Security Enhancement System through Reversible Data Embedding Technique in Encrypted Images

E. Famidha[1], G. Gajalakshmi[2], S. Devisaranya[3]

M.E Communication Systems, Department of ECE, Mailam Engineering College, India

Abstract: ***The project proposes the enhancement of security system (RDH) for secret data communication through data embedding in encrypted images. A given input image is encrypted using cryptographic technique based on selective encryption method. After image encryption, the data hider will conceal the secret data into the encrypted pixels. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the encrypted image. In the data extraction module, the secret data will be extracted by using relevant key for choosing the encrypted pixels to extract the data. By using the decryption key, the image will be extracted from encryption to get the information about the images.***

Keywords: Selective encryption, LSB replacement, Decryption key, RDH, Data Hiding

1. Introduction

In some applications, an inferior assistant or a channel administrator hopes to append some additional message, such as the origin information, image notation or authentication data, within the encrypted image though he does not know the original image content. And it is also hopeful that the original content should be recovered without any error after image decryption and message extraction at receiver side. A content owner encrypts the original image using an encryption key, and a data-hider can embed additional data into the encrypted image using a data-hiding key though he does not know the original content. With an encrypted image containing additional data, a receiver may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data-hiding key. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits (LSB) of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key.

2. Proposed Scheme

The proposed encryption and multiplexing technique not only enhances the security of confidential fingerprint information by making the information inaccessible to any interloper having a random code, but also improves the system resource utilization by reducing the storage and/or transmission bandwidth requirement. The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases.

2.1 Encryption and Data Hiding

A given input image is encrypted using cryptographic technique based on selective encryption method. After image encryption, the data hider will conceal the secret data into the encrypted pixels. The process of recovering plaintext from cipher text is called decryption. The accepted view among professional cryptographers (formalized in KIRKHOFF's law) is that the encryption algorithm should be published, whereas the key must be kept secret. A very effective method to encrypt an image, which applies to a binary image, consists in mixing image data and a message (the key in some sense) that has the same size as the image: a XOR function is sufficient when the message is only used once. A generalization to gray level images is straightforward: encrypt each bit plane separately and reconstruct a gray level image. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the encrypted image. The encryption process requires an encryption algorithm and a key. This paper introduces a new, principled approach to detecting least significant bit (LSB) steganography in digital signals such as images and audio. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision. The new steganalytic approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. The objective of steganographic is a method of embedding additional information into the digital contents that is undetectable to listeners. We are investigating its embedding, detecting, and coding techniques. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. In computing, the least significant bit (lsb) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The lsb is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digits further to the right. The least significant bit (LSB) insertion method is a simple steganographic algorithm that takes the least significant bit in some bytes of the cover medium and swaps them with a sequence of bytes containing the secret data in order to conceal the information in the cover medium. To evaluate the robustness of the proposed steganalytic approach, bounds on estimation errors are developed. Adaptive steganography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message. As the application domain of embedding data in digital multimedia sources becomes broaden, several terms are used by various groups of researchers, including steganography, digital watermarking, and data hiding. In computing, the least significant bit (lsb) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The lsb is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digits further to the right. This is as revealed by the statistical characteristics of its resultant stego images compared to the original cover images. To increase the level of imperceptibility and the hiding capacity in the LSB insertion method, this research proposes an enhanced LSB method that employs a selective and randomized approach in picking specific number of target image bits to swap with the secret data bits during the embedding process. To facilitate the selective picking of the target image bits, the standard minimal linear congruential number generator (LCG) is used. Maintaining the secrecy of digital information when being communicated over the Internet is presently a challenge. Given the amount of cheap computation power available and certain known limitations of the encryption methods it is not too difficult to launch attacks on cipher-text.

2.2 Decryption and Data Extraction

The secret data can be extracted from the embedded image with help of key matrix. The hidden encrypted pixels are determined for data extraction by using data hiding key and data will be recovered from the image. This extraction process is opposite to data embedding, pixel intensities and embedding rate are used here to extraction of data. The image also decrypted using selective method with help of key which is used in the encryption module. This paper proposes a low complexity for key generation. The image that is being recovered will be same at that of the original image. The receiver who wants information only about the data that is being embedded can get that information alone of he has only the data hiding key. It is not necessary that he should have information about the encryption key.

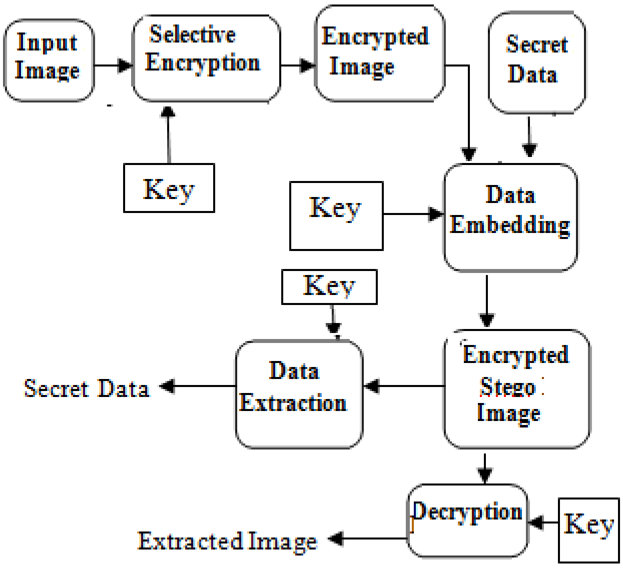
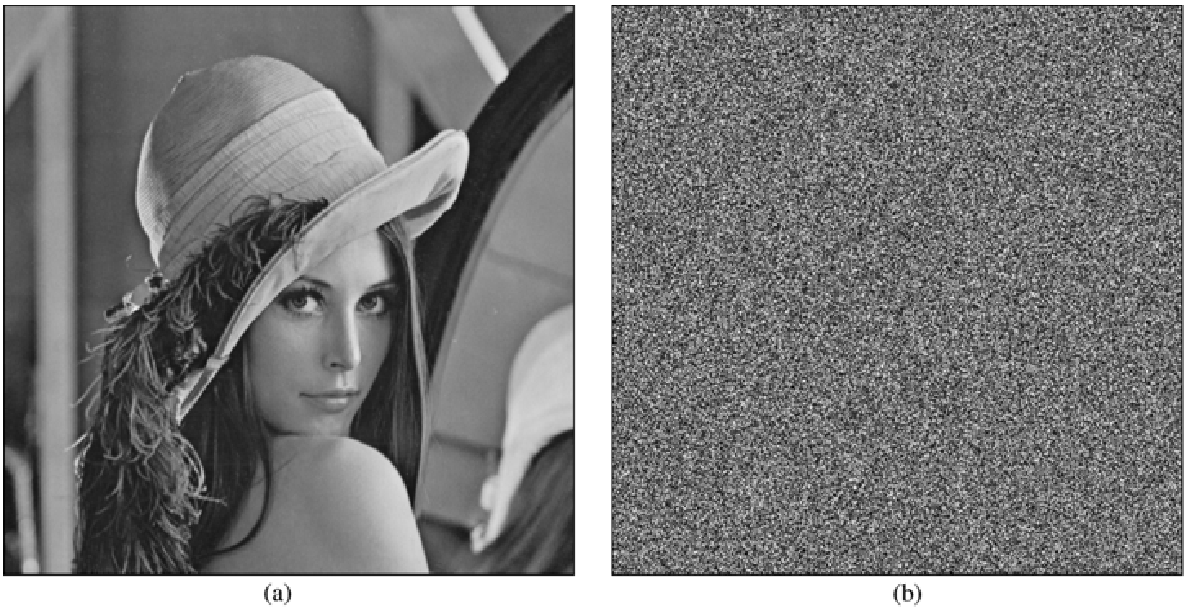


Figure 1: Encryption and Data Embedding



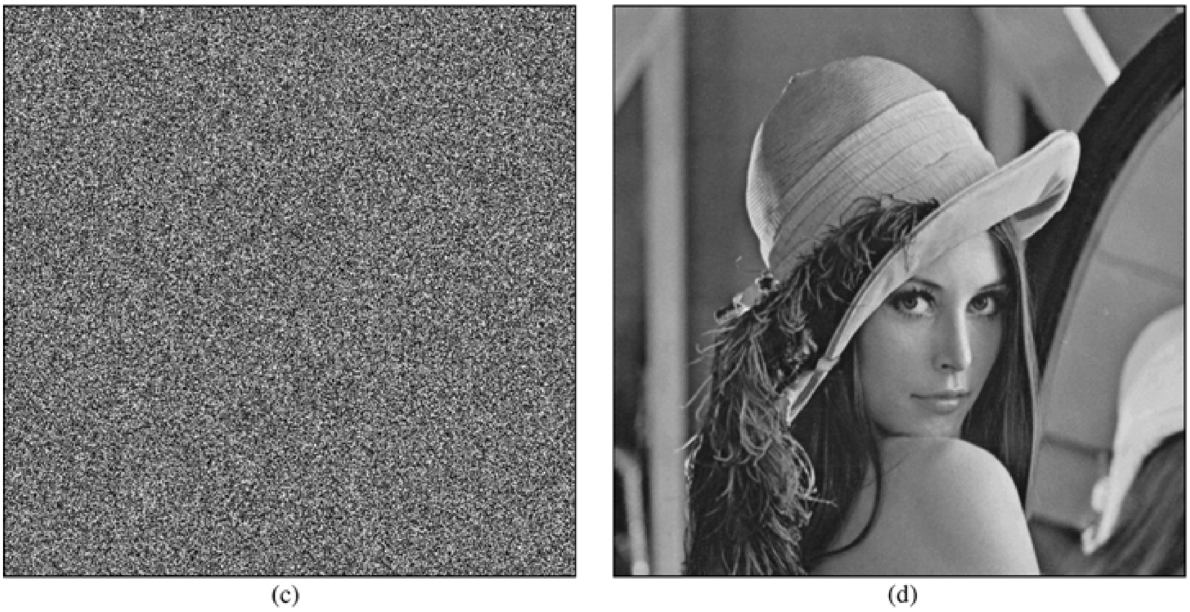


Figure 2: (a) Original Lena, (b) its encrypted version, (c) encrypted image containing embedded data and (d) directly decrypted

2.3 Quality Measures for Image

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE}=\frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right)$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

3. Conclusion

This project is of hiding a data in encrypted images. The proposed encryption technique uses the key to encrypt an image and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After image encryption, the data hider will conceal the secret data into the encrypted pixels. Then at the receiver side the user can either extract the data that has been hidden by using the data hiding key or the original image can be obtained by using the decryption key. .It does not replace cryptography but rather boosts the security using its obscurity features. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the encrypted image. By using the decryption key, the image will be extracted from encryption to get the information about the images. Then the performance parameter such as MSE and PSNR for the image is calculated. The Encryption here is done in uncompressed cover image. This encryption mechanism can also be applied in the future for lossy compressed images. The PSNR values for the recovered image can be increased since when the PSNR value is high the there will not be any difference between the original image and the recovered image.

References

[1] R.Jose, G. Abraham, "A separable reversible data hiding in encrypted image with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy, 2013 Annual International conference on June 2013.

[2] C.Rengarajaswamy, K. Velmurugan, "Separable extraction of concealed data and compressed image", Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication system, Jan 2013.

[3] Xinpeng Zhang, "Seperable Reversible Data Hiding in Encrypted images", IEEE *Trans. Information Forensics And Security*, Vol. 7, no. 2, April 2012.

[4] R.Manikandan, M. Uma, S M. MahalakshmiPreethi, "Reversible Data Hiding for Encrypted Image", Journal of computer Application ISSN: 0974-1925, Volume-5, Issue E1CA2012-1, February 10, 2012.

[5] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," *Signal Processing:ImageCommun.*, vol. 26, no. 1, pp. 1–12, 2011

[6] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[7] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE*

Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010

[8] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," *IEEE Trans.Inform. Forensics Security*, vol. 5, no. 1, pp. 180–187, Feb. 2010.

[9] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inform. Forensics Security*, vol. 4, no. 1, pp. 86–97, Feb. 2009.

[10] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in *Proc. 11th ACM Workshop Multimedia and Security*, 2009, pp. 9–18.

[11] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative encryption and Watermarking in video compression," *IEEE Trans. Circuits Syst. VideoTechnol.*, vol. 17, no. 6, pp. 774–778, Jun. 2007.

[12] M. Kuribayashi and H. Tanaka, "Fingerprinting protocol for images based on additive homomorphic property", *IEEE, Trans. Image Process*. Vol. 14, no.12,pp. 2129-2139,Dec 2005

[13] 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, Feb. 2005.

[14] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," *IEEE Trans. SignalProcess.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.

[15] N. Memon and P. W. Wong, "A buyer-seller watermarking protocol,"*IEEE Trans. Image Process.*, vol. 10, no. 4, pp. 643–649, Apr. 2001.