Implementation of Reversible Data Hiding Using Suitable Wavelet Transform For Controlled Contrast Enhancement

Amita A. Ghadyalji
Department of Electronics and Telecommunication
G.H. Raisoni College Of Engineering & Management
Amravati (M.S.), India
smileamita@gmail.com

Sagar S. Badnerkar
Department of Electronics and Telecommunication
G.H. Raisoni College Of Engineering & Management
Amravati (M.S.), India
sagar.badnerkar@raisoni.net

Abstract - Data Hiding is important for secrete communication and it is also essential to keep the data hidden to be received by the intended recipient only. The conventional Reversible Data Hiding (RDH) algorithms pursue high Peak-Signal-to-Noise-Ratio (PSNR) at certain amount of embedding bits. Considering an importance of improvement in image visual quality than keeping high PSNR, a novel RDH scheme utilizing contrast enhancement to replace the PSNR was presented with the help of Integer Wavelet Transform (IWT). In proposed work, the identification of suitable transform from different wavelet families is planned to enhance the security of data by encrypting it and embedding more bits with the original image to generate stego image. The obtained stego image will be transmitted to the other end, where the receiver will extract the transmitted secrete data and original cover image from stego image using required keys. It will use a proper transformation for the purpose of Controlled Contrast Enhancement (CCE) to achieve the intended RDH so that the amount of embedding data bits and visual perception will be enhanced. The difference of the transmitted original image and restored original image is minor, which is almost invisible for human eyes though more bits are embedded with the original image. The performance parameters are also calculated.

Keywords-*Reversible Data hiding, encryption, decryption, controlled contrast enhancement, embedding, extraction, etc*

*****

I. INTRODUCTION

Over the last two decades, the rapid development of internet requires confidential information that needs to be protected from the unauthorized users. This is accomplished through Data hiding. It is a method of hiding secret messages into a cover medium so that an unintended observer will not be aware of the existence of the hidden messages. This is achieved by steganography. The term steganography is retrieved from the Greek words 'stegos' means cover and 'grafia' meaning writing defining it as 'covered writing'. The similarity between steganography and cryptography is that, both are used to conceal information. But the difference is that the steganography does not reveal any suspicious about the hidden information to the user. Therefore the attackers will not try to decrypt information.

Since the rise of the Internet is one of the most important factors of information technology and communication also needs to keep the security of information, cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. Data Hiding is the technique by which some data is hidden into a cover media. At receiver side, the original image must be extracted from the hidden encrypted format. The receiver must have both the keys for getting original image as well as the information or data. This can be achieved with the use of Reversible Data Hiding. In Reversible Data Hiding technique, the original image is obtained at the receiver side after encryption of data with the help of some secret keys. The Reversible Data Hiding is one of the techniques to reversibly get the original and secrete data back which was sent from the transmitter to the receiver. The Reversible Data Hiding is mainly used for secrete communication to achieve data security and to protect the data from the attackers. The main motivation towards this project is that one can embed more data bits with the original image and get more improved performance parameters with less distortion and less processing time.

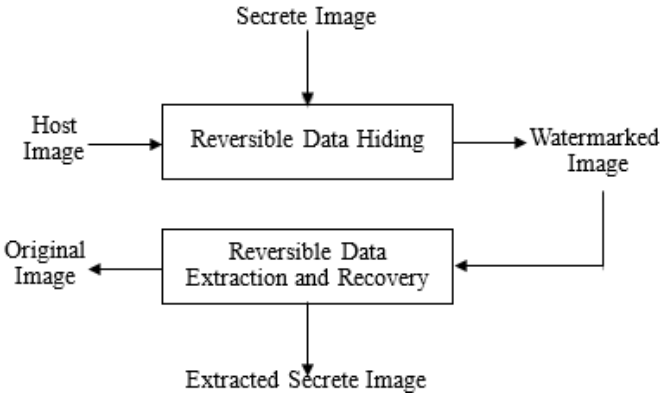

Fig 1: Reversible Data Hiding Procedure

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

II. LITURATURE SURVEY

A novel reversible data hiding scheme [1] for encrypted image with a low computation complexity was proposed, which consists of image encryption, data embedding and data extraction/ image recovery phases. After encrypting the entire data of an uncompressed image by a stream cipher, the additional data can be embedded into the image by modifying a small portion of encrypted data. Although a data-hider does not know the original content, he can embed additional data into the encrypted image by modifying a part of encrypted data. With an encrypted image containing additional data, one may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. Although someone with the knowledge of encryption key can obtain a decrypted image and detect the presence of hidden data using LSB-steganalytic methods.

Xiaolong Li et.al. Suggested a method based on two-dimensional difference histogram Modification [2]. A novel reversible data hiding (RDH) scheme was proposed by using difference-pair-mapping (DPM). First, by considering each pixel-pair and its context, a sequence consisting of pairs of difference values was computed. Then, a two-dimensional difference-histogram was generated by counting the frequency of the resulting difference-pairs. Finally, reversible data embedding was implemented according to a specifically designed DPM. Here, the DPM was an injective mapping defined on difference-pairs. It was a natural extension of expansion embedding and shifting techniques used in current histogram-based RDH methods. Compared with the conventional one-dimensional difference-histogram and one-dimensional prediction-error-histogram-based RDH methods, the image redundancy can be better exploited and an improved embedding performance was achieved by this approach. This method uses peak and minimum points of the pixel-intensity-histogram to embed data. It changes each pixel value at most by 1, and thus a good marked image quality can be obtained. However, since only one pixel of a pixel-pair was allowed to be modified by 1 in value, EC (Embedding Capacity) was low and this method does not work well if the cover image has a flat histogram.

Kede Ma, Weiming Zhang, Xianfeng Zhao, proposed a novel method by reserving room before encryption with a traditional RDH algorithm [3]. The authors studied that more and more attention was paid to reversible data hiding (RDH) in encrypted images, since it maintains the excellent property that the original cover can be losslessly recovered after embedded data was extracted while protecting the image content's confidentiality. All previous methods embed data by reversibly vacating room from the encrypted images, which may be subject to some errors on data extraction and/or image restoration. In this paper, authors proposed a novel method by reserving room before encryption with a traditional RDH algorithm, and thus it was easy for the data hider to reversibly embed data in the encrypted image. The proposed method achieved real reversibility that was, data extraction and image recovery were free of any error.

Huang Lidong, Zhao Wei described that Image enhancement has an important role in image processing applications [4]. Contrast limited adaptive histogram equalization (CLAHE) was an effective algorithm to enhance the local details of an image. However, it faces the contrast overstretching and noise enhancement problems. To solve these problems, this study presented a novel image enhancement method, named CLAHE-discrete wavelet transform (DWT), which combines the CLAHE with DWT. The new method includes three main steps: First, the original image was decomposed into low frequency and high-frequency components by DWT. Then, the authors enhanced the low-frequency coefficients using CLAHE and kept the high-frequency coefficients unchanged to limit noise enhancement. This is because the high-frequency component corresponds to the detail information and contains most noises of original image. Finally, reconstruct the image by taking inverse DWT of the new coefficients. To alleviate over-enhancement, the reconstructed and original images were averaged using an originally proposed weighting factor. The weighting operation can control the enhancement levels of regions with different luminances in original image adaptively. This is important because bright parts of image are usually needless to be enhanced in comparison with the dark parts.

Taranch Najafi and Farzad Zargari described a new hybrid method for contrast enhancement [5]. The proposed method was a combination of two basic contrast enhancement methods i.e. transform and histogram. At first, Non-sub-sampled Contourlet Transform (NSCT) was applied on the source image, and then NSCT coefficients were mapped to fuzzy domain and modified by a mapping function in fuzzy domain. After transforming the modified membership values from fuzzy domain into frequency domain, the enhanced image was reconstructed from the modified NSCT coefficients by inverse NSCT. Finally, histogram of the image was equalized by Contrast Limited Adaptive Histogram Equalization (CLAHE).

The conventional reversible data hiding (RDH) algorithms pursue high Peak-Signal-to-Noise-Ratio (PSNR) at the certain amount of embedding bits. But it was deemed that the improvement of image visual quality is more important than keeping high PSNR. Based on this viewpoint, Guangdong Gao and Yun-Qing Shi presented a novel RDH scheme[6], utilizing contrast enhancement to replace the PSNR. However, when a large number of bits were embedded, image contrast was over-enhanced, which introduced obvious distortions for human visual perception. Motivated by this issue, a new RDH scheme was proposed using the controlled contrast enhancement (CCE) and Haar integer wavelet transform (IWT).

Shruti M. Rakhunde and Archana A. Nikose presented a novel scheme for reversible data hiding with lossless recovery of original image [7]. The scheme described a method for hiding data in an image before encryption and then utilizes a novel method for encrypting the image using visual cryptography. A modified algorithm for reversible data hiding using difference expansion technique was used in this scheme. This scheme reserves the room before encryption. Then for hiding data improved Difference expansion technique was used which increases the data hiding capacity by hiding data in separate color component. For image encryption after hiding a data instead of using any standard cipher, a method of visual cryptography was used. For retrieving the complete image, all the random shares will be required.

Sheetal A. Kulkarni and Shubhangi B. Patil developed asymmetric key [8] which consists of reshuffling and secret arrangement of secret signal data bits in cover signal data bits. Here, the authors have performed the encryption process on secret speech signal data bits-level to achieve greater strength of encryption which is hidden inside the cover image. The secret key is generated within the encryption algorithm directly according to the entered letters and numbers at transmitter end. The secret key is generated within the encryption algorithm directly according to the entered letters and numbers at transmitter end. The secret data will be received by the authorized person at receiver end only when the secret key is entered correctly. The encryption algorithm applied with embedding method was the robust secure method for data hiding.

Ting Luo, Gangyi Jiang et al. presented a novel prediction error based reversible data hiding method using histogram shifting in spatial domain [9]. Three predictors including Mean, JPEG lossless and median edge detector (MED) are employed to compute prediction values for current pixels, respectively. Prediction error is defined as the difference between a pixel and the predicted value from its context. In the processes of data hiding, firstly the predication value was computed for each pixel and then prediction error was computed to build histogram bins. Histogram shifting mechanism was designed so that bins with large prediction errors are shifted based on hiding level, and thus, it will not hurt marked image if hiding level is not high. Histogram bins with small error predictions are used to hide secret data.

Punam V. Maitri, Dattatray S. Waghole and Vivek S. Deshpande investigated an algorithm with parameters of network security [10]. Information security is major obstacle in different areas like military, network application, bank application. File is forwarded from one location to another location in the network. Many hackers can illegally access the information. To provide solution to this problem many authors have introduced different algorithms and techniques .The different algorithms like AES, DES and triple DES achieve more security but it takes more time for encrypting and decrypting files. These algorithms increase the complexity. Byte Rotation Algorithm provides more security and takes smallest amount of time for file encryption and decryption. This algorithm can be applied on different types of files like text, image, audio, video files. The Byte Rotation Algorithm involves two techniques. One is random key generation technique and second is parallel encryption and decryption process which is a multithreading technique. Key size of random key generation technique is 128 bit.128 bit random key generation is difficult to crack for attackers.

Hao-Tian Wu, and Yun-Qing Shi proposed a novel reversible data hiding (RDH) algorithm [11] for digital images. Instead of trying to keep the PSNR value high, the proposed algorithm enhances the contrast of a host image to improve its visual quality. The highest two bins in the histogram are selected for data embedding so that histogram equalization can be performed by repeating the process. The side information is embedded along with the message bits into the host image so that the original image is completely recoverable. The proposed algorithm was implemented on two sets of images to demonstrate its efficiency.

III. PROPOSED WORK

Data Hiding is applied extensively to the fields of ownership protection, fingerprinting, authentication and secrete communication. The data may be any text related to the image such as authentication data or author information. In some high precision applications such as medical, military and remote

sensing; it is highly desired that the original image should be perfectly recovered after data extraction. A data hiding technique satisfying this requirement is known as Reversible Data Hiding. It is also called as Invertible, Lossless or Distortion-free data hiding. The Reversible Data Hiding technique can not only extract the embedded bits but also restore the original image without any error. The block diagrams for the transmission of hidden secrete data and recovery of the transmitted secrete data with the original image at receiver in the proposed scheme are shown in figures 2 and 3 respectively below.

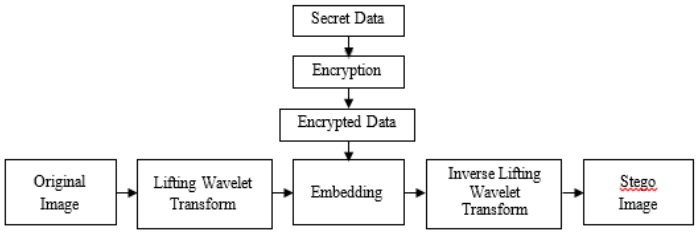

Fig 2: Transmission of secrete data with original image

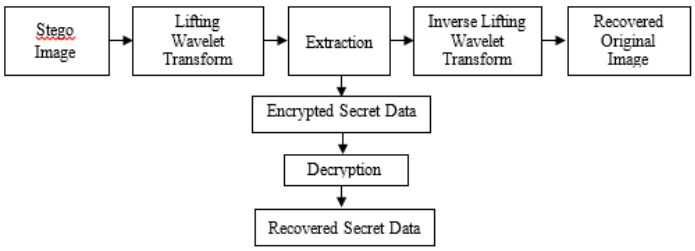

Fig 3: Recovery of secrete data and original image

In this work, for embedding the secrete message with original image, a lifting wavelet transform is applied to the original image first which performs a 2-D lifting wavelet decomposition with respect to a particular lifted wavelet, as shown in figure 2 above. The encrypted secrete image is then embedded with this lifted original image. Inverse lifting wavelet transform then performs a 2-D lifting wavelet reconstruction and a stego image is obtained as an output. Now at the time of extraction at receiver, a lifting wavelet transform is applied to the obtained stego image and secrete data is recovered using decryption function first. The applied inverse lifting wavelet transform then reconstructs the original image as shown in figure 3.

The secrete data is encrypted using encryption function to enhance the security of data.

The multiple encryption system provides sufficient security. But the performance and speed of these systems is low. Their complexity is very high. Hence, a new encryption algorithm named “Byte – Rotation Algorithm (BRA)” [10] with parallel encryption model is discovered which is applied on different blocks of plaintext and executes in parallel manner through multithreading concept of single processor system. This algorithm is an attempt to invent a new encryption simulator which is more secure and very fast to others. This algorithm enhances the security as well as speed of the encryption scheme.

The BR algorithm has the following features… q

- It is a Symmetric Key Block Cipher Algorithm
- Each block size is of 16 bytes
- Size of Key matrix is 16 bytes
- Values of Key matrix are randomly selected and ranging from 1 to 26
- Mono alphabetic substitution concept is followed
- Byte-Rotation technique is used

The steps of proposed Byte-Rotation Encryption Algorithm:

1. The letters of alphabet are assigned numerical values from 1 to 26 in sequence i.e. A, B, C, ..., X, Y, Z assigned numerical values 1, 2, 3, ..., 24, 25, 26 Respectively, the digits from 1 to 9 assigned numerical values from 27 to 35 respectively and the zero (0) remains as it is
2. The plaintext is partitioned into fixed-length blocks of size 16 bytes (or 128 bits) each. These blocks are represented by a matrix Mp
3. The values of Key matrix (K) are randomly selected from the range 1 to 26. The size of Key matrix is equivalent to the block size of plaintext i.e. 16 bytes. K = [k1, k2, ..., k16] K = Random (1, 26, 16)
4. Calculate the Transpose matrix of plaintext block matrix (Mp), which is denoted by MpT
5. Calculate encrypted Key matrix Ke using the following formula: Ke = K mod 2
6. Add both the matrices MpT and Ke and the resultant matrix is denoted by Cpk. Cpk = MpT + Ke
7. Rotate first three rows horizontally of Cpk matrix such that rotate one byte from first row, rotate two bytes from second row, rotate three bytes from third row and fourth row remains untouched. The resultant matrix is denoted by Chr
8. Rotate first three columns vertically of Chr matrix such that rotate one byte from first column, rotate two bytes from second column, rotate three bytes from third Column and fourth column remains untouched. The resultant matrix is denoted by Cvr
9. Replace numeric values of Cvr matrix by their corresponding letters and if 36 exist in Cvr matrix, it is replaced by the special character #. The resultant Matrix is denoted by Ce

ISSN: 2321-8169
148 – 153

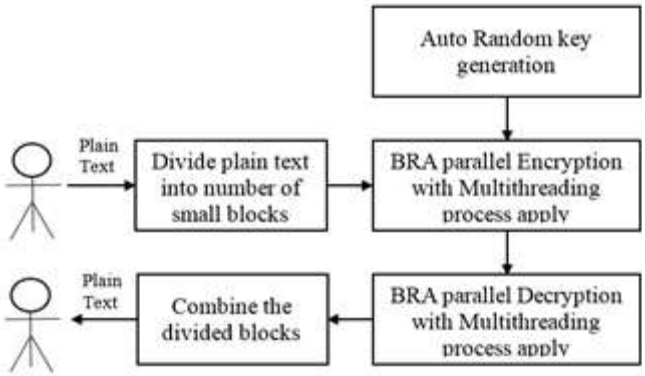

Fig 4: Architecture of BRA (Byte Rotation Algorithm)

The different performance parameters like Mean Square Error, Root Mean Square Error, Signal to Noise ratio, Peak Signal to Noise ratio, Correlation, Histogram etc. are also calculated here.

IV. RESULTANT DISCUSSION

The implementation results for Lena image with proposed work are shown in Fig. 5 below. The input and output image histograms are also shown here.

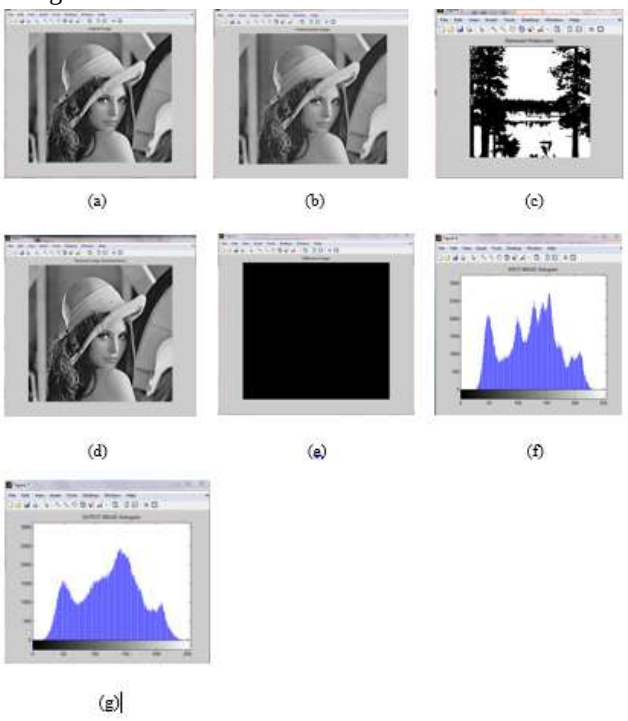

Fig 5: (a) original Lena (b) watermarked Lena (c) retrieved watermark (d) restored image(e) Difference of original and restored image f) input image histogram (g) output image histogram

Fig 6 : Comparison of visual perception & embedding capacity of marked image among Wu et al.'s [11], Ou et al.'s [15], Gao et al.'s [6] and proposed scheme for Lena(a) original image (b) [11],168001 bits (c) [15],113000 bits (d) [6],214918 bits(e) proposed,276881 bits

Figure 6 shows that when Lena is given as an original image and Sailboat is given as a secrete image, the hidden secrete image and the distortion-less original image are restored with minor error, which is invisible for human eyes. The input and the output image histograms which are nearly equal are also shown here.

	Lena	Baboon	Jet	Barbara	Tiffani	Boat
Ou et al.[15]	113000	41000	150000	89000	88000	70000
Dragoi et al.[16]	117960	39322	165150	107480	128450	83886
Xuan et al.[17]	73400	10485	104857	39321	47185	34078
Gao et al.[6]	214918	173807	253310	161933	267629	221586
Proposed	276881	386007	281218	331019	284287	299279

Table 1: Comparison of amount of embedded bits among [15], [16], [17], [6] and Proposed Scheme

Table 1 shows the Comparison of amount of embedded bits among various papers and the Proposed Scheme for different images.

	Lena	Baboon	Jet	Barbara	Tiffani	Boat
MSE	29.0317	13.2180	14.8159	26.7629	28.1990	19.0270

RMSE	2.321	1.9067	1.9619	2.2745	2.3044	2.0889
PSNR	33.5021	36.9192	36.4235	33.8555	33.6285	35.3371
Correlation	0.987	0.9917	0.9934	0.990	0.9660	0.9914
SNR	9.5700	12.9297	12.9107	10.017	9.3356	11.5336

Table 2: Performance parameter values for different images
Table 2 shows the different performance parameter values for different images taken under consideration.

V. CONCLUSION AND FUTURE SCOPE

In this work under consideration, a new Reversible Data Hiding scheme utilizing suitable wavelet transform for controlled contrast enhancement was proposed. The proposed scheme have encrypted the secrete image to be hide using Byte Rotation Encryption technique and then embedded it with an original image. The hidden secrete image and the original image is then extracted separately. The difference of the transmitted original image and restored original image is minor, which is almost invisible for human eyes. Furthermore, compared with other existing RDH algorithms, the proposed scheme can embed significantly larger amount of data and achieve better visual quality from human vision point of view. High embedding data rate also avoids severe distortions.

As security is an important factor in communication system, a lot of work can be done in future to achieve more security with better visual perception of an image. In many fields like medical, ownership protection, authentication etc., secure communication is very essential to keep the information or data secrete. Based on this viewpoint, One can try to increase the amount of secrete data with better recovery. The research on adaptively determining RCE threshold will be carried on in future to further improve the algorithm performance.

REFERENCES

[1] Xinpeng Zhang, "Reversible Data Hiding in Encrypted Image", in IEEE signal processing letters, VOL. 18, NO. 4, pp 255-258, april 2011

[2] Xiaolong Li, Weiming Zhang, Xinlu Gui, and Bin Yang, "A Novel Reversible Data Hiding Scheme Based on Two-Dimensional Difference-Histogram Modification", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, pp 1091-1100,JULY 2013

[3] Kede Ma, Weiming Zhang, Xianfeng Zhao,, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 3, pp 553-562,MARCH 2013

[4] Huang Lidong, Zhao Wei et.al, "Combination of contrast limited adaptive histogram equalisation and discrete wavelet transform for image enhancement", School of Electronic and Information Engineering, IET Image Process., Vol. 9, Iss. 10, pp. 908–915, April 2015

[5] Taraneh Najafi and Farzad Zargari, "A Hybrid Method for Contrast Enhancement", IEEE International Conference on Consumer Electronics – Berlin, pp. 352-355, 2011

[6] Guangyong Gao and Yun-Qing Shi, "Reversible Data Hiding Using Controlled ContrastEnhancement and Integer Wavelet Transform", IEEE SIGNAL PROCESSING LETTERS, VOL. 22, NO. 11, pp. 2078-2082,NOVEMBER 2015

[7] Shruti M. Rakhunde and Archana A. Nikose,"New Approach for Reversible Data Hiding Using Visual Cryptography", Sixth International Conference on Computational Intelligence and Communication Networks, pp. 846-855,2014.

[8] Sheetal A. Kulkarni and Shubhangi B. Patil," A Robust Encryption Method for Speech Data Hiding in Digital Images for Optimized Security", International Conference on Pervasive Computing (ICPC), pp. 978-982,2015.

[9] Ting Luo, Gangyi Jiang, Mei Yu, and Wei Gao, "Novel Prediction Error Based Reversible Data Hiding Method Using Histogram Shifting", International Journal of Computer Theory and Engineering, Vol. 7, No. 5,pp. 332-336, October 2015

[10] Punam V. Maitri and Vivek S. Deshpande," Low Latency for File Encryption and Decryption Using BRA Algorithm in Network Security", International Conference on Pervasive Computing (ICPC), pp. 978-981,2015.

[11] Hao-Tian Wu and Yun-Qing Shi, "Reversible Image Data Hiding with Contrast Enhancement", IEEE SIGNAL PROCESSING LETTERS, VOL. 22, NO. 1, pp. 81-85,JANUARY 2015.

[12] P. Bas and T. Furon, "A new measure of watermarking security: The effective key length," IEEE Trans. Inf. Forensics Secur., vol. 8, no. 1, pp. 1306–1317, 2013.

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

[14] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3, pp. 873–882, 2011.

[15] B. Ou, X. Li, Y. Zhao, R. Ni, and Y. Q. Shi, "Pairwise prediction error expansion for efficient reversible data hiding," IEEE Trans. Image Process., vol. 22, no. 12, pp. 5010–5021, 2013.

[16] I. Dragoi and D. Coltuc, "Local prediction based difference expansion reversible watermarking," IEEE Trans. Image Process., vol. 23, no. 4, pp. 1779–1790, 2014.

[17] G. Xuan, C. Yang, Y. Zhen, Y. Q. Shi, and Z. Ni, "Reversible data hiding using integer wavelet transform and companding technique," Lecture Notes in Computer Science, vol. 3304, pp. 115–124, 2005.

[18] H. Wu, J. Dugelay, and Y. Q. Shi, "Reversible image data hiding with contrast enhancement," IEEE Signal Process. Lett., vol. 22, no. 1, pp.81–85,2015.

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

[20] D. Coltuc, "Improved embedding for prediction-based reversible watermarking," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 3, pp. 873–882, 2011.