ISSN 2319 – 2518 www.ijeetc.com
Vol. 2, No. 2, April 2013

Research Paper

INFORMATION HIDING METHOD USING JPEG2000 BASELINE

Nayab Rasool[1]* and G Gouri Sankar Reddy[1]

**Corresponding Author: Nayab Rasool,* ✉ *lifesgood497@gmail.com*

In this paper, JPEG2000 compression will be used to embedding and extracting of cover image and secret image. For this purpose, redundancy evaluation method will be used to increasing the hiding capacity. In this redundancy evaluation method, large amount of data will be embedded with slightly change in Peak Signal to Noise Ratio (PSNR). In this JPEG2000, there are two algorithms will be used, i.e., secret message embedding algorithm and secret message extraction algorithm. Simulation shows that the proposed method is feasible, effective, and secure.

Keywords: Secret communication, JPEG2000, Data hiding, Information security, EBCOT encoder

INTRODUCTION

Modern information hiding technology is an important branch of information security. Now a days information hiding keeps major role in all security purpose. So while designing such a system we keep on some characteristics such as capacity, security. Capacity means how much of payload it can be stored and security means how those payload will be keeping undetectable and invisible. For this, in image processing there are many compression systems.

Least Significant Bits (LSB) Method: It is one of the compression methods used in image processing. In this method the secret which can be embedded into least significant bit levels of cover image or host image. Here the coefficients are in discrete cosine transform type.

JPEG Coding: In JPEG coding system, modified DCT coefficients can be used for embedding process. So the coefficients will be just varied from LSB substitution method.

OUR METHOD

In this paper I can use JPEG2000 compression system. In this compression system we can use two images, one is host or

[1] ECE Department, SV University College of Engineering, Tirupathi, AP, India.

cover image and second one is secret image. Host or cover image is the image where the watermark has to be embedded. Generally cover images can be taken as standard images. Compared to cover image, secret image is the low information image and in our process this secret image can be embedded in cover image and produces watermarked image.

There are two algorithms which can be used in JPEG2000 for embedding and extracting secret images. Those are:

- Secret message embedding algorithm.
- Secret message embedding algorithm.

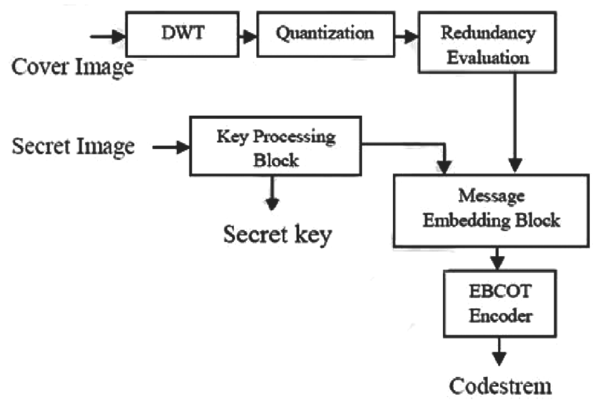
Secret Message Embedding Algorithm

The block diagram of secret message embedding algorithm is shown in Figure 1. The image where the watermark is to be embedded is called the host image or cover image.

Discrete Wavelet Transform

By using discrete wavelet transform, the cover image can be divided into different sub bands. These sub bands will be encoded by using MQ encoder. After this encoding EBCOT encoder will produces finely embedded bit stream.

Figure 1: Secret Message Embedding Block Algorithm



Quantization

Quantization is used for purpose of quantizing the cover image and assign discrete gray level values to that quantized levels.

Redundancy Evaluation

Redundancy evaluation method will be used to remove the unwanted information in the secret image. This will be based on visual masking and brightness sensitivity of human visual system.

Key Processing Block

In this block the secret key will be used to encoding of secret image into cover image for embedding process. The secret message must be divided into small fragments before it is embedded into number of code blocks of a cover image. Some kind of predefined synchronization information is necessary for accurately extraction of the hidden message.

$$\textit{Encrypted Data} = m_i \oplus n_i \qquad ...(1)$$

Message Embedding Block

In this section, message will be embedded into quantized wavelet coefficient and threshold is assigned for embedding process. The wavelet coefficients which will be greater than threshold can be considered as candidate embedding point. Mathematically it can be calculated as.

$$\textit{Threshold} = 2^n$$

where $n = 4, 5, 6, 7$ ...(2)

Embedded Block Coding and Optimized Truncation (EBCOT) Encoder

There are three coding passes are used in EBCOT encoder for encoding purpose:

1) Significance propagation pass; 2) Magnitude refinement pass; 3) Clean-up pass. These three coding passes are used for encoding purpose. Final output of this EBCOT encoder block is one dimensional code stream.

Secret Message Extraction Algorithm

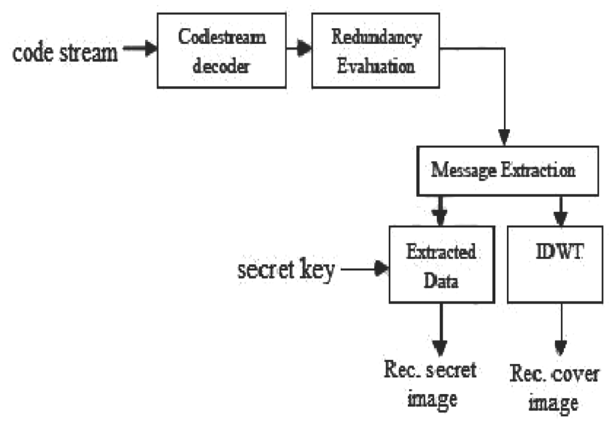
Extraction process is simply inverse process to that of embedding process. The block diagram of secret message extraction algorithm is shown in Figure 2.

Code stream is the input for secret message extraction algorithm. Output of the code stream decoder is sub bands. After code stream decoder redundancy is to be evaluated as described in secret message embedding algorithm. By using quantization redundancy matrix r_i secret bits are extracted from sub bands. So the original secret image recovered by using:

$$m_i = \textit{Encrypted Data} \oplus n_i \qquad ...(3)$$

where m_i a recovered secret is image and n_i is encryption key. Encryption key used at embedding operation and extraction operation are same. Inverse Discrete Wavelet Transform (IDWT) is used for recovering cover image.

Figure 2: Secret Message Extraction Algorithm



RESULTS AND DISCUSSION

In this paper, the cover image can be taken be taken as Lena with gray scale of 512 × 512, and secret image can be taken as GIKI which is 80 × 80 binary image with a pixel depth of just one bit. Therefore, there are 6400 bits of secret message in total shown in Figure 3. By using secret message embedding algorithm, the secret image can be embedded into cover image and the water marked image is shown in figure.

Similarly, by using secret message extraction algorithm, the secret image can be extracted from cover image. Simulation results shows that the original cover image, i.e., Lena image and secret image GIKI and recovered Lena image and GIKI image will be same indicates that there is no loss of information. By comparing the two original and reconstructed images, the block colour indicates there is no loss of information. That means by using this JPEG2000 more amount of information will be embedded with small amount of change in Peak Signal to Noise Ratio (PSNR).

Here Figures 3a and 3b shows that the standard lena image as original cover image and secret image and Figure 4 shows that the watermarked image which is the embedded image of both cover and secret image and finally Figures 5a and 5b shows the reconstructed cover image and secret image respectively.

Similarly for barbara

Similarly Figures 6a and 6b shows that the standard barbara image as original cover image and secret image and Figure 7 shows that the watermarked image which is the

Figure 3: (a) Lena Image Used as Cover Image, (b) The Binary Logo Image Used as Secret Message

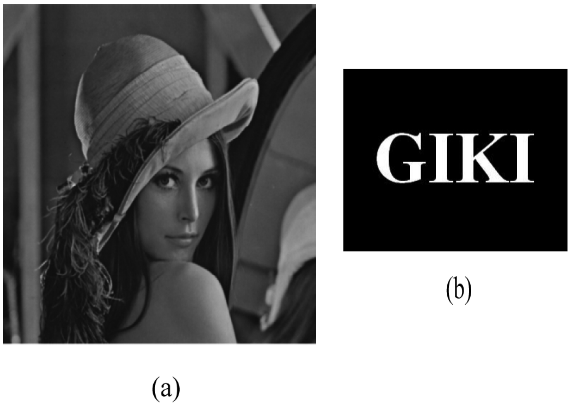


Figure 4: Watermarked Image

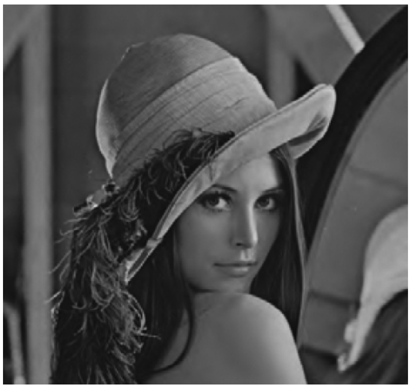


Figure 5: (a) Reconstructed Original Cover Image, (b) Reconstructed Secret Image

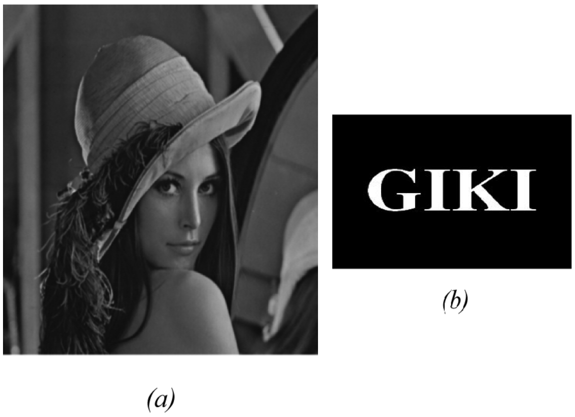


Figure 6: (a) Barbara Image Used as Cover Image, (b) The Binary Logo Image Used as Secret Message

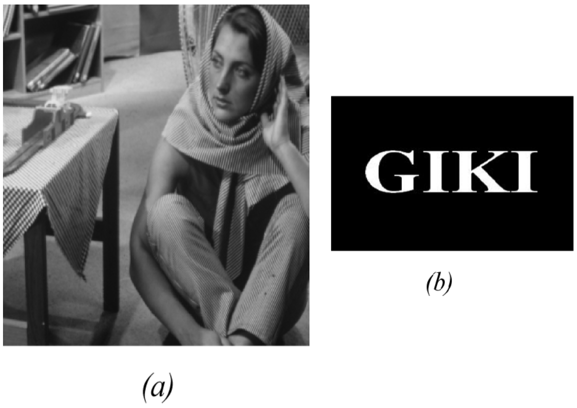


Figure 7: Watermarked Image

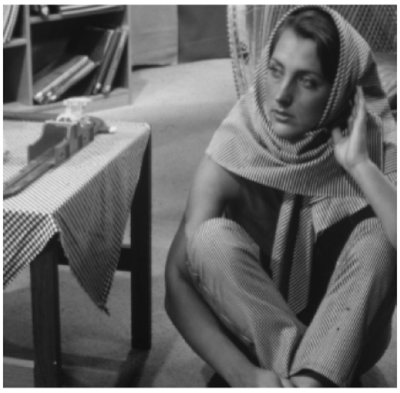
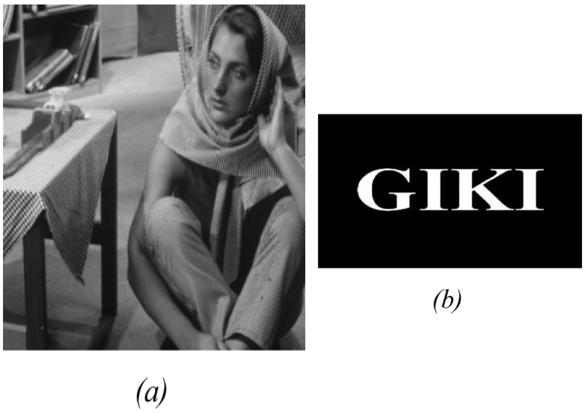


Figure 8: (a) Reconstructed Original Cover Image, (b) Reconstructed Secret Image



embedded image of both cover and secret image and finally Figures 8a and 8b shows the reconstructed cover image and secret image respectively. So the same results will be obtained for boat, bridge, peppers and Elaine also.The below Table 1 shows the data-to-watermark ratio of different standard images.

Table 1: Data-to-Watermark Ratio (DWR) in db and Resulting PSNR (db) for the Test Images

DWR	PSNR (db)					
	Lena	Elaine	Barbara	Boat	Bridge	Peppers
16	48.40	51.66	48.70	46.50	46.83	47.30
20	51.86	53.96	51.03	50.19	50.45	51.76
24	52.38	58.76	52.69	51.77	52.96	53.30

CONCLUSION

By using JPEG2000 compression system, the embedding capacity will be more with slight change in peak signal to noise ratio and also redundancy evaluation method gives more results than non-redundancy evaluation method. So finally simulation results shows that this method is secure and increasing hiding capacity.

REFERENCES

1. Arjun Nichal and Shraddha Deshpande (2012), “A High Capacity Data Hiding Method Using JPEG2000 Compression System”, Vol. 2, pp. 751-755.
2. Chan C K and Cheng L M (2004), “Hiding Data in Images by Simple LSB Substitution”, *Pattern Recognit.*, Vol. 37, No. 3, pp. 469-474.
3. Chang C C, Chou Y C and Kieu T D (2007), “High Capacity Data Hiding for Gray Scale Images”, in Proc. 1st Int. Conf. Ubiquitou Information Management and Communication, February, pp. 139-148, Seoul, Korea.
4. Farid H (2002), “Detecting Hidden Messages Using Higher-Order Statistics Models”, in Proc. EEE Int. Conf. Image Processing, pp. 905-908, New York.
5. Fridrich J and Goljan M (2002), “Practical Steganalysis of Digital Images State of the Art”, in Proc. SPIE, Vol. 4675, pp. 1-13.
6. Gilani S A M, Kostopoulos I and Skodras A N (2002), “Color Image-Adaptive Watermarking”, in Proc. 14th Int. Conf. Digital Signal Processing, Vol. 2, pp. 721-724.
7. Holotyak T, Fridrich J and Voloshynovskiy S (2005), “Blind Statistical Steganalysis of Additive Steganography Using Wavelet Higher Order Statistics”, Presented at the 9th IFIP TC-6 TC-11 Conf. Communications and Multimedia Security.
8. JPEG2000 Part 1: Final Committee Draft Version 1.0, ISO/IEC. FCD 15444-1, 2000.
9. JPEG2000 Part 2: Final Committee Draft, ISO/IEC FCD 15444-2, 2000.
10. Westfeld A and Pfitzmann A (2000), “Attacks on Steganographic Systems”, in *Lecture Notes in Computer Science*, Springer-Verlag, Vol. 1768, pp. 61-75, Berlin, Germany.