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

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW ON ENCODING AND RECONSTUCTION OF ENCRYPTED IMAGES

Shweta M. Ghorpade*, Prof.Khandagle K. R.
Research student, Assistant Professor
Department of Electronics and Communication,
MIT College Of Engineering,Aurangabad
India

ABSTRACT

This paper gives a scheme of encoding of encrypted greyscale images while transmission of images for security purpose. In the encryption phase, the original pixel values are masked by a modulo-256 addition with pseudorandom numbers that are derived from a secret key. After decomposing the encrypted data into a downsampled subimage and several data sets with a multiple-resolution construction, an encoder quantizes the subimage and the Hadamard coefficients of each data set to reduce the data amount. Then, the data of quantized subimage and coefficients are regarded as a set of bitstreams. At the receiver side, while a subimage is decrypted to provide the rough information of the original content, the quantized coefficients can be used to reconstruct the detailed content with an iteratively updating procedure. Because of the hierarchical coding mechanism, the principal original content with higher resolution can be reconstructed when more bitstreams are received.

KEYWORDS: Pseudorandom number generator(PRNG), Bitsreams, Hadamard Transform, Cryptography, Quantization.

INTRODUCTION

Digital image processing is the use of computer algorithms to perform image processing on digital images. The 2D continuous image is divided into N rows and M columns. The intersection of a row and a column is called a pixel. The image can also be a function of other variables including depth, colour, and time. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor. For display, the image is stored in a rapid-access buffer memory, which refreshes the monitor at a rate of 25 frames per second to produce a visually continuous display.

In recent years, encrypted signal processing has attracted considerable research interests. 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. In joint encryption and data hiding, a part of significant data of a plain signal is encrypted for content protection, and the remaining data are used to carry buyer–seller protocols, the fingerprint data are embedded into an encrypted version of digital multimedia to ensure that the seller cannot know the buyer's watermarked version while the buyer cannot obtain the original product. A number of works on compressing 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 tend to reduce the data amount due to the limited channel resource

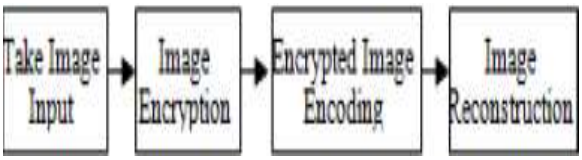
METHODOLOGIES USED

Basically, the purpose of cryptography and steganography is to provide secret communication. However, steganography is not the same as cryptography. Cryptography hides the contents of a secret message from a malicious people, whereas steganography even conceals the existence of the message. Steganography must not be confused with cryptography, where we transform the message so as to make it meaning obscure to a malicious people who intercept it. Therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system need the attacker to detect that steganography has been used and he is able to read the embedded message[11].

In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it. Cryptography can also provide authentication for verifying the identity of someone or something[1].
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 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

In the proposed scheme, a series of pseudorandom numbers derived from a secret key are used to encrypt the original pixel values. After decomposing the encrypted data into a subimage and several data sets with a multiple-resolution construction, an encoder quantizes the subimage and the Hadamard coefficients of each data set to effectively reduce the data amount. Then, the quantized subimage and coefficients are regarded as a set of bit streams. When having the encoded bit streams and the secret key, a decoder can first obtain an approximate image by decrypting the quantized subimage and then reconstructing the detailed content using the quantized coefficients with the aid of spatial correlation in natural images. Because of the hierarchical coding mechanism, the principal original content with higher resolution can be reconstructed when more bit streams are received.

A. Image Encryption

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 N_1 and N_2 and the pixel number as ($N=N_1 \times N_2$). 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 number 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]. An encrypted image is produced by a one-by-one addition modulo 256 as follows:

$$g^{(0)}(i,j) = \mathrm{mod}\,[p(i,j) + e(i,j), 256],$$

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. Clearly, the encrypted pixel values $g^{(0)}(i, j)$ are pseudorandom numbers since $e(i, j)$ values are pseudorandom numbers. It is well known that there is no probability polynomial time (PPT) algorithm to distinguish a pseudorandom number sequence and a random number sequence until now. Therefore, any PPT adversary cannot distinguish an encrypted pixel sequence and a random number sequence. That is to say, the image encryption algorithm that we have proposed is semantically secure against any PPT adversary.

Figure 2

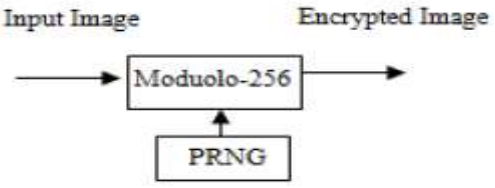
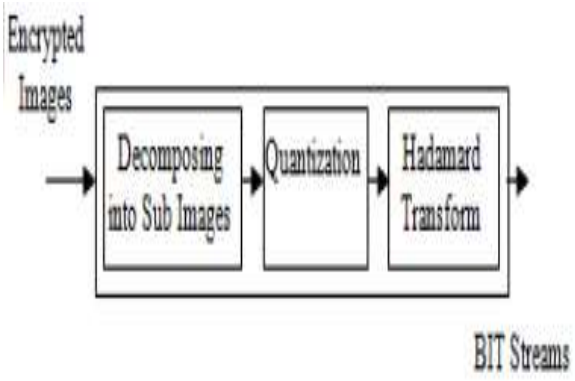


Image Encryption

B. Encrypted Image Encoding

Although an encoder does not know the secret key and the original content, he can still compress the encrypted data as a set of bitstreams the encoder decomposes the encrypted image into a series of subimages and data sets with a multiple-resolution construction. A higher resolution image can be reconstructed when more bitstreams are obtained at the receiver side. Here, the total compression ratio R_C, which is a ratio between the amount of the encoded data and the encrypted image.

Figure 3



Encrypted Image Encoding

C. Image Reconstruction

The bitstreams and the secret key, a receiver can reconstruct the principal content of the original image, and the resolution of the reconstructed image is dependent on the number of received bitstreams. While BG provides the rough information of the original content, $BS^{(t)}$ can be used to reconstruct the detailed content with an iteratively updating procedure.

CONCLUSION

In this project we are trying to obtain image after reception of image. So to get original image we use this technique. This scheme has a approach of scalable encoding of encrypted images. 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. At the receiver side, 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. K.R.Khandagle, Professor 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, MIT College of engineering, Aurangabad 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.
[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.
[11] Fridrich, Jessica; M. Goljan and D. Soukal (2004). "Searching for the Stego Key" (http://www.ws.binghamton.edu/fridrich/Research/Keysearch_SPIE.pdf). *Proc. SPIE, Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents VI* 5306: 70–82. Retrieved 23 January 2014.