Reserve room technique for reversible data hiding

Dr.M.Anto Bennet[1], G.Sankar Babu[2]& S.Natarajan[3]
[1]Professor, Department of ECE, VELTECH, Chennai-600062
[2]Assistant ProfessorDepartment of ECE, VELTECH, Chennai-600062
[3]Assistant ProfessorDepartment of EEE, VELTECH, Chennai-600062
***Corresponding author: E.Mail:bennetmab@gmail.com**

ABSTRACT

The paper presents the enhancement of data protection system for secret communication through common network based on reversible data concealment in encrypted images with reserve room approach. The Blue plane will be chosen for hiding the secret text data. The image is then separated into number of blocks locally and lifting wavelet will be used to detect approximation and detailed coefficients. The approximation part is then encrypted using chaos encryption method. 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 detailed coefficients which are reserved before encryption. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using a symmetric key method. This is the reason a new security approach called reversible data hiding arises. The data hiding technique uses the adaptive 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 keys, the image and extracted text data will be extracted. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery.

Key words: Discrete Wavelets Transform, Encryption, Decryption,Image embedding Methods

INTRODUCTION

Over the past several years, the wavelet transform has gained widespread acceptance in signal processing in general and in image compression research in particular. In applications such as still image compression, discrete wavelets transform (DWT) based schemes have outperformed other coding schemes like the ones based on DCT. Since there is no need to divide the input image into non-overlapping 2-D blocks and its basis functions have variable length, wavelet-coding schemes at higher compression ratios avoid blocking artifacts. Because of their inherent multi -resolution nature, wavelet-coding schemes are especially suitable for applications where scalability and tolerable degradation are important. Recently the JPEG committee has released its new image coding standard, JPEG-2000, which has been based upon DWT. Basically we use Wavelet Transform (WT) to analyze non-stationary signals, i.e., signals whose frequency response varies in time, as Fourier Transform (FT) is not suitable for such signals.To overcome the limitation of FT, Short Time Fourier Transform (STFT) was proposed. There is only a minor difference between STFT and FT. In STFT, the signal is divided into small segments, where these segments (portions) of the signal can be assumed to be stationary. For this purpose, a window function "w" is chosen. The width of this window in time must be equal to the segment of the signal where it is still be considered stationary. By STFT, one can get time-frequency response of a signal simultaneously, which can’t be obtained by FT. The short time Fourier transform for a real continuous signal is defined as:

$$X\,(f,t) = \int_{-\infty}^{\infty} [x(t)w\ \ (t-\tau)^{*}]e^{-2j\pi ft}dt \text{ --------} \qquad (1)$$

Where the length of the window is (t-τ) in time such that we can shift the window by changing value of t and by varying the value τ we get different frequency response of the signal segments. The Heisenberg uncertainty principle explains the problem with STFT. The wavelet transform (WT) has been developed as an alternate approach to STFT to overcome the resolution problem. The wavelet analysis is done such that the signal is multiplied with the wavelet function, similar to the window function in the STFT, and the transform is computed separately for different segments of the time-domain signal at different frequencies. This approach is called Multi-resolution Analysis (MRA) [4], as it analyzes the signal at different frequencies giving different resolutions. MRA is designed to give good time resolution and poor frequency resolution at high frequencies and good frequency resolution and poor time resolution at low frequencies. This approach is good especially when the signal has high frequency components for short durations and low frequency components for long durations, e.g., images and video frames.The wavelet transform involves projecting a signal onto a complete set of translated and dilated versions of a mother wavelet Ψ(t). The strict definition of a mother wavelet will be dealt with later so that the form of the wavelet transform can be examined first. For now, assume the loose requirement that Ψ(t) has compact temporal and spectral support (limited by the uncertainty principle of course), upon which set of basic functions can be defined. LWT decomposes the image into different subbands images, namely, LL, LH, HL, and HH for embedding the messages in the pixel coefficients of subbands. Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information. LL subbands contains the significant part of the spatial domain image. High-frequency sub band contains the edge information of input image. These coefficients are selected as reserved space foe hiding the text data. The secret text data is embedded into the wavelet coefficients of high frequency subbands because it is non sensitive to human visual system. The basis set of wavelets is generated from the mother or basic wavelet is defined as:

$$\Psi_{a,b}(t) = \frac{1}{\sqrt{a}}\,\psi\left(\frac{t-b}{a}\right);\ a, b \in \Re \text{ and } a > 0 \quad \text{------------ (2)}$$

The variable ‘a’ (inverse of frequency) reflects the scale (width) of a particular basis function such that its large value gives low frequencies and small value gives high frequencies. The variable ‘b’ specifies its translation along x-axis in time. The term $1/\sqrt{a}$ is used for normalization.

PROPOSED METHOD

The paper proposes the enhancement of protection system for secret data communication through encrypted data concealment in encrypted images with reserve room approach. To preserve an image quality during image recovery, reserving room approach is used to reserve space for embedding a privacy text messages (shown in fig 1).Here, chaos encryption is used to scramble an image except reserved space to make protection of image details during transmission. After an encryption, the data hider will conceal the encrypted secret data into the reserved coefficients using adaptive LSB replacement algorithm. Finally, image and hidden text will be recovered without any loss based same methods which are used at embedding stage shown in fig 2.

Encryption and Embedding

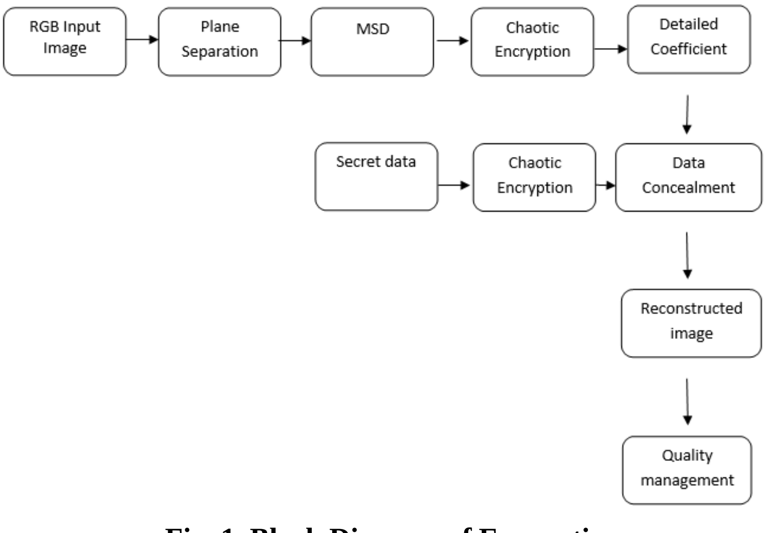

Fig. 1. Block Diagram of Encryption

Decryption and Data Extraction

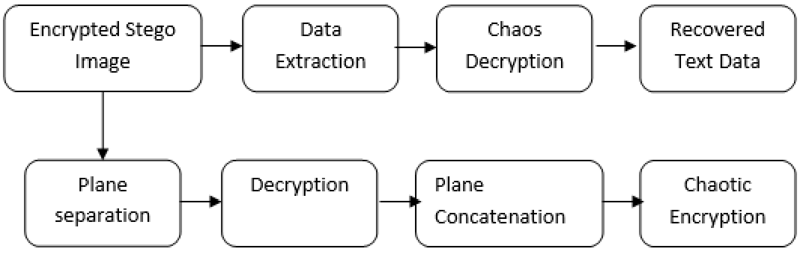

Fig. 2. Block Diagram of Decryption

2-D TRANSFORM HEIRARCHY

The 1-D wavelet transform can be extended to a two-dimensional (2-D) wavelet transform using separable wavelet filters. With separable filters the 2-D transform can be computed by applying a 1-D transform to all the rows of the input, and then repeating on all of the columns shown in fig3.

LL1	HL1
LH1	HH1

Fig.3.Sub-bands Labeling Scheme for a one level, 2-D Wavelet Transform

LIFTING WAVELET COMPUTATION

In order to obtain an efficient wavelet computation, it is important to eliminate as many unnecessary computations as possible. A careful examination of the forward and reverse transforms shows that about half the operations either lead to data which are destroyed or are null operations (as in multiplication by 0). The one-dimensional wavelet transform is computed by separately applying two analysis filters at alternating even and odd locations. The inverse process first doubles the length of each signal by inserting zeros in every other position, then applies the appropriate synthesis filter to each signal and adds the filtered signals to get the final reverse transform.

Decomposition Flow:

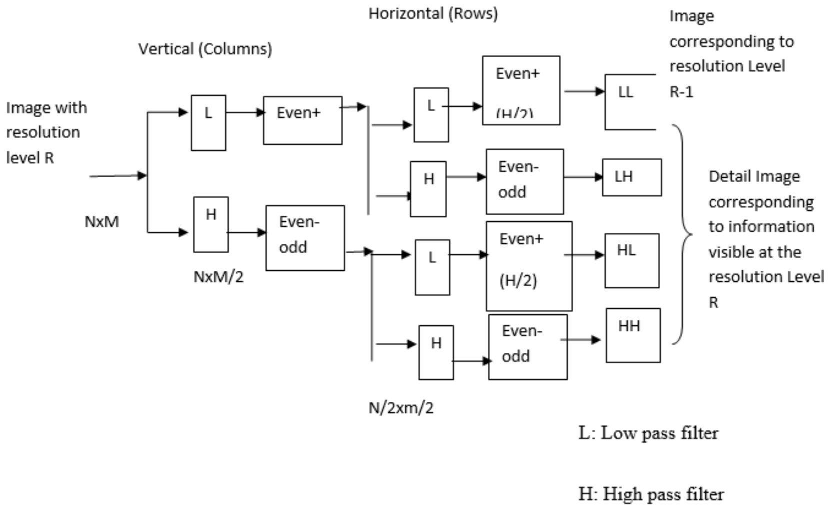

Fig.4.Decomposition Flow

Forward transform

Step1: Column wise processing to get H and L (Fig 4)

H = (Co-Ce); L = (Ce+*H*/2)

Where Co and Ce is the odd column and even column wise pixel values

Step 2: Row wise processing to get LL,LH,HL and HH, Separate odd and even rows of H and L,

Namely, Hodd – odd row of H, Lodd- odd row of L, Heven- even row of H

Leven – even row of L

LH = Lodd-Leven; LL = Leven + (*LH* / 2)

HH = Hodd – Heven; HL = Heven + (*HH* /2)

IMAGE ENCRYPTION- Chaos Crypto system

This method is one of the advanced encryption standard to encrypt the image for secure transmission. It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit xor operation Here logistic map is used for generation of chaotic map sequence .It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking. The chaotic systems are defined on a complex or real number space called as boundary continuous space. Chaos theory generally aims that to recognize the asymptotic activities of the iterative progression (Wei *et al.*, 2006) The properties essential for chaotic systems designed for cryptography is sensible to an initial condition with topology transitivity (Hermassi*et al.*, 2010) is shown in fig 5.

Chaotic Encryption Scheme:

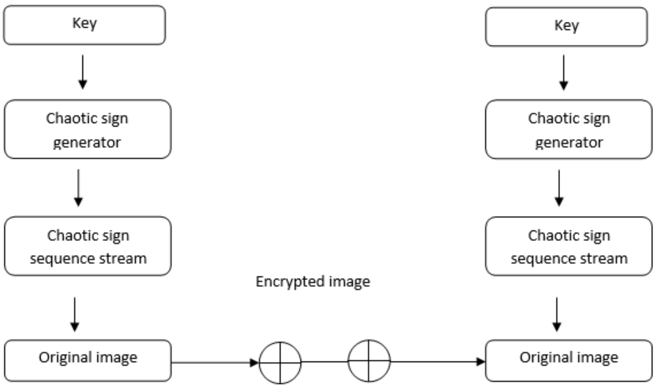

Fig.5.Chaotic Encryption Scheme

The broad chaos encryption method is the simplest technique to encrypt video data or message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security.. Identical trajectory only can produce the same values. The topology transitivity defines that the state points reside in a bounded space state and approaches.The chaotic encryption method is proposed by (Baptista, 1998). It seems to be a much better encryption algorithm than traditional algorithms were used. We first identify the mapping scheme for a trajectory to encrypt the message. Subsequently decide the initial state and parameters for the key. We assume the initial condition as the current route (trajectory). Iterate the chaotic equation until the path reaches the target site and then store the amount of iterations as a code for each message symbol. Encrypt the next message by iterating the recent trajectory. Produce the next cipher according it and so on.

Process Flow

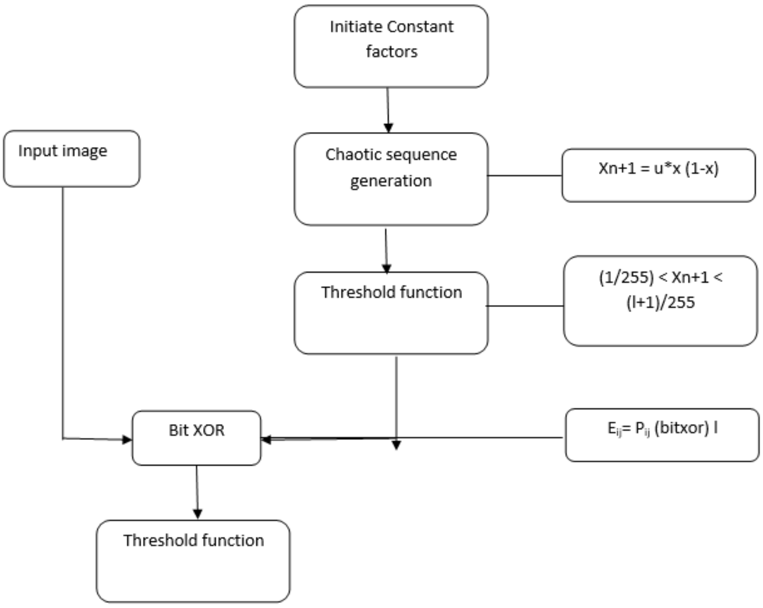
Initiate Constant factors
Input image
Chaotic sequence generation
Xn+1 = u*x (1-x)
Threshold function
(1/255) < Xn+1 < (l+1)/255
Bit XOR
E_{ij}= P_{ij} (bitxor) I
Threshold function

Fig.6.Process Flow

Image embedding Methods

Maintain 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. An ideal stegnography technique embeds message information into a carrier image with virtually imperceptible modification of the image. Adaptive stegnography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message. The objective of stegnography 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. As the application domain of embedding data in digital multimedia sources becomes broaden, several terms are used by various groups of researchers, including stegnography, digital watermarking, and data hiding. This paper introduces a new, principled approach to detecting least significant bit (LSB) stegnography 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. To evaluate the robustness of the proposed stego analytic approach, bounds on estimation errors are developed. Furthermore, the vulnerability of the new approach to possible attacks is also assessed, and counter measures are suggested is shown in fig 6.

To Encode the Hidden Data:

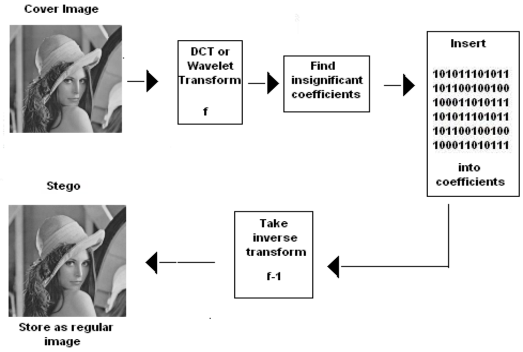

Fig.7. Encoding Of Hidden Data

- ○ Take the DCT or wavelet transform of the cover image
- ○ Find the coefficients below a certain threshold
- ○ Replace these bits with bits to be hidden (can use LSB insertion)
- ○ Take the inverse transform
- ○ Store as regular image(fig 7)

To Decode the Hidden Data:

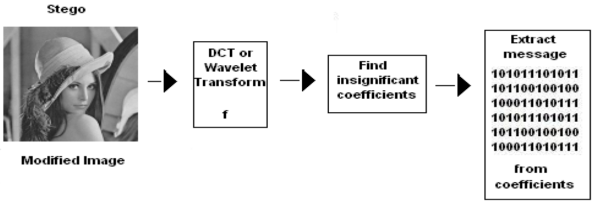

Fig.8.Decoding Of Hidden Data

- Take the transform of the modified image
- Find the coefficients below a certain threshold
- Extract bits of data from these coefficients
- Combine the bits into an actual message (fig 8)

Least Significant Bit Insertion (LSB): In random LSB insertion methods, a pseudo-random number generator is used to randomly distribute and hide the bits of a secret message into the least significant bits (LSBs) of the pixels within a carrier image, called the cover image. A popular approach to achieve this is the random interval method. Both communication parties share a stego-key, k usable as a seed for a random number generator. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. This is usually accomplished with two complementary techniques:

SIMULATED RESULTS

Original Image and its B Plane: The original image and its B plane extraction are displayed in the Fig.9. The B plane which is extracted from the original image is the darkest frame and thus the information in it is invisible.

Reserved Spaces (Dark Region) using LWT: The B plane image is partitioned using the Lifting Wavelet Transformation (LWT). Now a space is reserved for hiding the message while the other spaces are encrypted.

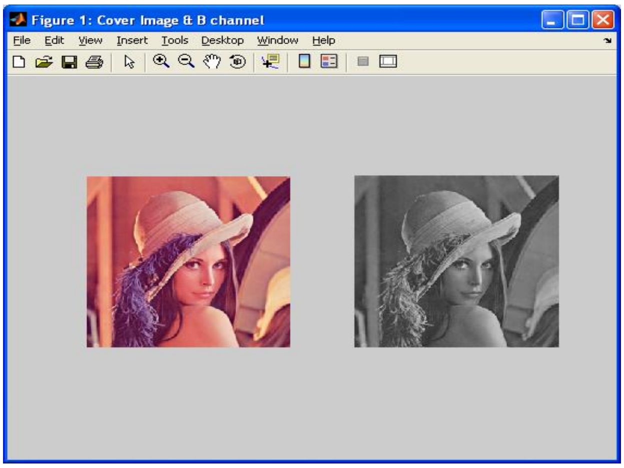
Figure 1: Cover Image & B channel
File Edit View Insert Tools Desktop Window Help

Fig.9.Original data and b plane

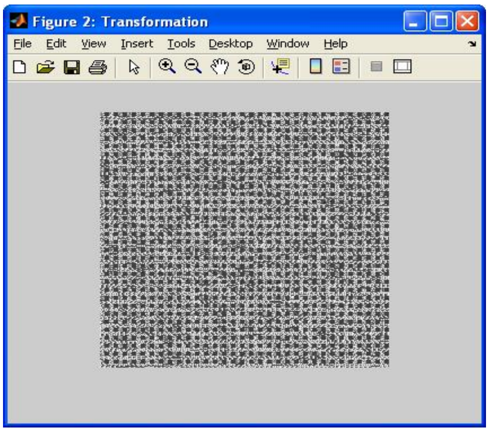

Fig.10.Transformed Image

c) Encrypted Image and its Recovery:

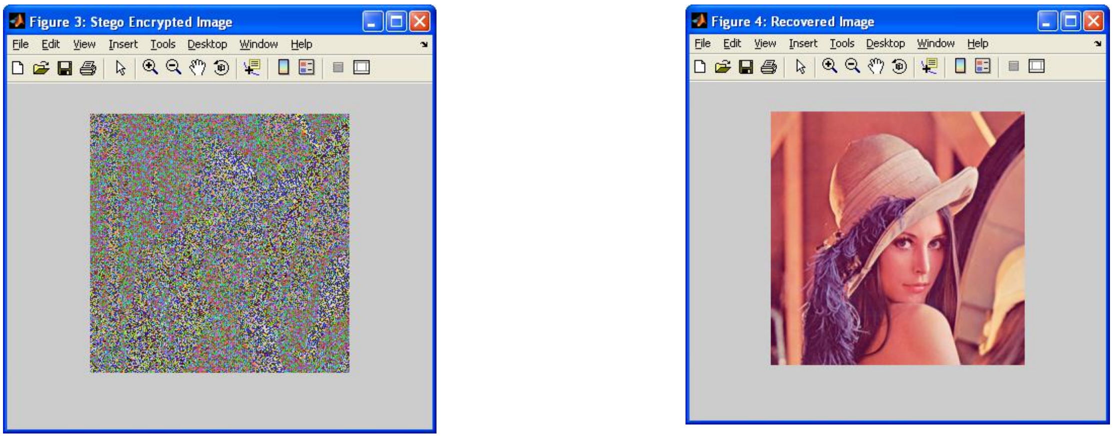
Figure 3: Stego Encrypted Image
File Edit View Insert Tools Desktop Window Help
Figure 4: Recovered Image
File Edit View Insert Tools Desktop Window Help

Fig.11.Encrypted Image And Its Recover

The encrypted image is then decrypted at the reception section. Such a recovered image after decryption is displayed in the Figure 11.

CONCLUSION

The paper presented that protection of image quality and hidden data during transmission based on approach of reserve room technique and chaotic crypto system with LSB based data concealment. Here, lifting wavelet transform was used to reserve space for concealing data effectively and chaos encryption was used as to protect image contents. This system was generated the stego-image with less error under maximum data hiding capacity. Finally, the performance of system was evaluated with quality metrics such as error and SNR factor. It was better compatible approach and flexibility with better efficiency rather than the prior schemes.

REFERENCES

A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC, 2007.

A. M. Alattar, Reversible watermark using the difference expansion of a generalized integer transform,IEEE Trans. Image Process., 13(8), 2013, 1147–1156.

D.M. Thodi and J. J. Rodríguez, Expansion embedding techniques for reversible watermarking,IEEE Trans. Image Process., 16(3), 2012, 721–730.

H.-C. Wu, C.-C. Lee, C.-S. Tsai, Y.-P. Chu, and H.-R. Chen, A high capacity reversible data hiding scheme with edge prediction and difference expansion,J. Syst. Softw., 82, 2012, 1966–1973.

J. Fridrich, M. Goljan, and R. Du, Lossless data embedding for all image formats, Proc. Security and Watermarking of MultimediaContents IV, Proc. SPIE, 4675, 2013, 572–583.

J. Tian, Reversible data embedding using a difference expansion,IEEE Trans. Circuits Syst. Video Technol., 13(8), 2013, 890–896.

K. Hwang and D. Li, Trusted cloud computing with secure resources and data coloring,IEEE Internet Comput, 14(5), 2005, 14–22.

L. Kamstra and H. J. A. M. Heijmans, Reversible data embedding into images using wavelet techniques and sorting,IEEE Trans. Image Process., 14(12), 2010, 2082–2090.

L. Luoet, Reversible imagewatermarking using interpolation technique,IEEE Trans. Inf. Forensics Security, 5(1), 2010, 187–193.

M. Goljan, J. Fridrich, and R. Du, Distortion-free data embedding, Proc. 4th Int. Workshop on Information Hiding, Lecture Notes inComputer Science, 2013, 2137, 27–41.

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.

M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, Lossless generalized- LSB data embedding,IEEE Trans. Image Process., 14(2), 2013, 253–266.

V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y.-Q. Shi, “Reversible watermarking algorithm using sorting and prediction,” IEEE Trans.Circuits Syst. Video Technol., vol. 19, no. 7, pp. 989–999, Jul. 2009.

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. 2002.

X. Wang, X. Li, B. Yang, and Z. Guo, Efficient generalized integer transform for reversible watermarking,IEEE Signal Process. Lett., 17(6), 2012, 567–570.

X. Zhang, Reversible data hiding in encrypted images,IEEE Signal Process. Lett., 18(4), 2001, 255–258.