International Journal of Advanced Computer and Mathematical Sciences
ISSN 2230-9624. Vol 5, Issue4, 2014, pp84-87
http://bipublication.com

An Efficient and Lossless Separable Reversible Data Hiding in Encrypted Images

S. Monisha, M. A. Muthiah and Tharun kumar.

Departmentof ECE,

Sathyabama University, India

[Received-16/07/2014, Accepted-15/09/2014]

ABSTRACT:

In most image data hiding methods the host image is permanently distorted and it cannot be restored from the marked content. A method called Reversible data hiding (RDH) in which the host image can be fully restored after data embedding. Histogram shifting is one of the efficient reversible data hiding technique. A RDH algorithm is obtained by simply designing the shifting and embedding functions. Here an RC4 cryptographic algorithm is used to convert the input text into a cipher text and an encoder is used to compress the encrypted data. The compressed data is embedded into the image by histogram shifting. An LFSR is used to generate random values which are used to select the regions randomly in order to increase the security level. The proposed system is implemented with Verilog HDL and simulated using MODELSIM to verify the functionality of MATALAB processed digital image and PSNR (dB) value of the reconstructed image is obtained.

Keywords- Steganography, linear feedback shift register (LFSR), LSB

[I] INTRODUCTION

In recent years hiding data has resulted in a growth of Steganography. The rapid growth in publishing and broadcasting technology also demands an alternative solution in information hiding.The copyright of digital media such as audiovisual and other media in digital form are more prone to illegal copying. This is because the digital formats provide high resolution under various copying conditions. Steganography is the art of science of hiding information by embedding the secret messages within other, seemingly harmless messages. As the goal of Steganography is to hide the presence of a message and to create a covert channel, where the same concept is complemented as cryptography, in which content is hidden.

Reversible data hiding (RDH) in images is a technique, by which the real image can be recovered after the hidden message is extracted. This technique is used in law forensics, military imagery and medical imagery where no distortion of the original image is allowed.

[II] REVERSIBLE DATA HIDING

Reversible data hiding [1,2], also known as lossless data hiding, enables marked media to be restored to their original form without any distortion. This technique is applied in fields such as content authentication of multimedia data, law enforcement, medical imagery and

astronomical research. Many reversible data hiding methods have been proposed mostly for grayscale images. In [3], the least significant bit (LSB) plane is obtained so that there is additional space for embedding the secret data. Compressing the quantization residuals of pixels yields to additional space to embed a message. In [4], a method is presented that expands the difference between two neighboring pixels to obtain redundant space for embedding a message. Here the difference between a pixel and the mean value of its neighboring pixels to embed a message.

2.1Implementation of LFSR

As mentioned previously more peaks yield larger data hiding capacities. In [6], the number of pixels constituting the peak in the histogram of a cover image is equal to the data hiding capacity because only a single peak in a cover image is used. In [7], the cover image is divided into blocks so as to generate a respective peak for each block.This technique successfully enhances the data hiding capacity because the total data that can be hidden in multiple blocks is generally larger than that can be hidden in a single cover image as mentioned previously. Furthermore, the peak location in the histogram indicates generally that a great number of pixels are gathered in the neighbor area around the peak point. For this reason, in [8] they have used the two neighboring points beside the peak point to embed the data.

[III] STEGANOGRAPHY

In modern world, information is converted from paper type to digital information. Hence improving security in data saving and exchanging is very important. Different techniques of cryptography are used for data encryption but all of these methods can be identified by invaders. If the information can be embedded in a medium in such a way that it cannot be identified easily, it will not raise any hunch for the invaders. This is the main idea of Steganography. The image formats used in such steganographical methods are lossless and the data can be directly manipulated and recovered. The bmp images use lossless compression one form of LSB attempts to use bmp images. However, other image formats are used as cover image as well.

RC4 was originally very widely used due to its simplicity and speed. For stronger encryption 16 byte keys are used, but shorter key lengths are also widely used due to export restrictions. Over time this code was shown to produce biased outputs under certain sequences in first few bytes of the key stream generated. RC4 encryption, you need a key, which is often user-defined and between 40-bits and 256-bits. The 40-bit key indicates a five character ASCII code that gets translated into its 40 character binary equivalent.

Key-scheduling algorithm

```
for i from 0 to 255
S[i] := i
end for j := 0
for i from 0 to 255
j := (j + S[i] + key[i mod keylength])
 mod 256
swap(S[i],S[j])
end
```

The number of iterations performed is the key length, and each value of S is traded at least once beyond 256 iterations

3.1Algorithm-Data embedding process.

Input: a cover image I divided into blocks with size M x N, and a message M in bit string form to be embedded with random key for RC4 encryption.

Output is a stego-image I' with M embedded, key K in the form of an integer number sequence.

3.2 Security enhancement

To enhance the security level, many data hiding methods make use of the keys to control the data extraction process [14-15]. In general, data are embedded into the cover medium in a specific order which is determined by the key. A key is usually constructed by meaningless numbers, and behaves as a seed for a random number generator which produces a series of numbers to specify the data embedding order. In this study, we use differently a scheme of forming the key by the block division

information yielded by the method, as done in Algorithm.

In addition, about the generated location map, its size will depend on the numbers of pixels with values 0 and 255 existing in the test image. In the test images selected randomly for use in our experiments, the sizes of the text that used to be embedded are varying. But if other images are used, the sizes of the maps might not be fixed. Generally, pixels with extreme values 0 and 255 are limited in number in most of the images, and for common images the proposed method will yield location maps of small sizes.

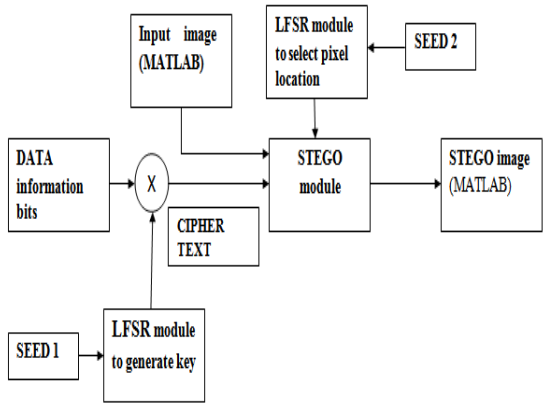

Fig.1. Block diagram of proposed Steganography method in functional mode.

[IV] DISTORTION ANALYSIS

Step 1: The input image is saved as text file and it is read in digital form using modelsim. The image is divided into blocks and is stored in memories RAM1 and RAM2.

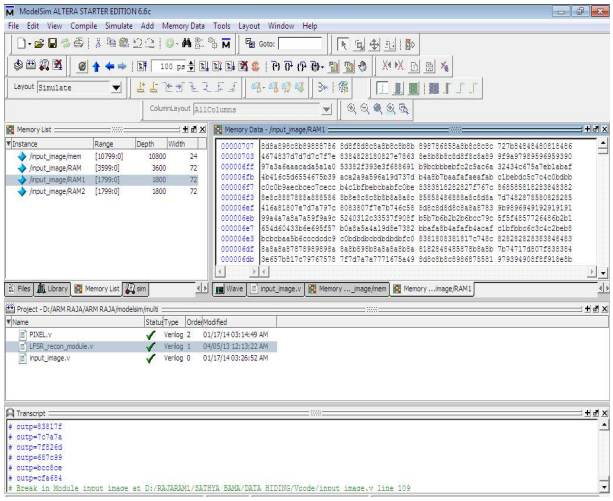

Fig 2: Digitized form of Input Image

Step 2: In pre phase the input data (text) is converted into cipher text using RC4 encryption algorithm and then it is embedded into the image in the post phase the cipher text is retrieved from the image and it is decrypted using RC4 algorithm.

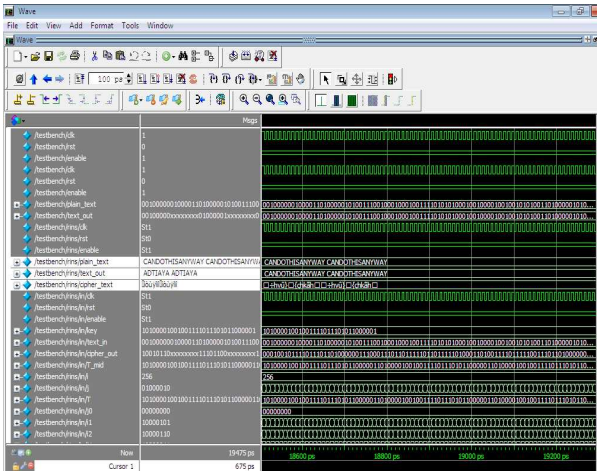

Fig 3: RC4 Simulated Output

Step 3: The LFSR is used to randomly select the blocks in the image for hiding the data according to the seed value given.

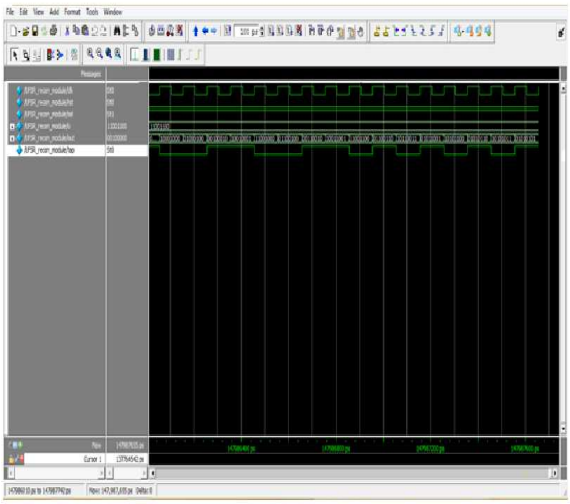

Fig 4: Simulated LFSR output

Step 4: The images can be distorted in embedding process because of changing pixel bits. The performance of each method was tested using a 512×512 grayscale image as a cover image and part of a 512×512 grayscale image as secret data. Distortion is measured by means of two parameters namely, Mean Square

Error (MSE) and Peak Signal to Noise Ratio (PSNR).

MSE can be calculated by,

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - Y_{ij})^2$$

The PSNR is calculated using,

$$PSNR = 10log_{10}\left\{\frac{i^2 max}{MSE}\right\}db$$

Imax is the maximum intensity value of each pixel which is equal to 255 for 8 bit gray scale images. Higher value of PSNR leads to better image quality. The size of these images is 256*256 pixels.

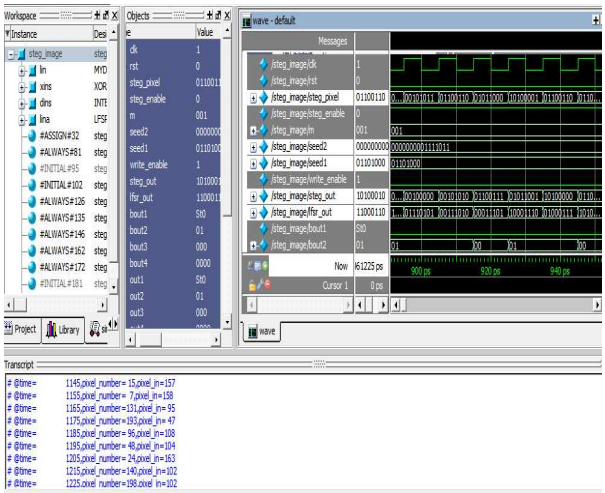

Fig 5: Simulated output for proposed stenography method

Fig 6: STEGO image with PSNR value

As shown here, message embedding is done with no dramatic changes in image quality.

The area utilization report, the timing analysis report and the frequency estimation summary are obtained using QUARTUS II tool

[V] CONCLUSION

The proposed technique is highly efficient because, it increases the security levels of the transmitted data and it also increases the embedding capacity. The proposed system is implemented with Verilog HDL and simulated using MODELSIM to verify the functionality of MATALAB processed digital image and PSNR (dB) value of the reconstructed image is obtained.

REFERENCES

1. A. P. Chandrakasan, N. Verma, and D. C. Daly, “Ultra low power electronics for biomedical applications,” Annual Review of Biomedical Engineering, vol. 10, pp. 247-274, August 2008.
2. L. Mateu and F. Moll, “Review of energy harvesting techniques and applications for microelectronics,” Proc. SPIE Microtechnologies for the New Millennium, pp. 359-373, 2005.
3. V. Raghunathan and P. H. Chou, “Design and power management of energy harvesting embedded systems,” Proc. International Symposium on Low Power Electronics and Design, pp. 369-374, 2006.
4. C. Lu, S. P. Park, V. Raghunathan, and K. Roy, “Efficient power conversion for ultra low voltage micro scale energy transducers,” Proc. Design, Automation and Test in Europe, pp. 1602-1607, 2010.
5. OptobionicsCorp. (http://optobionics.com/)
6. For other image processing references
7. [6] C. Lu, V. Raghunathan, and K. Roy, “Maximum power point considerations for micro-scale solar energy harvesting systems,” Proc. International Symposium on Circuits and Systems, pp. 273-276,2010.
8. [7] E. Esram and P. L. Chapman, “Comparison of photovoltaic array maximum power point tracking techniques,” IEEE Transactions on Energy Conversion, vol. 22, no. 2,
9. pp. 439-449,June