Scholars Journal of Engineering and Technology (SJET) **ISSN 2321-435X (Online)**
Sch. J. Eng. Tech., 2016; 4(1):1-5 **ISSN 2347-9523 (Print)**

(An International Publisher for Academic and Scientific Resources)
www.saspublisher.com

Original Research Article

Image Encryption and Compression Using Scalable Coding Techniques

Karpakam S[1], Amutha A[2]
[1,2]Assistant professor, Department of Electronics and Communication Engineering, SVS College of Engineering Coimbatore, Tamil Nadu, India

***Corresponding author**
Karpakam S
Email: eben4uever@gmail.com

Abstract: The security becomes an important issue of communication and storage of image due to the growth of multimedia application. Encryption is one of the ways to ensure high security. Images are used in many fields such as military and medical science. They are stored or transferred through network, security of such image data is important. Encryption involves applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. Information privacy becomes a challenging issue. In order to protect valuable data or image from undesirable readers, image encryption and decryption is essential. In this approach, encryption phase by using selective encryption technique original image pixel values are completely concealed so that an attacker cannot obtain any statistical information from an original image. An encoder quantizes the sub images and Hadamard transform is applied to reduce the data amount. At the receiver side with the cryptographic key, the principal content with higher resolution can be reconstructed when more bit streams are received. The quality of the reconstructed image is measured by calculating peak signal to noise ratio (PSNR).
Keywords: Hadamard Transform, Pseudo Random Number Generator (PRNG), Image Encryption, Compression, Decryption, Peak Signal to Noise Ratio (PSNR).

INTRODUCTION

In recent years, encrypted signal processing has attracted in many research interests [1].based on the homomorphic properties of a cryptosystem [2], [3] the discrete Fourier transform and adaptive filtering can be implemented in the encrypted domain and to reduce the complexity [4] a composite signal representation method can be used. A part of significant data of a plain signal is encrypted for the purpose of content protection, and the remaining data are used to carry the additional message for copyright protection [5], [6] in joint encryption and data hiding.

A number of works on encrypted compressing have been also presented. When an original image is encrypted by a sender for privacy protection, a channel provider without the knowledge of a cryptographic key and the original information may reduce the information amount due to the less number of channel resource. In [7] the compression of encrypted data is analyzed with the theory of source coding and decoder. So it represents the performance of compressing encrypted data may be good when compare with the compressing non encrypted data.

Image compression by using reversible integer wavelet transform [8] has several advantages. The most important one is through the use of suitable techniques, a full bit stream can be generated .And also, the decoder can extract a lossy version of the image, continue to decode at higher rates until the image is perfectly reconstructed. But this technique contains the major disadvantage that, if resolution scalability is not desired instead, the decoder can't extract a low resolution version of image and continue to decode the bit stream.

In [9] an encrypted image is decomposed in a progressive manner by using rate-compatible punctured turbo codes, the data in most significant planes are compressed, based on local statistics of a low resolution version of the image. Furthermore, lossy compressive encrypted images have been developed, by using several metods.in [10] with the help of pixel permutation, the original gray scale image is encrypted then the encrypted data are compressed by removing rough and fine information of coefficients generated from orthogonal transform. However [11] encryption rate distortion performance is low and which has the leakage of statistical information. In [12] binary images are converted into binary phase encoded pixels and which are encrypted by binary random phase XOR operation. But the security of this technique is very less when compare with the encryption in compressed

domain. .So to overcome the above disadvantages a new scalable coding algorithm is used for image compression and encryption.

This paper proposes a novel scheme of scalable coding for encrypted gray images. The pixel values are completely concealed in the encryption phase of proposed scheme. So that an attacker cannot obtain any statistical information from its original image. Then, the encrypted data are decomposed into several parts; bit stream is achieved by combining each part. At the receiver side with the help of cryptographic key, if the more bit streams are received the original content will be reconstructed with higher resolution.

The rest of this paper is ordered as follows. In Section II a brief review of encryption for an uncompressed image is given. In Section III the proposed scalable coding algorithm is introduced and discussed by calculating its performance factors. Finally some conclusions and future avenues for research are represented in Section IV.

ENCRYPTION FOR UNCOMPRESSED IMAGES

A secure computing environment is completed only by considering encryption technology. The term encryption refers the original information can only be decoded, read and understood by people for whom the information is intended. It is the process of encoding data to prevent unauthorized parties from viewing or modifying it. Encryption is used to provide highest levels of security to network communication, e-mail, files stored on hard drives or floppy disks, and other information that requires protection. By generating key we can provide the higher security. Only an authorized person can use the key value to encode or decode the original content. Keys are denoted in different forms such as passwords, numbers which are generated by an algorithm. By using key value sender and recipient of message can understand how the message can be encrypted. By using the key value recipient can properly decode the message.

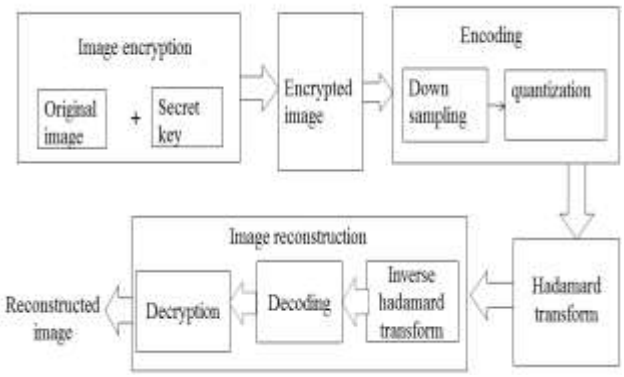

Fig.1: Block Diagram Of Scalable Coding Algorithm

Initially original image pixel values are added with the pseudo random numbers. Here XOR operation is done to add the every pixel values of original image with the pseudo random bit sequence. After that encrypted image is given to the encoding operation. In this phase down sampling is done to reduce the sampling rate of encrypted image. Then quantization is done to round off the encrypted pixel values into its nearest integer pixel values. Then Hadamard transform is applied to compress the encoded bit streams. Transform is basically a mathematical tool, which allows us to move from one domain to another domain to perform the task at hand in easier manner. The transformation may place the image data in a more compact form so that they can be stored and transmitted efficiently. Transforms play a major role in various image processing applications such as image analysis, image enhancement, and image filtering and image compression. After that inverse Hadamard transform is applied at the receiver side to get back the uncompressed encrypted image. Then decoding is done covert data into its original format after that by using secrete key in decryption phase original image is reconstructed.

A very effective method to encrypt an image, which applies to a binary image, consists of a message and mixing image data (the key in some sense) that has the same size as the image. With this approach distinction is not introduced between bit planes even though the subjective relevance of each bit plane is not equal and also the generality of the gray level image is straight forward.

Let X be the original image is in an uncompressed format and that the pixel values are within [0, 255], and denote the numbers of rows and columns as N1 and N2 and the pixel number as (N=N1xN2).Therefore, the bit amount of the original image is 8N.

Scalable Coding Algorithm For Image Encryption

The steps followed in the image encryption and decryptions are as follows.

Step1:

Generates a pseudorandom bit sequence with a length of 8N and assume the content owner and the decoder have the same pseudorandom number generator (PRNG) and a shared secret key used as the seed of the PRNG.

Step 2:

Divides the pseudorandom bit sequence into N pieces, each of which containing 8 bits and convert each piece as an integer number within [0,255].An encrypted image is produced by a one-by-one modulo 256 additions as follows:

$$g^{(0)}(i,j)=\text{mod}\,[p(i,j)+e(i,j),256],$$
$$1\le i\le N_1,\ 1\le j\le N_2 \qquad (1)$$

where P(i,j),represents the gray values of pixels at positions (i,j), e(i,j) represents the pseudorandom numbers within [0, 255] generated by the PRNG, and $g^{(0)}(i,j)$ represents the encrypted pixel values.

Step 3:

An encoder does not know the secret key and the original content, it can still compress the encrypted data as a set of bit streams.

The complete encoding procedure is given below.

a) Encoder is used to convert the one form of data into another form. Encoder is usually associated with the audio and video signal. Here, the encoder decomposes the encrypted image into a series of sub images and data sets with a multiple resolution construction.

b) The sub images at the (t+1) and $G^{(t+1)}$th level is generated by down sampling the sub image at the t th level as follows

$$g^{(t+1)}(i,j) = g^{(t)}(2i,2j) \;.\; t=0,1\ldots\ldots T-1 \qquad (2)$$

Where $G^{(0)}$ is just the encrypted image and T is the number of decomposition levels.

c) The encrypted pixels that belong to $G^{(t)}$ but do not belong to $G^{(t+1)}$ form data set $Q^{(t+1)}$ as follows:

$$Q^{(t+1)} = \{g^{(t)}(i,j) | \text{mod}(i,2) = 1 \text{ or } \text{mod}(j,2) = 1\}, \qquad (3)$$

Where t=0,1……T-1

That means each $G^{(t)}$ is decomposed into $G^{(t+1)}$and $Q^{(t+1)}$, and the data amount of $Q^{(t+1)}$ is three times of that of $G^{(t+1)}$.

d) After the multiple-level decomposition, the encrypted image is updated as
$G^{(T)}$, $Q^{(T)}$, $Q^{(t-1)}$ …, and $Q^{(1)}$.

Step 4:

Perform quantization for the values of encoded pixels.

$$b(i,,j) = g^{(T)}(i,j)/\Delta \qquad (4)$$

Where $\Delta = 256/M$

For each data set $Q^{(t)}$ (t=1,2….T), the encoder permutes and divides encrypted pixels in it into $K^{(t)}$groups, each of which containing $L^{(t)}$pixels. group the $L^{(t)}$pixels in the entire image which are denoted as $q_k^{(t)}(1), q_k^{(t)}(2)\ldots\ldots, q_k^{(t)}(L^{(t)})$.

Step 5:

Perform the Hadamard transform in each group as follows:

$$\begin{pmatrix} C_K^{(t)}(1 \\ C_K^{(t)}(2) \\ . \\ .= \text{ H.} \\ C_K^{(t)}(L^{(t)}) \end{pmatrix} \quad . (3.5) \quad \begin{pmatrix} q_K^{(t)}(1) \\ q_K^{(t)}(2) \\ . \\ q_K^{(t)}(L^{(t)}) \end{pmatrix}$$

Where H is $L^{(t)}$ x $L^{(t)}$ Hadamard matrix.

Step6: Calculate the Compression Ratio

High quality image data requires large amounts of storage space and transmission band-width, so the current technology is unable to handle technically and economically. One of the possible solutions to this problem is to compress the information so that the storage space and transmission time can be reduced. By using image compression we can store the image in compact manner and can be transmitted faster.

The encoder transmits the bit streams with an order of {BG, $BS^{(T)}$, $BS^{(T-1)}$ ….$BS^{(1)}$}.Here, the total compression ratio is denoted as Rc which is the ratio between the amount of the encoded data and the encrypted image data,

$$R_c = \frac{\log_2 M}{8.4^T} + \frac{3}{8}\sum_{t=1}^{T}\frac{\log_2 M^{(t)}}{4^t} \qquad (5)$$

Scalable Coding Algorithm for Image Reconstruction

Step1: Initially, consider the encrypted sequence, reversed key sequence and the array used in encryption.

Step2: Next, consider the first element in the key and group the bits in the encrypted sequence based on the number.

Step3: Now convert each group to corresponding decimal number.

Step4: Depending on the length of input sequence, divide the decimated sequence to equal length sub-sequences such that each sub-sequence length should be expressed as power of 2.

Step5: Represent each sub-sequence as a column matrix. Now, multiply each sub-sequence matrix with the modified hadamard matrix, such that the matrix of the form modulo 2x-1 must be used to perform multiplication.

Step6: Now, multiply two modulo 2x-1 matrices and find the divisor such that the resultant matrix obtained is thus represented as an identity matrix.

Step7: Calculate the modulo multiplicative inverse for the divisor that is, a*y mod 2x-1 =1[5] where y is the divisor and a is modulo multiplicative inverse.

Step8: Multiply the resultant matrix obtained in step 7.

Step9: Apply modulo 2x-1 on the resultant values obtained after multiplication.

Step10: Check for the corresponding array index for every 0 in the decimal sequence, replace 0 with 2x-1if the index has an element 1.

Step11: Convert each decimal number in the sequence to corresponding binary values.

Step12: Remove all consecutive 0s at end of the sequence such that, the resultant sequence length is equal to power of 2.

EXPERIMENTAL RESULTS AND DISCUSSION

A test image Lena and camera man that are sized as 256×256,which are used as the original images in the experiment and these images are encrypted by generating pseudo random bit sequence. After that we let assume threshold value T=3 and encoded the encrypted images using M=24, $L^{(2)}$=8, $L^{(3)}$=4, and $L^{(1)}$=24 to produce the bit streams BG, $BS^{(3)}$, $BS^{(2)}$, and $BS^{(1)}$. Here T represents the threshold value which is a point beyond which there is a change in the manner a program starts to execute correctly .Then Hadamard transformation is applied for the compression purpose.

In this case, the total compression ratio R_C=1.Fig. 2 gives the reconstructed Lena using (BG), (BG, $BS^{(3)}$), (BG,$BS^{(3)}$,$BS^{(2)}$) and (BG, $BS^{(3)}$,$BS^{(2)}$,$BS^{(1)}$)respectively. When more bit streams were used reconstructed results with higher resolution were obtained. Reconstructed results PSNR values of Lena are denoted as 35.9656, 36.9782 and 37.9791, for camera man as 35.9672, 37.9784 and 37.9892 for Elaine as 35.9658, 36.9788 and 37.9895.The gray scale ''Lena'' of size 256×256,Input image, encrypted image and its reconstructed is shown in the following figure 2,3,4,5,6,7 respectively.

Fig. 2: Input Image

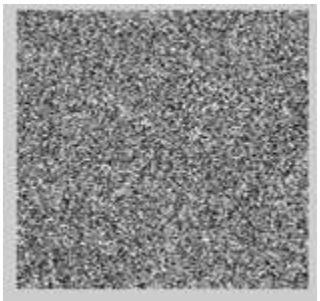

Fig. 3: Encrypted Image

(a)

(b)

(c)

Fig. 4: (a, b, c)Reconstructed Lena Using final image bit stream 1,bit stream 2 and bit stream 3 $\{Bs^{(B)}\},\{Bs^{(B)},Bs^{(3)}\ Bs^{(2)}\},\{Bs^{(B)}Bs^{(3)}Bs^{(2)}Bs^{(1)}\ \}$.

Fig. 7: Reconstructed Image

PSNR

This ratio is often used as a quality measurement between the original and a reconstructed image. The experimental value is db. Table 1 shows the values of PSNR for Lena, Camera man and Elaine images with different Integer value M.

Table 1: PSNR value of input image with different M.

Input image	Integer Value (M)	PSNR (db)
Lena	18	35.9656
	22	36.9782
	24	37.9791
Camera man	18	35.9672
	22	37.9784
	24	37.9892
Elaine	18	35.9658
	22	36.9788
	24	37.9895

Based on the integer value M and the Threshold value T, compression ratio of original input image Lena is denoted as 0.4750,0.5180,0.6430, for camera man as 0.4951,0.5382,0.6732 and for Elaine as 0.4852,0.5281,0.6530.

When an encrypted image is decomposed within more levels, more data are involved in compression and quantization. Therefore the PSNR performance is better and more iteration for image reconstruction is needed. It is also shown that the performance is not important when using a higher T more than 3.

Performance Criteria

In the evaluation of the performance of the encryption scheme, we use the peak signal to noise ratio PSNR between original and reconstructed image. By calculating peak signal to noise ratio we can identify the security of the scalable coding algorithm technique. Here the original image pixel values are assumed to be 8 bits to give a maximum pixel value of 255. By analyzing different bit streams at the receiving side security of the input image will be extended.

CONCLUSION

In the proposed work, the original image is encrypted by a modulo-256 addition with pseudorandom numbers, and the encoded bit streams are made up of a quantized encrypted sub image and the quantized remainders of Hadamard coefficients. At the receiver side, while the sub image is decrypted to produce an approximate image, the quantized data of Hadamard coefficients can provide more detailed information for image reconstruction. Since the bit streams are generated with a multiple-resolution construction, when more bit streams are received the principal of content with higher resolution can be obtained. In encryption technique, Scalable coding algorithm includes more number of advantages like amount of secrecy (key size) determines amount of labor. So in this scalable coding technique Set of keys and enciphering algorithm are simple and Implementation of algorithms is simple, Errors do not propagate from the sender side to receiver side. Size of cipher text is not larger than original message. The Lossless compression and scalable coding for encrypted image with better performance deserves further investigation.

REFERENCES

1. Bianchi T, piva A, and Bami M; Composite signal representation for fast and storage-efficient processing of encrypted signals. IEEE Trans. Inf. Forensics Security, 2010; 5(1): 180–187.
2. Dewitte S, Cornelis J; Lossless integer wavelet transform. IEEE Signal Processing Lett., 1997; 4: 158–160.
3. Kuribayashi M, Tanaka H; Finger printing protocol for image based on additive homomorphic property. IEEE Trans. Image Process., 2005; 14(12): 2129–2139.
4. Kumar A, Makur A; Lossy compression of encrypted image by compressive sensing technique, in Proc. IEEE TENCON , 2009; 1–6.
5. Lian S, Liu Z, RenZ; commutative encryption and watermarking in video compression. IEEE Trans. Circuits Syst. Video Technol., 2007; 17(6): 774–778.
6. Lazzeretti R, Barni M; lossless compression of encrypted gray level and color image, in Proc. 16th EUSIPCO, Lausanne, Switzerland, 760-764, 2008.
7. Memon N, Wong PW; A buyer-seller watermarking protocol. IEEE Trans. Image Process., 2001; 10(4): 643–649.
8. Schonberg D, Draper SC, Ramchandran K; On blind compression of encrypted correlated data approaching the source entropy rate, in Proc. 43rd Annu. Allerton Conf., Allerton, IL, 2005; 7: 153-156.
9. Schonberg D, Draper SC, Yeo C, Ramchandran; Toward compression of encrypted images and video sequences. IEEE Trans. Inf. Forensics Security,2008; 3(4): 749–762.
10. Taubman D; High performance scalable image compression with EBCOT. IEEE Trans. Image Process, 2000; 9(7): 1158–1170.
11. Troncoso-pastoriza JR, perez-Gonzalez F; secure adaptive filtering. IEEE Trans. Inf. Forensics Security, 2011;6(2): 469–485.
12. Woods JW, Naveen T; A filter based bit allocation scheme for sub band compression of HDTV. IEEE Trans. Image Processing, 1992; 1: 436–440.
13. Zhang X, Feng G, Ren Y, Qian Z; Scalable coding of encrypted images. Image Processing, IEEE Transactions on, 2012; 21(6):3108-3114.