IJMTST | Volume: 2 | Issue: 06 | June 2016 | ISSN: 2455-3778

Encrypted Data Hiding in Images by Using Reversible Side Match Logic

M. Muzammil Pravez[1] | Ch. Lakshmana[2] | B. Bhiksham[3]

[1, 2] Assistant Professor, Department of ECE, DVR & Dr HS MIC College of Technology, Kanchikacharla, Andhra Pradesh, India.
[3] PG Scholar, Department of ECE, DVR & Dr HS MIC College of Technology, Kanchikacharla, Andhra Pradesh, India.

ABSTRACT

This paper proposes a scheme for Enhanced Separable Reversible Data Hiding in Encrypted images Using Side Match. In the first step the original image is encrypted using an encryption key. Then additional data is embedded into the image by modifying a small portion of the encrypted image using a data hiding key. With an encrypted image containing additional data, if a receiver has the data hiding key, he can extract the additional data. If the receiver has the encryption key, he can decrypt the image, but cannot extract the additional data. If the receiver has both the data hiding key and encryption key, he can extract the additional data and recover the original content by exploiting the spatial correlation in natural images. The accuracy of data extraction is improved by using a better scheme for measuring the smoothness of the received image, and uses the Side Match scheme to further decrease the error rate of extracted bits.

KEYWORDS: *Encrypted image, reversible data hiding, smoothness, data extraction, side match.*

I. INTRODUCTION

Digital image processing remains a challenging domain of programming for several reasons. First the issue of digital image processing appeared relatively late in computer history, it had to wait for the arrival of the first graphical operating systems to become a true matter. Secondly, digital image processing requires the most careful optimisations and especially for real time applications. Comparing image processing and audio processing is a good way to fix ideas. Let us consider the necessary memory bandwidth for examining the pixels of a 320x240, 32 bits bitmap, 30 times a second: 10 Mo/sec. Now with the same quality standard, an audio stereo wave real time processing needs 44100 (samples per second) x 2 (bytes per sample per channel) x 2 (channels) = 176Ko/sec, which is 50 times less. Obviously we will not be able to use the same signal processing techniques in both audio and image. Finally, digital image processing is by definition a two dimensions domain; this somehow complicates things when elaborating digital filters.

The original and basic way of representing a digital coloured image in a computer's Memory is obviously a bitmap. A bitmap is constituted of rows of pixels, contraction of the words '*Picture Element*'. Each pixel has a particular value which determines its appearing colour.

II. EXISTING METHOD

Information Security: In general, security denotes "the quality or state of being secure to be free from danger". Security is classified into different layers depending on the type of content intended to be secured:

- Physical security: Defines the required issues that are needed to protect the physical data or objects from unauthorized intrusion.
- Personal security: It is defined as the security of the individuals who are officially authorized to access information about the company and its operations.

- Operational security: It mainly relies on the protection of the information of a particular operation of the chain of activities.
- Communication's security: The communication's security encompasses the security issues regarding the organization's communication media, technology and content.
- Network security: The network security is responsible for safeguarding the information regarding the networking components, connections and contents.
- Information security: Information security is the protection of information and the systems and hardware that use, store, and transmit that information. Information security can be defined as measures adopted to prevent the unauthorized use or modification of use of data or capabilities.

The main objective of the project is to propose the method and critically discuss the properties which help to transmit the data or information over a network without any modifications.

The critical characteristics of information are

1) Availability
2) Accuracy
3) Authenticity
4) Confidentiality
5) Integrity

1. Availability: It is the Prevention of unauthorized disclosure of information. It enables users who need access the information to do so without any interference or obstruction and to receive it in the required format. The availability of information requires the verification of the user as one with authorized access to information (Whitman, 2007).

In other words the availability can be defined as "Ensuring timely and reliable access to make use of information. A loss of availability is the disruption of access to or use of information or an information system.

2. Accuracy: The information is deemed accurate if it does not contain any mistakes / errors and possesses the value that end user expects. If the information holds a value different from that of the end user's expectations because of intentional or unintentional modifications of its content it becomes no longer accurate (Whitman, 2007).

3. Authenticity: Authenticity refers to the quality or state of being genuine or original. It should not be a reproduction or fabrication of any previously known data. The Information is considered authentic when it is originally created, placed, stored or transferred. In general, authenticity is ensuring that all the data remains in its original state by stopping any ways of the unauthorized modification of information (Whitman, 2007).

4. Confidentiality: "The confidentiality is the quality or state of preventing disclosure or exposure to unauthorized individuals or system". Confidentiality is basically privacy and secrecy which means protection of personal data or that of data belonging to an organization. Confidentiality of information ensures that only those with the rights and privileges access a particular set of information and prevent from unauthorized access (Whitman, 2007).

5. Integrity: It is the prevention of unauthenticated modification of data. "The quality or state of being whole, complete and uncorrupted is the integrity of information". The integrity of any data is lost when it is subjected to corruption, damage (external / internal), destruction or other disruption of its authentic state by intended or unintended sources.

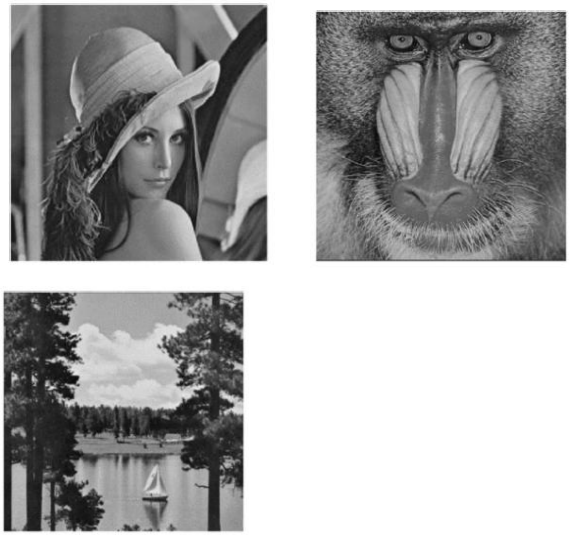

Figure1. Four test images (a)Lena (b) Baboon (c)Sailboat (d)Splash

Reversible Data Hiding in images is a technique that embeds data in digital images by altering the pixel values for secret communication, and the embedded image can be recovered to its original state after the extraction of the secret data. Many reversible Data Hiding methods have been proposed recently. One method embeds data bits by expanding the difference of two consecutive pixels. Another one uses a lossless compression technique to create extra spaces for carry data bits. Another method shifts the bins of image histograms to leave an empty bin for data embedment. Another one adopts the difference expansion and histogram shifting for data embedment. Another one embeds data by shifting the histogram of prediction errors while considering the local activity of pixels to further enhance the quality of stego-image.

Other applications could be for when the owner of the carrier might not want the other person, including data hider, to know the content of the carrier before Data Hiding is actually performed, such as military images or confidential medical images. In this case, the content owner has to encrypt the content before passing to the data hider for data embedment. The receiver side can extract the embedded message and recover the original image. For example, our method encrypts the cover image before embedding is actually performed. The cover image is encrypted by applying bitwise exclusive-or (XOR) operator to every bit of pixels using an encryption key. Let be an 8-bit cover image of size W*H and Ii, j be the pixel value at (i, j).

III. Proposed Method

In [9], the evaluation of block smoothness is crucial for obtaining a correct data extraction. However, the four borders of each block do not join the calculation of block smoothness. This may decrease the rate of correctness of data extraction, especially when the block size is small. For example, for a block of size 8X8, there are 64 pixels and around 43.75% of them (28 pixels) are located in the four borders. These border pixels are not employed to calculate the block smoothness, and the percentage is increased as the block size decreased. Besides, [9] extracts the embedded bits by evaluating the smoothness of a single block. However, flipping 3 LSBs of these complex blocks will not cause a significant increase in complexness. Based on these observations, this letter proposes an improved version for a better estimation of block smoothness. In the new smoothness estimation, the summation of the absolute of two neighboring pixels is employed. Moreover, the extraction and recovery are performed starting from the most noticeable changes in smoothness to the least ones. Besides, we also adopt the side-match technique to evaluate the block smoothness by concatenating the border of recovered blocks to the unrecovered blocks. The data encryption and data embedding process is the same as [9]. Therefore, we address only the calculation of smoothness and the process of image recovery.

IV. Conclusion

This paper proposes a scheme for Enhanced Separable Reversible Data Hiding in Encrypted images Using Side Match. We used a new algorithm to better estimate the smoothness of image blocks. The extraction and recovery of blocks are performed according to the descending order of the absolute smoothness difference between two candidate blocks. The side match technique is employed to further reduce the error rate. The experimental results show that the propose method effectively improves Zhang's method, especially when the block size is small.

References

[1] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, 2003.

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized- LSB data embedding," IEEE Trans. Image Process., vol. 14, no. 2, pp. 253–266, 2005.

[3] Z. Ni, Y. Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 8, pp. 354–362, 2006.

[4] D.M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," IEEE Trans. Image Process., vol. 16, no. 3, pp. 721–730, 2007.

[5] W. Hong and T. S. Chen, "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism," J. Vis. Commun. Image Represent., vol. 22, no. 2, pp. 131–140, 2011.

[6] D.Kundur andK.Karthik, "Video fingerprinting and encryption principles for digital rights management," Proc. IEEE, vol. 92, pp. 918–932, 2004.