An Efficient Approach for Protecting Personal Information in IoT

Anupam Kumar Bairagi, Md. Golam Robiul Alam, Sarder Fakhrul Abedin, Ashis Talukder, Choong Seon Hong*

Kyung Hee University, Korea

Email : {anupam, robi, saab0015, ashis, cshong}@khu.ac.kr

Abstract

The number of edge devices are increasing exponentially as the emergence of Internet of Things (IoT) and Fog computing. In addition, the Bring your own device (BYOD) concept also inspires people to use personal device for storing more corporate information as well as personal information locally at the edge of the network. Hence, the utilization of personal mobile devices for storing private information is mounting significantly. As a result, protecting the privacy and security of personal information have become a major concern and hindrance towards digital engagement. In this paper, we address this issue and propose an efficient algorithm for protecting information in personal device. We apply the proposed algorithm and found the superiority of our algorithm over the robust RGB channel based technique and improved LSB based technique in perspective of data imperceptibility and capacity.

1.Introduction

'iCloud hacking' is a storm on the horizon for cloud storage since 2014. It shows us the security and privacy flaws of our personal information stored in the cloud environment. There is simply no way to be completely sure enough that the data will be secured in the cloud. Bruce Schneier, a security expert, rightly said, "you have no way of knowing. You can't trust anybody. Everybody is lying to you". Once personal information is compromised, there is no way of getting it back and may cause significant personal and financial loss.

In the era of Internet of Things (IoT) and Fog computing, a huge number of personal devices like smart phones, laptops, tablets and other smart devices are connecting to the internet for accessing different services for people's daily life. Gartner, Inc. forecasts that in 2015, there will be 4.9 billion connected things and by 2020, it will reach to 25 billion among which more than 50% are consumer devices[1]. The statistics also indicates that more than 50% of users will use tab or smartphone first for online activities by 2018[2]. This devices are increasingly getting more powerful with a large range of connectivity options and can store enormous amount of information. Alongside, with the introduction of BYOD (bring your own device) concept, the utilization of personal devices also increased. The users increasingly take advantage of smart devices for sensitive transactions like online shopping, banking, and store important personal (health record, e-mail, photo, PIN information etc) and corporate information (strategy, meeting, customer information etc) in it. This plethora makes the devices an ideal target for attackers. With the installation of third-party applications in the smart devices, the chance of malicious programs also increase that may eventually lead a system to harm's way. A report published by Kaspersky Lab [3], said that, "just two years of smartphone malware evolution are equivalent to twenty years of work in PCs malware". A report on IoT [4] finds that at least one piece of personal information is collected via the device, cloud or its mobile application by 90% of IoT devices. So security and privacy of information in smart devices is a great concern for the users.

Cryptograhy and steganography are two most used techniques in case of protecting information in communication channel. But securing communication is no longer enough as such, we need to protect our data stored on mobile devices and other endpoints. Cryptography defends against threat by stopping them from getting anything useful from the device. On the other hand, steganography protects information by hiding into a carrier without causing suspicion to the attackers. Various secure storage solutions [5], [6] exist that can be used to protect data on wireless sensor network. In [7], authors present a framework for the IoT to secure storage and communication by using cryptography.

We extend the idea of [8] for preserving the privacy and security of information that is stored in the personal smart devices with the help of steganography technique. In [8], the authors proposed an image steganography technique for secured communication of information over the internet. We have compared the performance (imperceptibility and capacity) of our proposed method with that of [8] and [9].

2. Proposed Method

The proposed protection process consists of two main operations: (i) storing the information (ii) recovering the information. The overview of the process is shown in the Fig. 1. Here both the steps use the same secret key (SK).

A. Storing Process

For storing information in the carrier, we use RGB image of (MxN), information (I) and SK with the following algorithm 1.

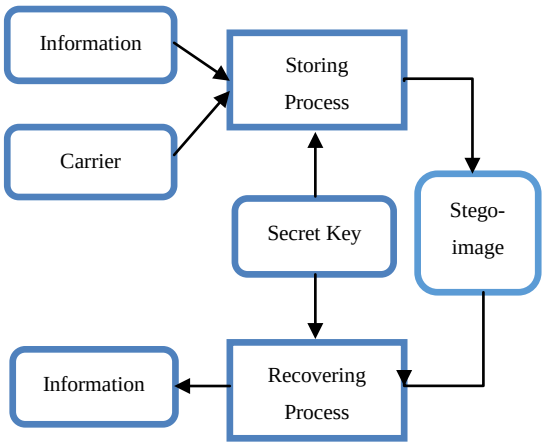


Fig. 1 Overview of the System

Algorithm 1: Information Storing

1. Set i=1, j=1, l=1and P_{ij} is a pixel of the carrier image

2.Calculate p_c=(val(P_{ij}(c))+SK- val(P_{ij}(c,1))- val(P_{ij}(c,2))) mod 6+3, c∈(1,2,3)

3.Calculate q_c=(val(P_{ij}(c))+SK- val(P_{ij}(c,1))- val(P_{ij}(c,2))+2) mod 6+3, c∈(1,2,3)

4.Set $n_1 = \sum_{c=1}^{3}(P_{ij}(c, p_c) = I(l))$ *with l=l+1 when there is equality and, c∈(1,2,3)y*

5. Set l=l-n_1 and $n_2 = \sum_{c=1}^{3}(P_{ij}(c, q_c) = I(l))$ *with l=l+1 when there is equality and c∈(1,2,3)*

6.If n_1>n_2 then indicate it using a pattern of bit in the LSBs of P_{ij}; otherwise use different pattern to indicate.

7.Set j=(j<N)?j+1:1 and i=(i<M)?i+1:M+1

8.Go to step 2 and continue until all the information is stored in the image

B. Recovering Process

For recovering information from the stego-carrier (MxN), we use same SK with the following algorithm 2.

Algorithm 2: Information Recovering

1. Set i=1, j=1, and P_{ij} is a pixel of the stego-carrier image

2.Check LSBs of the RGB channels of the pixel P_{ij} to find how many bits are stored and calculate the positions by using either p_c=(val(P_{ij}(c))+SK- val(P_{ij}(c,1))- val(P_{ij}(c,2))) mod 6+3, or q_c=(val(P_{ij}(c))+SK- val(P_{ij}(c,1))- val(P_{ij}(c,2))+2) mod 6+3, c∈(1,2,3)depending on the scenario

3.Retrive the bit(s) from channels of P_{ij} by using the positions p_c or q_c based on step 2 and store them into a memory M

4.Set j=(j<N)?j+1:1 and i=(i<M)?i+1:M+1

5.Go to step 2 and continue until all the information is retrieved from the stego-image

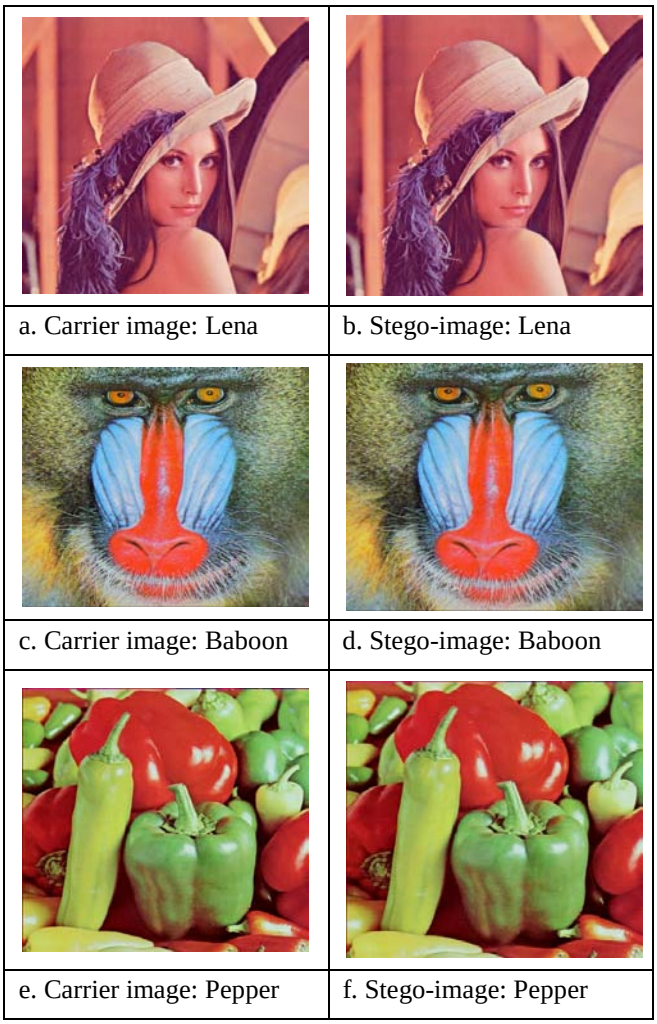
6.Separate each 8 bits and covert them into character to get the original information and store them in a file

3. Simulation and Evaluation

We have used MATLAB R2013a for storing and recovering the valuable personal information by using algorithm 1 and 2 and also to assess the proposed method. Table 1 shows the details of the experiment. The stored information and the recovered information using the algorithm 1 and 2 are the same. Generally imperceptibility, capacity and robustness are the evaluation criteria of such information storing technique. We have used peak signal-to-noise ratio (PSNR) and histogram to measure the quality (imperceptibility) of the stego-images with respect to the original carrier images and bit per pixel (BPP) to measure the capacity of the proposed method.

Table 1. Details of the experiment

Cover Image	Image Size	Hidden Data(Byte)	Capacity (Byte)	Bit Per Pixel
Lena	512X512	15,122	63,088	1.93
Baboon	512X512	15,122	64,085	1.96
Pepper	512X512	15,122	63,777	1.95



a. Carrier image: Lena | b. Stego-image: Lena

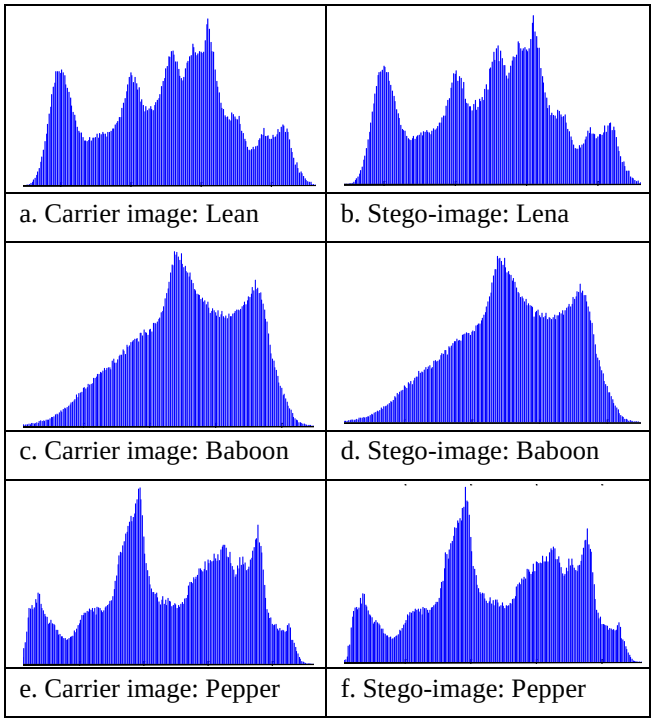
c. Carrier image: Baboon | d. Stego-image: Baboon

e. Carrier image: Pepper | f. Stego-image: Pepper

Fig. 2 Carrier images and Stego-images

From Fig. 2, one can observe that there is no visual artifact between the carrier images and the stego-images. The histogram

analysis between carrier image and corresponding stego-image is shown in Fig 3 and they are looking alike. Fig. 4 presents a comparison of PSNR values among proposed method and the methods published in [8] and [9] in case of all three images. The proposed method finds better PSNR value indicating better quality images than method [8] and [9] except Lena image for method [9].



a. Carrier image: Lean | b. Stego-image: Lena
c. Carrier image: Baboon | d. Stego-image: Baboon
e. Carrier image: Pepper | f. Stego-image: Pepper

Fig. 3 Histogram of Carrier images and Stego-images

Fig. 5 depicts the capacity of the proposed method with that of method [8] and [9]. It is measured as BPP and shows fairly better values in all the three cases rather than the methods indicated in [8] and [9] without sacrificing image quality.

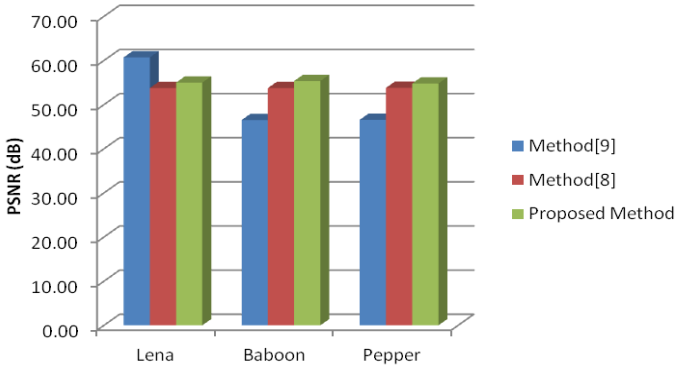


Fig. 4 Comparison of PSNR values

4. Conclusion

Protecting personal information is necessary to increase the faith to the digital system and also for pervasive adaptation of new IoT products and services. It is a critical job when we consider the whole open environment and 'iCloude hacking' is one of the examples of such security breach. Information in personal device is more vulnerable as less measures are taken to protect it. From the experiment, we show that our technique outperforms over the existing techniques in terms of imperceptibility and capacity.

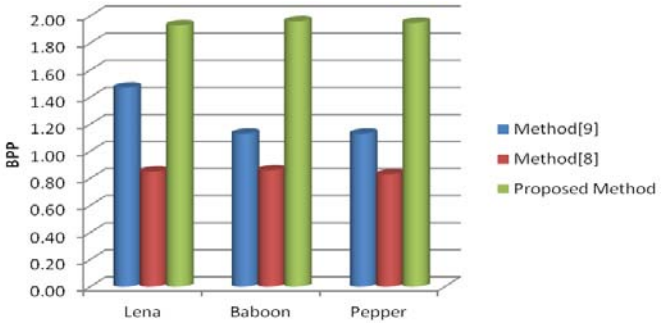


Fig. 5 Comparison of capacity

Acknowledgement

This work was supported by the Industrial Core Technology Development Program(10049079 , Development of Mining core technology exploiting personal big data) funded by the Ministry of Trade, Industry and Energy (MOTIE, Korea). *Dr. CS Hong is the corresponding author.

References

[1] A press release of Gartner, Inc. available at http://www.gartner.com/newsroom/id/2905717

[2] An article of Gartner, Inc. available at http://www.gartner.com/newsroom/id/2939217

[3] A. Gostev, “Mobile malware evolution: An overview,” Kaspersky Lab’s Report on Mobile Viruses, 2006.

[4] Report on Internet of Things Research by HP, available at www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf

[5] I. E. Bagci, M. R. Pourmirza, S. Raza, U. Roedig, and T. Voigt,“Codo: Confidential data storage for wireless sensor networks,” in 8th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS 2012), October 2012.

[6] N. Tsiftes, A. Dunkels, H. Zhitao, and T. Voigt, “Enabling large-scale storage in sensor networks with the coffee file system,” in Proceedings of the 2009 International Conference on Information Processing in Sensor Networks. IEEE Computer Society, 2009, pp. 349–360.

[7] I. E. Bagci, S. Raza, T. Chung, U. Roedig, and T. Voigt,“ Combined Secure Storage and Communication for the Internet of Things”, in 2013 IEEE International Conference on Sensing, Communication and Networking (SECON), 2013.

[8] A. K. Bairagi, S. Mondal and R. Debnath," A Robust RGB Channel Based Image Steganography Technique using a Secret Key", in 16th Int'l Conf. Computer and Information Technology, 8-10 March 2014, Khulna, Bangladesh.

[9] M. Juneja and P. S. Sandhu,"Improved LSB based Steganography Techniques for Color Images in Spatial Domain", International Journal of Network Security, Vol.16, No.6, PP.452-462, Nov. 2014.