An RGB Image Encryption Supported by Wavelet-based Lossless Compression

Ch. Samson[1]
Dept. of Information Technology, SNIST,
Hyderabad, India,

V. U. K. Sastry[2]
Dept. of Computer Science & Engineering., SNIST,
Hyderabad, India,

***Abstract*— In this paper we have proposed a method for an RGB image encryption supported by lifting scheme based lossless compression. Firstly we have compressed the input color image using a 2-D integer wavelet transform. Then we have applied lossless predictive coding to achieve additional compression. The compressed image is encrypted by using Secure Advanced Hill Cipher (SAHC) involving a pair of involutory matrices, a function called Mix() and an operation called XOR. Decryption followed by reconstruction shows that there is no difference between the output image and the input image. The proposed method can be used for efficient and secure transmission of image data.**

Keywords- Image compression; Wavelet Transform; image encryption; Lifting Wavelet ; Secure Advanced Hill Cipher.

I. INTRODUCTION

When network bandwidth and storage space are limited, an image to be transmitted has to be compressed. It is necessary to protect confidential image data during transmission from unauthorized access. Compression [1] reduces the storage space required to represent a given quantity of information. Image compression [1] is of two types: lossy and lossless (error- free). Lossless compression schemes are reversible so that the original data can be reconstructed exactly, while lossy schemes accept some loss of data in order to achieve higher compression. Lossless compression can be used for text, medical images and legal documents etc. whereas lossy compression is used for natural images, speech signals etc. Cryptography plays an important role in information security. Encryption [2] is the process of converting information into an unintelligible form. Image encryption has applications in Internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

Wavelet Transform has emerged as a powerful mathematical tool in many areas of science and engineering. The power of Wavelets comes from the use of multiresolution analysis. In a recent investigation [3], we have studied the encryption of an image supported by lossy compression by using multilevel Wavelet Transform.

The study of integer wavelets based on lifting scheme [4] has gained considerable impetus in the recent years. Unlike classical wavelets which are obtained by translations and dilations of one function in the frequency domain, the wavelets governed by the lifting scheme are obtained by a new approach based on spatial domain. Many researchers [5-9] have dealt with image compression using lifting based wavelet transform.

In one of the recent investigations, Bibhudendra et al. [10] have proposed an advanced Hill cipher algorithm which uses an Involutory key matrix for image encryption. We have enhanced the advanced Hill cipher by introducing a pair of involutory matrices, a function called Mix( ) and XOR operation, and we have called this cipher as Secure Advanced Hill Cipher (SAHC).

In the present paper, our objective is to develop a method for an RGB image encryption using lifting scheme based on lossless compression. Firstly, we compress the input image using lifting wavelet transform and then encrypt the compressed image applying Secure Advanced Hill Cipher.

In what follows we present the plan of the paper. In section 2, we explain the proposed method. Section 3 describes the process of image compression using lifting wavelet transform. We present an approach for SAHC based image encryption in section 4. Section 5 deals with computations that are carried out in this analysis and draw conclusions.

II. PROPOSED METHOD

Encryption following compression leads to a faster and secure transmission of image data across a channel. So image is compressed prior to encryption. Perfect reconstruction is possible with Lifting Wavelet Transform. A digital color image is represented in terms of three color components, namely, Red, Green and Blue (RGB). Each component is like gray scale image. So the three components of an RGB image can be coded separately and concatenated at the end. The Schematic diagram of the proposed method is shown in Figure 1.

The proposed method is developed by the following steps.

1. Lifting scheme based Transform coding: Choose an integer wavelet and number of lifting steps (levels) N. Perform the transform coding of the image at level N.

2. **Encoding**: Use lossless predictive coding to achieve additional compression.

3. Encryption: Encrypt the encoded image using Secure Advanced Hill Cipher.

4. Decryption: Get encoded image by performing decryption using Secure Advanced Hill Cipher.

5. **Decoding:** Use lossless predictive decoding to get the transform coded image.

6. Reconstruction: Use Lifting scheme based inverse transform coding to get reconstructed original input image.

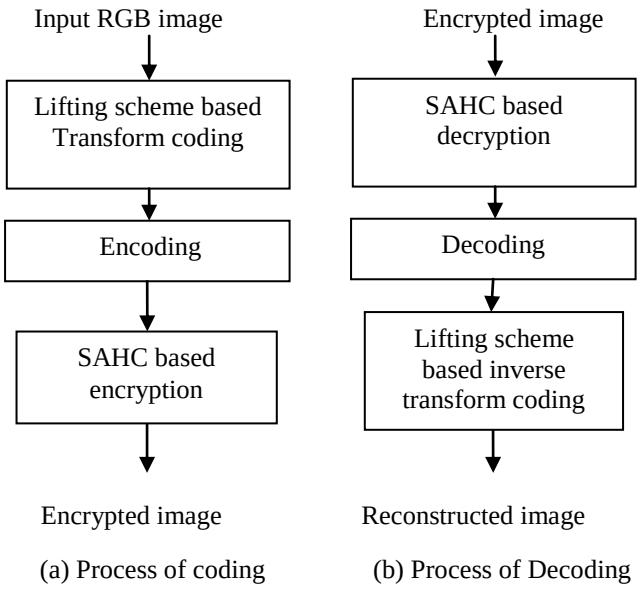

Figure 1. Schematic diagram of the proposed method

III. LIFTING SCHEME FOR IMAGE COMPRESSION

Lifting scheme is an alternative approach to Discrete Wavelet Transform. It was proposed by Sweldens [5]. Lifting is a way of describing and calculating wavelets. It calculates wavelets in place, which means that it takes no extra memory to do the transform. Every wavelet can be written in lifting form. The input signal is first split into even and odd indexed samples. The samples are correlated, so that it is possible to predict odd samples from even samples as given below.

$$odd_{new} = odd_{old} + \alpha\,(even_{left} + even_{right})$$

where α is the predict step coefficient. The difference between the actual odd samples and the prediction becomes the wavelet coefficients. The operation of obtaining the differences from the prediction is called the lifting step. The update step follows the prediction step, where the even values are updated from the input even samples and the updated odd samples.

$$even_{new} = even_{old} + \beta\,(odd_{left} + odd_{right})$$

where β is the update step coefficient. They become the scaling coefficients which will be passed on to the next stage of transform. This is called the second lifting step. This lifting scheme, called forward lifting scheme, is shown in Figure 2.

The basic idea of the reverse process of the above lifting scheme is displayed in Figure 3.

The lifting scheme provides integer coefficients and so it is exactly reversible. The total number of coefficients before and after the transform remains the same.

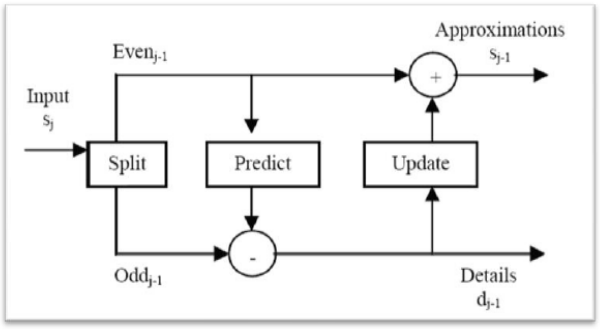

Figure 2. Forward Lifting Scheme.

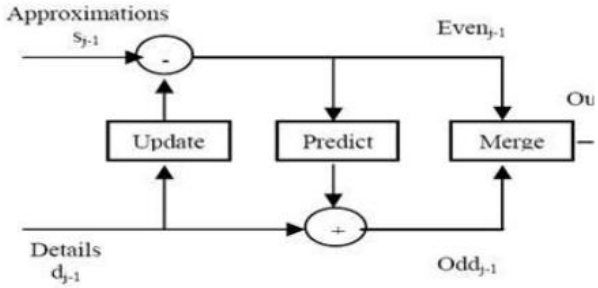

Figure 3. Reverse Lifting Scheme

The inverse transform gets back the original signal by exactly reversing the operations of the forward transform with a merge operation in place of a split operation. The number of samples in the input signal must be a power of two, and these samples are reduced by half in each succeeding step until the last step which produces one sample.

To achieve additional compression, lossless predictive coding [1] is applied to each sub band using different values of predictor coefficients alpha and beta, giving an encoded image as output. The reverse process is applied to the encoded image to get back the transformed image. Then on applying inverse transform coding on the transformed image, we get back the reconstructed image. The reconstructed image which we have obtained in our analysis is an exact replica of the original input image.

Let us now consider an RGB image given in Figure 4. and focus our attention on one of the component images. On adopting the process of compression, described above, we get the corresponding compressed image. The same procedure is applied on the remaining component images to obtain the corresponding compressed images.

IV. SAHC BASED IMAGE ENCRYPRTION

In the advanced Hill cipher, the basic equations governing encryption and the decryption are given by

$$C = AP \bmod N,$$
$$P = AC \bmod N.$$

respectively. Here A is an involutory matrix which includes the key matrix. As A is an involutory matrix, we have $A^{-1} = A$, where A^{-1} is the modular arithmetic inverse of A. Thus in the case of this cipher, we need not compute the modular arithmetic inverse of A separately, once A is known to us. This is the advantage which is being achieved in this cipher.

Image encryption using Secure Advance Hill Cipher includes a pair of involutory matrices A and B, as multiplicands of the input matrix P, a function called Mix( ) and an operation called XOR . The function Mix( ) is used for mixing the binary bits to create confusion and diffusion thoroughly. The values of d and e are integers required in the development of the involutory matrices A and B. In our analysis, they are taken as 5 and 7 respectively. The value of N is taken as 256.

ALGORITHM FOR ENCRYPTION

1. Read P, K, L, d,e,r, N
2. A = Involute (K, d)
   and
   B = Involute (L,e)
3. Construct NT and ST
4. for i = 1 to r
   P = (APB) mod N
   P = Mix (P)
   P = P $\oplus$ ST
   end
5. C = P
6. Write C.

ALGORITHM FOR DECRYPTION

1. Read C, K, L, d,e,r, N
2. A = Involute (K, d)
   and
   B = Involute (L,e)
3. Construct NT and ST
7. for i = 1 to r

   C = XOR (C,ST)
   C = Imix (C)
   C = (ACB) mod N
   end
7. P = C
8. Write P.

Here K and L are the key matrices, NT is the number table containing the numbers 0 to 255, ST is the substitution table, and r denotes the number of rounds taken as 16. The details of the advanced Hill cipher can be found in [11].

On adopting the SAHC based encryption algorithm discussed in this section, on each one of the compressed component images separately, we get the encrypted image corresponding to each one of the component images. On combining all these encrypted component images in an appropriate manner, we get the encrypted form of the color image presented in Figure 7. On using SAHC decryption algorithm, we get back the encoded image.

V. COMPUTATIONS AND CONCLUSIONS

In this paper we have implemented an RGB image encryption supported by lifting scheme based lossless compression using MATLAB [12]. In this analysis, we have considered lifting wavelet based on Haar transform. The input image and its corresponding transform coded image, encoded image, encrypted image, decrypted image, decoded image and reconstructed image are shown in Figures 4 to 10 respectively. It is interesting to note that the reconstructed image is exactly identical to the original input image.

Figure 4. Input RGB image of a baby

Figure 5. Image obtained after transform coding.

Figure 6. Encoded image.

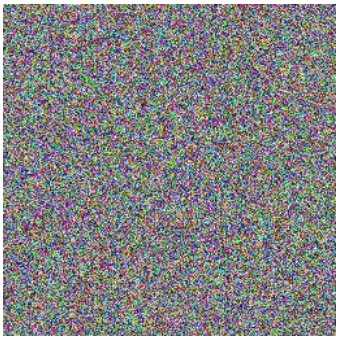

Figure 7. Encrypted image.

Figure 8. Decrypted image.

Figure 9. Decoded image.

Figure 10. Reconstructed image

The same experiment is carried out with another color image which is given in Figure 11.

Figure 11. An RGB color image.

Thus we get the following images at various stages of the process.

Figure 12. Image obtained after lifting based transform coding

Figure 13. Encoded image.

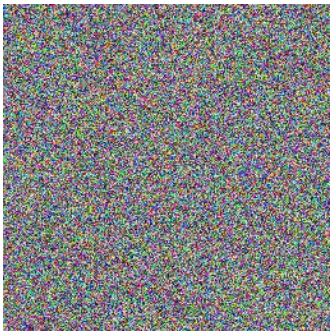

Figure 14. Encrypted image.

Figure 15. Decrypted image.

From the above analysis, we conclude that the encryption supported by compression is an interesting one and it can be used for the transmission color images more effectively in a secured manner.

REFERENCES

[1] Rafael C. Gonzalez & Richard E. Woods,— Digital Image processing, 2ndEdition Pearson Education 2004.

[2] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson, 2003.

[3] Ch.Samson,V. U. K. Sastry," A novel method for image encryption supported by compression using multilevel Wavelet Transform", International Journal of Advanced Computer Science and Applications,Vol. 3. No. 8,August 2012.

Figure 16. Decoded image.

Figure 17. Reconstructed image

[4] K.P. Soman, K.I. Ramachandran, Insight into Wavelets from theory to practice, Second edition, PHI, 2006.

[5] W. Sweldens. "The Lifting Scheme: A New Philosophy in Biorthogonal Wavelet Constructions."*Proc. SPIE*, vol. 2569, pp. 68-79, 1995.

[6] C. Lian, K. Chen, H. Chen, and L. Chen, "Lifting Based Discrete Wavelet Transform Architecture for JPEG2000*," IEEE Int. Symp. Circuits and Systems*, vol. 2, pp. 445-448, May 2001.

[7] Pei-Yin Chen, "VLSI implementation for one-dimensional multilevel lifting-based wavelet transform," IEEE Trans. Computers, Vol. 53, pp.386-398, April 2004.

[8] H. Liao, M. K. Mandal, and B.F. Cockburn, "Efficient architectures for 1-D and 2-D liftingbased wavelet transforms" IEEE Trans. Signal Processing, Vol. 52, pp. 1315-1326, May 2004.

[9] Dr.B Eswara Reddy and K Venkata Narayana,' A Lossless Image Compression Using Traditional and Lifting based Wavelets', Signal & Image Processing : An International Journal (SIPIJ) Vol.3, No.2, April 2012.

[10] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, 2007, pp. 14-21..

[11] V. U. K. Sastry, Ch.Samson," Cryptography of a Gray Level Image and a Color Image Using Modern Advanced Hill Cipher Including a Pair of Involutory Matrices as Multiplicands and Involving a Set of Functions", International Journal of Engineering Science and Technology,Vol. 4 No. 7 July 2012.

[12] Alasdair Mcandrew, —Digital Image processing with MatLab, Cengage learning 2004.

AUTHORS PROFILE

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur, India and worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 80 research papers in various international journals. He received the best Engineering College Faculty Award in Computer Science and Engineering for the year 2008 from the Indian Society for Technical Education (AP Chapter) and Cognizant- Sreenidhi Best faculty award for the year 2012. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

Mr. Ch. Samson obtained his Diploma from Govt. Polytechnic, Hyderabad in 1994, B. E. from Osmania University in 1998 and M. E from SRTM University in 2000. Presently he is pursuing Ph.D. from JNTUH, Hyderabad since 2009. He published 10 research papers in various international journals and two papers in conferences. He is currently working as Associate Professor and Associate Head in the Dept. of Information Technology (IT), SNIST since June 2005. His research interests are Image Processing, Image Cryptography and Network Security.