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality). It is most easily defined by the mean squared error (MSE) which for two m x n monochrome images I and K where one of the image is considered as a noisy expression of the other is defined as:

The PSNR in decibels (db) is computed using Here MAX I is the maximum possible pixel value of the image. When the pixels are represented using 8 bit per sample, this is 255 [11].

IV.

9 PROPOSED METHOD

Previous work is carried out using text steganography and image steganography and for this purpose PNG (Portable Network Graphic) image is used. In the future work Author suggested that it could be implemented on JPEG file. So in this paper we have done the JPEG steganography-using concept of F5 algorithm [5] we can summarize the method as follows:

In the first step partitioned plan in 8x8 pixel blocks. Secondly generate DCT [Discrete Cosine transform] Coefficient block. The basic idea for a steganography algorithm is that, embeds a secret message into a JPEG image is to alter the quantization step, the algorithm embeds more zeroes than ones, and this could be statistically detectable. Moreover, the histogram of the coefficients contains much odd than even coefficients. We also embedded text in text using text steganography [15] a) Steps for procedure: Get the original message which is combination of text SMS and JPEG image Get the text to hide (Text which has to be hidden in original message) Encrypt the message before hiding. Count the length of message which has to be hide Check the possibility of receiving text to hide (limitation of hiding text) Hide the bits according to the order of (1,2,4,16,?) in the text. After completion in text part remaining bits hide in the image. For receiver side follow the procedure in reverse order. b) Step to hide in text: In all four cases we do not change more than one bit [5].

10 d) Encryption for text:

In this paper for encryption in text which has to be hide, ”Tiny encryption Algorithm” has been used. It can be used as replacement of DES, and short enough to write in to almost any program on any computer [9].It has 32 rounds of simple processes which are shifts, additions and XORs. It is suitable encryption for J2ME implementation.

11 RESULT

We have used different images to embed the data inside. Here one message is conveyed and text is hidden inside it. After embedding the whole message converted in capital letters and replacement has done according to few matching word list shown in table **??**.

Table **??** shows the PSNR value for different images hiding the same data. Original image contain the hidden data ”Roopesh” which produce stego image. The PSNR value gives peak signal to nose ratio. Usually PSNR more than 35db is considered good quality so our results have the good values. [1] [2] [3]

[1] © 2011 Global Journals Inc. (US)

[2] August

[3] Domain”, IEEE, Consumer Communications and Networking Conference (CCNC),pp.1-5,Jan2010.

Figure 1:

1 $$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Figure 2: Fig. 1 :

3 $$PSNR = 20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right)$$

Figure 3: Fig. 3 :

I

Figure 4: Table I :

2

Figure 5: Table 2 :

.1 CONCLUSION

Previously steganography was implemented using PNG images. Images contain different formats. Most widely used format is JPEG.F5 is the algorithm for JPEG steganography. In this paper it is implemented for steganography in MMS using JPEG over mobile communication. It is too much secure because data which has to be hide is encrypted first than embed in to message in both text as well as image. We can also develop the algorithm using wavelet transformation. Further study can be applied on audio steganography in MMS.

[Wu et al. ()] 'A New Steganalytic Algorithm for Detecting Jsteg'. M Wu , Z Zhu , S Jin . *Proceeding of the Network and Distributed System Symposium*, Lecture Notes in Computer Scienceon Networking and Mobile Computing (eeding of the Network and Distributed System SymposiumSanDiego,CA; Washington, D.C) 2005. 2005. February 2002. NDSS2002 Internet Society. 3619 p. . (Detecting Stegaraphic Content on the Internet)

[Wheeler et al. ()] 'A Tiny Encryption Algorithm'. R Wheeler , Needham , Tea . *Proceeding of the 1995 Fast Software Encryption Workshop*, (eeding of the 1995 Fast Software Encryption Workshop) 1995. Springer-Verlag. p. .

[Papapanagiotou et al. (2005)] 'Alternatives for multimedia messaging system steganography'. K Papapanagiotou , E Kellinis , G F Marias , P Georgiadis . *IEEE International Conference on Computational Intelligence and Security (CIS 2005), Part II*, (Xian, China) Dec. 2005. 3802 p. .

[Cachin (2004)] 'An Information -Theoretic Model for Steganography'. Cachin . *Journal of Information and Computation* July 2004. 192 (1) p. .

[Zhang et al. (2009)] 'Classification Method of Jsteg Stego Images and F5 Stego-Images'. Q Zhang , Y Liu , S Zhang , K Chen . *Fourth International Conference*, Dec 2009. p. . (Innovative Computing Information and control (ICICIC)

[Jain (1989)] *Computer Vision, Graphics and image processing*, A K Jain . June 1989. 46 p. 400. (Fundamental of digital image processing)

[Dhobale et al. (2010)] D Dhobale , S B Patil , H S Patil . *MMS Steganography for Smartphone Devices "Computer Engineering and Technology (ICCET), 2 nd International Conference*, April 2010. 4 p. .

[Cheddad et al. (2010)] 'Digital image steganography: Survey and analysis of current Methods'. A Cheddad , J Condell , K Curran , P M Kevitt . *Journal Signal Processing* March 2010. Elsevier. 90 p. .

[Hernandez et al.] 'Distinguishing TEA from a Random Permutation: Reduced Round Versions of TEA Do Not Have the SAC or Do Not Generate Random Numbers'. J C Hernandez , J M Sierra , A Ribagorda , B Ramos , J C Mex-Perera . *Proceeding of the 8 th IMA international conference on Cryptography and Coding*, (eeding of the 8 th IMA international conference on Cryptography and Coding) p. .

[Hasan Shirali et al. (1998)] 'Exploring Steganography: Seeing the unseen'. M Hasan Shirali , M Shahreza , Sirali , Shahreza . *Computer System and Applications, AICCSA, IEEE International Conference*, . N F Johnson, S Jajodia (ed.) March 2008. Feb-1998. p. . (Steganography in SMS by Sudoku puzzle)

[Westfield ()] 'F5-steganographic algorithm: High capacity despite better steganalysis'. Westfield . Lecture Notes in Computer Science 2001. Springer Verlag. 2137 p. .

[Chandramouli et al. ()] 'Image Steganography and Steganalysis: Concepts and Practice'. R Chandramouli , M Kharrazi , N Memon . *International workshop on digital watermarking, IWDW 2003*, 2004. 2939 p. .

[Petitcolas et al. (1999)] 'Information Hiding -A Survey'. A P Petitcolas , R J Anderson , M G Kuhn . *Proceeding of the IEEE*, (eeding of the IEEE) Jul 1999. 87 p. .

[Amoroso and Masotti (2006)] 'Lightweight steganography on smart phones'. M Amoroso , Masotti . *3 rd IEEE Conference on Consumer Communications and Networking*, 2006. Jan. 2006. 2 p. .

[Mohsen and Marzieh (2008)] 'Performance evaluation of a JPEG-based multipledescription image coder'. M Mohsen , A Marzieh . *Information Technology, ITSIM2008, International Symposium*, August 2008. 4 p. .

[Sarreshtedari and Ghaemmaghami] S Sarreshtedari , S Ghaemmaghami . *High Capacity Image Steganography in Wavelet*,

[Shareja ()] 'Steganography in MMS'. Shirali Shareja , M . *IEEE International Multitopic Conference*, 2007. 2007. p. .

[Shahreza et al. ()] 'Text Steganography in SMS'. M Shirali Shahreza , M H Shirali , Shahreza . *Convergence Information Technology, International Conference*, 2007. p. .