ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON HIGH RESOLUTION IMAGE ENCRYPTION AND RECONSTRUCTION USING SCALABLE CODING

Nirali.R.Burad*, Prof.Harish Bhangale
Research student, Head Of Department
Department of Electronics and Communication, G.H.Raisoni Institute Of Engineering & Management, India

ABSTRACT

In today's connected world, research. This paper proposes a unique scheme of scalable coding of transmitting and receiving images in an extreme protected way using Hadamard transform. In the encryption phase, the original pixel values are masked by a modulo-256 addition with non-random numbers that are derived from a secret key.Then, the encrypted data are decomposed into several parts, and each part is compressed as a bit stream. After decomposing the encrypted data into a down sampled subimage and several data sets with a multiple-resolution construction, an encoder calculates the subimage and the Hadamard coefficients of each dataset to condense the data quantity. Then, the data calculates subimage and coefficients are observed as a set of bitstreams. Because of the hierarchical coding mechanism at the receiver side with the cryptographic key, the principal content with higher resolution can be reconstructed when more bit streams are received.

KEYWORDS: Bitsreams, hadamard Transform, Image encryption, Quantization Scalable coding.

INTRODUCTION

Image encryption and Image compression plays an important role between sender and receiver. The goal of image encryption is that the attacker or hacker or intruder should not obtain the statistical information. Various Cryptographic techniques are developed to secure the data between transmission and reception. The frequency domain and adaptive filtering can be engaged in the encrypted area based on the homomorphic properties of a cryptography [3], [4], and a complex signal representation method can be used to decrease the size of encrypted information and computation difficulty [2]. An invisible watermarking technique in which the seller does not get to know the exact watermarked copy that the buyer receives [5]. With several buyer– seller code of behaviour [1], [6], the some secrete data such as balm print, finger print are embedded into an encrypted form of digital multimedia to make sure that the seller cannot know the buyer's watermarked version while the buyer cannot obtain the original product. A number of works on compression encrypted images have been also presented . when a sender encrypts an original image for privacy protection, a channel provider without the knowledge of a cryptographic key and original content may be given to reduce the data amount due to the limited channel resource. In [7], the compression of encrypted data is looked into with the theory of source coding with side information at the decoder, and it is pointed out that the performance of compressing encrypted data may be as good as that of compressing non-encrypted data in theory.

Two practical approaches are also given in [7]. In the first one, the original binary image is encrypted by adding a pseudorandom string, and the encrypted data are compressed by finding the syndromes of low-density parity-check (LDPC) channel code. In the second one, the original Gaussian sequence is encrypted by adding an independent identically distributed Gaussian sequence, and the encrypted data are quantized and compressed as the syndromes of trellis code. While Schonberg *et al.* [8] study the compression of encrypted data for memoryless and hidden Markov sources using LDPC codes, Lazzeretti and Barni [9] present several lossless compression methods for encrypted gray and color images by employing LDPC codes into various bit planes. In [10], the encrypted image is decomposed in a progressive manner, and the data in most important planes are compressed using rate-compatible punctured turbo codes.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

RELATED WORK

The combination of cryptographic technique and signal processing is used which is togetherly known as secure signal processing. An emerging area of related work to secure multimedia retrieval is secure signal processing, which aims at performing normal signal processing tasks but keeping the signals being processed secret. Erkin et al. provided a review of related cryptographic primitives and some applications of secure signal processing in data analysis and content protection. However, applying cryptographic primitives to content-based multimedia retrieval is not straightforward. Effective multimedia retrieval typically relies on evaluating the similarity of two documents using the distance between their visual features, such as color histograms, shape descriptors, or salient points [1].

More advances take place in signal processing. More investigation take place on implementation of the discrete Fourier transform in the encrypted domain, by using the homomorphic property of the cryptosystem. Several algorithms were used such as direct DFT, radix-2, and radix-4 fast Fourier algorithm but it is not applicable to all other applications. This includes a C++ prototype implementation of encrypted domain discrete cosine transform (e-DCT) based on Paillier homomorphic cryptosystem. It provides both standard and fast (based on Hou's algorithm) DCT-II and DCT-III. The archive also includes routines for composite representation and a demo applying encrypted domain 8x8 block DCT/fast DCT using both standard and composite representations[2].

Novel scheme of scalable coding for encrypted images is described. The concept of Hadamard transforms is used. The discrete Fourier transform and adaptive filtering can be implemented in the encrypted domain based on the homomorphic properties of a cryptosystem and a composite signal representation method can be used to reduce the size of encrypted data and computation complexity[3].

The growth of digital television technology and the revolution in image and video compression (such as JPEG2000, broadcast TV, and video phone), highlighting the need for standardization in processing static and moving images and their exchange between computer systems[5].

Describes a unique scheme of scalable coding of transmitting and receiving images in an extreme protected way using Absolute Moment block truncation coding (AMBTC)[6].

It was shown that it is theoretically possible to compress encrypted data to the entropy rate of the unencrypted source. Since good encryption makes a source look completely random, traditional algorithms are unable to compress encrypted data. For this reason, traditional systems make sure to compress before they encrypt. Johnson et al.[7] show that the problem of compressing encrypted data is related to source coding with side information. It was shown that neither compression performance nor security need be impacted under some reasonable conditions [7].

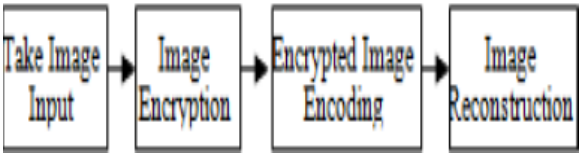
The idea of low density parity check codes[LDPC] is used[8]. Techniques to compress encrypted colour and gray level images are explain using XOR based algorithm [8].

The encrypted image should be decrypted first before extraction to separate the data extraction from image decryption Zeng emptied out space for data embedding following the idea of compressing encrypted images [10].

In recent years there are various changes in the encrypted signal processing. The discrete Fourier transform and adaptive filtering can be implemented in the encrypted domain and composite signal representation method can be used to reduce the size of encrypted data.

PROPOSED SCHEME

Figure1



General Block Diagram

The general block diagram of the proposed system of high resolution image encryption and reconstruction using scalable coding is shown above. All the blocks are explained in detail one by one. The rough idea of preoject is first the image is transmitted later on on that image encryption is done. After encryption with the help of some cryptographic technique encoding is done. After that to get image back reconstruction is done which is known as image reconstruction.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

A.Image Encryption

Encryption is one of the ways to ensure high security for real time applications. The processing of encrypted signals has emerged as a new and challenging research field. In the proposed system, Assume that 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 N2and the pixel number as N(N = N1 × N2). Therefore, the bit amount of the original image is 8N. The content owner generates a pseudorandom bit sequence with a length of 8N.

Here, we assume the content owner and the decoder has the same pseudorandom generator (PRNG) and a shared secret key used as the seed of the PRNG. Then the content owner divides the pseudorandom bit sequence into N pieces, each of which containing 8 bits, and converts each piece as an integer number within [0,255]. Pseudorandom numbers are used to encrypt the original pixel values. Encoder is used to convert the one form of data into another form. Encryption is the main process for image transmission. Encryption is done only on primary part of image and remaining part is sent as a plain image for secure data communication.

Detail diagram of image encryption is as follows:

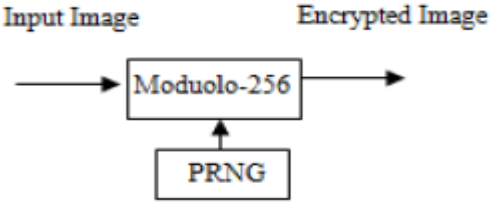


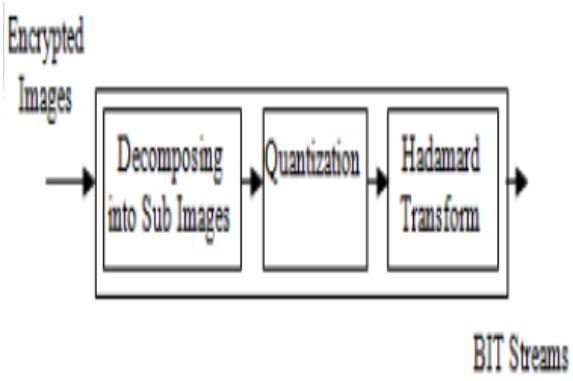
Figure2

Image Encryption

B. Encryptemage Encoding

Here, after decomposing the encrypted data into a series of subimage and the coefficient of each data set to effectively reduce the data amount. Then, the quantized subimage and coefficients are regarded as a set of bit streams. Detailed diagram of encrypted image encoding is as follows:

Figure3



Encrypted Image Encoding

C. Image Reconstruction

In Image Reconstruction process the procedure we follow is similar to Image encoding but the decryption of original data is performed firstly by subtracting the pseudo random number we have added to the image.

Figure4

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

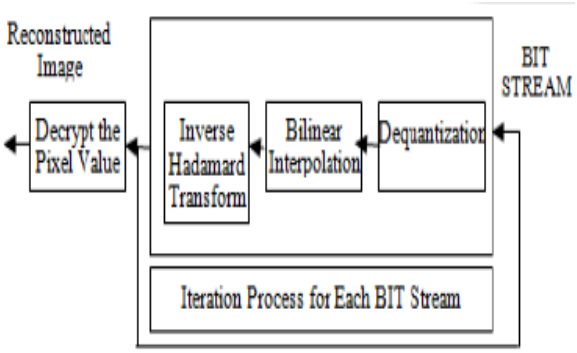


Image Reconstruction

Hence we get the Original data and then we multiply the step size since we quantized the data by dividing with step size during encoding to obtain detail content. bit streams and the secret key obtained, a decoder can first obtained an approximate image by decrypting the quantized subimage and then reconstructing the principal content of the original image and because of the hierarchical coding mechanism, if more number of bit-streams are received at receiver it leads to get high resolution of an image.The process in the image reconstructions involves

CONCLUSION

In this project we are trying to obtain more clear image after receiving file. Sometimes we are trying to send image with the help of Bluetooth or in mail etc. so to obtained clear image we use this technique. This proposed scheme has a novel approach of high resolution scalable coding for encrypted images and image compression. The original image is encrypted by a modulo – 256 addition with pseudorandom numbers (PN) and the encoded bit streams are made up of a quantized encrypted subimage and the quantized remains of Hadamard coefficient. At the receiver, whereas the subimage is decrypted to create an approximate image, the quantized data of Hadamard coefficient can be offered more exhaustive data for image reconstruction. Since the bit streams are generated with a multiple resolution construction, the principle content with higher resolution can be obtained when more bit streams are received. We are trying to implement the better technique so that we can get high resolution pic.

ACKNOWLEDGEMENTS

Authors would like to express sincere thanks and deep gratitude to Prof. H. K. Bhangale, Head of E&C Department who extended wholehearted co-operation to complete this work successfully.
Authors are also express deep and sincere gratitude to the principal, G.H. Raisoni institute of engineering & management,Jalgaon for being a constant source of inspiration.

REFERENCES

[1] Z. Erkin, A. Piva, S. Katzenbeisser, R. L.Lagendijk, J. Shokrollahi, G. Neven, and M.Barni, “Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing,” EURASIP J. Inf.Security, vol. 2007, pp. 1–20, Jan. 2007.
[2] T. Bianchi, A. Piva, and M. Barni, “On the implementation of the discrete Fourier transform in the encrypted domain,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009 .
[3] Xinpeng Zhang, Member, IEEE, Guorui Feng, Yanli Ren, and Zhenxing Qian”Scalable Coding of Encrypted Images” IEEE transactions on image processing, vol. 21, no. 6, June 2012.
[4] Rafael C. Gonzalez, Richard Eugene; “Digital image processing”, Edition 3, 2008, page 466
[5] M. Ghanbari "Standard Codecs: Image Compression to Advanced Video Coding" Institution Electrical Engineers, ISBN: 0852967101, 2003, CHM, 430 pages
[6] M.D.Lema, O.R.Mitchell, “Absolute Moment Block Truncation Coding and its Application to Color Image”, IEEE Trans. Coomun., Vol. COM-32, No. 10, pp. 1148-1157, Oct. 1984.
[7] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” *IEEE Trans. Signal Process.*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
[8] D. Schonberg, S. C. Draper, and K. Ramchandran, “On blind compression of encrypted correlated data approaching the source entropy rate,” in *Proc. 43rd Annu. Allerton Conf.*, Allerton, IL, 2005.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785
(ISRA), Impact Factor: 2.114

[9] R. Lazzeretti and M. Barni, "Lossless compression of encrypted greylevel and color images," in Proc. 16th EUSIPCO, Lausanne, Switzerland, Aug. 2008 [Online].Available:http://www.eurasip.org/Proceedings/Eusipco/Eusipco2008/papers/1569105134.pdf.

[10] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," *IEEE Trans. Signal Process*, vol. 19, no. 4, pp. 1097–1102, Apr. 2010.