ENCRYPTION AND DECRYPTION OF GRAY SCALE IMAGES USING SCALABLE CODING MECHANISM

Dr. T. R. Saravanan
Dept. of computer science and engg, JEEPIAR SRR Engineering College, Chennai, India,

Dr. K. Uma
School of Information Technology and Engineering, VIT University, Vellore, India

M. Basha Khaja,
Wipro, Software engineer, Ireland, United Kingdom,

ABSTRACT

Encrypted signal processing has attracted considerable research interests. 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. So we can use the new approach of the paper proposes a novel scheme of scalable coding for encrypted gray images. Although there have been a lot of works on scalable coding of unencrypted images, the scalable coding of encrypted data has not been reported. In the encryption phase of the proposed scheme, the pixel values are completely concealed so that an attacker cannot obtain any statistical information of an original image. Then, the encrypted data are decomposed into several parts, and each part is compressed as a bit stream. At the receiver side with the cryptographic key, the principal content with higher resolution can be reconstructed when more bit streams are received.

Keywords- Segmentation, Cryptosystem, cryptographic, Encryption, decryption, Compression, Scalable Coding


1. INTRODUCTION

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image [1]. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it. 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 homomorphism properties of a cryptosystem and a composite signal representation method can be used to reduce the size of encrypted data and computation complexity [2].

A secure the encrypted image using encoding. Normal encryption produces a textual output whereas advanced encryption masks the data completely. And to achieve compression we perform encoding produces a stream of bits which is a combination of 1’s and 0’s. After encryption we sample the image into several sub images and again the sub images are encoded. As a result the whole image will only consist of bits not text. So the compressed image can be used for transmission since memory occupation of compressed image will be less than uncompressed image [3][4]. This method of encoding achieves security of the contents and any attempt by an intruder to retrieve the contents will not succeed.

2. LITERATURE SURVEY

Signal-processing modules occupied directly on encrypted data provide an elegant solution to request scenarios where valuable signals must be protected from a malicious processing device. We investigate the implementation of the discrete Fourier transform (DFT) in the encrypted domain by using the homomorphic properties of the underlying cryptosystem [5].

The protection of digital data when it is processed by other parties has arisen as a major concern for the general public, and an important topic of research. The field of Signal Processing in the Encrypted Domain (SPED) has emerged in order to provide efficient and secure solutions for preserving privacy of signals that are processed by un-trusted agents. The impossibility of using a strategy based solely on current homomorphic encryption systems, and we propose several novel secure protocols for a privacy-preserving execution of the least mean squares (LMS) algorithm, combining different SPED techniques, and paying special attention to the error analysis of the finite-precision implementations [6].

Signal processing tools working directly on encrypted data could provide an efficient solution to application scenarios where sensitive signals must be protected from an untrusted processing device. In this paper, we consider the data expansion required to pass from the plaintext to the encrypted representation of signals, due to the use of cryptosystems operating on very large algebraic structures. A general composite signal representation allowing us to pack together a number of signal samples and process them as a unique sample is discussed [7].

The purposes of copy protection and copy deterrence for multimedia content are discussed. In copy deterrence, a content owner (seller) inserts a unique watermark into a copy of the content before it is sold to a buyer. If the buyer sells unauthorized copies of the watermarked content, then these copies can be traced to the unlawful reseller (original buyer) using a watermark detection algorithm [7].

Homomorphic property of public-key cryptosystems is applied for various cryptographic protocols, such as electronic cash, elective system, bidding protocols, etc. Several fingerprinting protocols also exploit the property to achieve an asymmetric system. However, their enciphering rate is particularly low and the implementation of watermarking technique is difficult [8].

When it is chosen to transmit redundant data over a insecure and bandwidth-constrained network, it is customary to first compress the data and then encrypt it. In this paper, we investigate the novelty of reversing the order of these steps, i.e., first encrypting and then compressing, without compromising either the compression efficiency or the information-theoretic security [9]. Although counter-intuitive, we show surprisingly that, complete the use of coding with side information principles, this reversal of order is indeed possible in some settings of interest without loss of either optimal coding efficiency or perfect secrecy [10].

Lossless compression of encrypted sources can be achieved through Slepian-Wolf coding. For encrypted real-world sources, such as images, the key to increase the compression efficiency is how the source dependency is exploited. Approaches in the literature that make use of Markov
properties in the Slepian-Wolf decoder do not work well for grayscale images [11]. In this correspondence, a resolution progressive compression scheme which compresses an encrypted image progressively in resolution, such that the decoder can observe a low-resolution version of the image, study local data based on it, and use the statistics to decode the next resolve level [12].

2.1. Existing System and Challenges
Adaptive filtering can be implemented in the encrypted domain based on the homomorphism 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 the additional message for copyright protection. With some 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.

- The pixel positions are shuffled and the pixel values are not masked in the encryption phase.
- We used to reduce the size of encrypted data and computation complexity

3. MATERIALS AND METHODS

3.1 Proposed System
A series of pseudorandom (is an algorithm for generating a sequence of numbers that approximates the properties of random numbers) numbers derived from a secret key are used to encrypt the original pixel values. After decomposing the encrypted data into a sub image and several data sets with a multiple-resolution construction, an encoder quantizes the sub image and the Hadamard coefficients of each data set to effectively reduce the data amount. Then, the quantized sub image 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 sub image 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.

ADVANTAGES

- 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.
- The original gray image is encrypted by pixel permutation.

3.1.1 Preprocessing
Authentication is the process of obtaining identification credentials such as name and password from a user and validating those credentials against some authority. If the credentials are valid, the entity that submitted the credentials is considered an authenticated identity. Once an identity has been authenticated, the authorization process determines whether that identity has access to a given resource.
The using the folder browser and browse the one picture in the device and edit. Select the image then only user can access all types of processing. In this module user select the image in module. User select the image is using uploading the file our computer. The particular image they will be selected to the project. After that we can create key. A gray scale image is given as input. The pixel values of such image are in the range of 0 to 255. The input image pixels are read and pixel values are modulo added with random values and make the contents of original image hidden. The image will be compressed using to enable it to transmit and therefore we reduce the image size. Now the image would be in an unreadable format. Fig.1 shows the user searching information.

Finally we get the Complete Natural image. They get the new picture in the file. All the process will complete they will get the clear image in the project. In complete the process the existing method image and proposed method image they will be compare. It has been big different to the image in both level. So the image store in our system. To achieve this, we perform decoding and decryption as shown in Fig.2.

**Figure.1.** Data searching

**Figure.2.** Preprocessing of images
Assume that the original image is in an uncompressed format and that the pixel values are within [0, 255] and denote the pixel number as N. 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 pixel values are added with pseudo random numbers to mask the original pixel values.

After pixel values are masked, the image is divided into sub images, where every sub image is organized as a data set. Now quantize the values in each data set by adding the values with Hadamard matrix (Hadamard matrix is a matrix made up of +1 and -1). And the same process is continued for all the data sets in the image. And the values are considered as bit streams.

The decoder receives the bit streams, reorganizes as data sets and converts them to sub images and decoding is done. The sub images are converted to original image using the pseudo random values in the range from 0 to 255.

3.1.2. Scalable Coding Algorithm for Image Encryption

**Step1:** Creates a pseudorandom bit order with a length of 8N bit and fix the content holder and the decoder have the equal pseudorandom number generator and a shared secret key used.

**Step 2:** Splits the pseudorandom bit order into N pieces, all which containing 8 bits and convert each piece as an integer number within [0,255].

**Step3:** An encrypted image is formed by a one-by-one modulo 256 additions as follows:

\[ m^{0}(i,j) = \text{mod} [r(i,j)+s(i,j),256], \]
\[ 1 \leq i \leq N_1, 1 \leq j \leq N_2 \]

where R(i,j) represents the gray values of pixels at positions R(i,j), S(i,j) represents the pseudorandom quantities within [0, 255] generated, and m(0)(i,j) represents the encrypted pixel range.

**Step 3:** An encoder does not identify the secret key and the new content, it can still compress the encoded data as a set of bit streams.

**Step 4:** Perform quantization (qn) for the values of encoded pixels (L(t)).

The entire image which are denoted as

\[ qn(1), qn(2), ..., qn(L(t)) \]

**Step 5:** Execute the Hadamard transform in each group.

\[ CK(t) \]
\[ CK(t) = H \]
\[ CK(t)(L(t)) = qn(t) \]
\[ qn(t)(L(t)) \]

Where H is L(t) x L(t) Hadamard matrix.

**Step 6:** Calculate the Compression Ratio

The size of the compressed image S_{comp}.

Now CR = S_{comp}/S_{uncomp}

Size of compressed image = size_in_bytes

Compression ratio: A: B

High class image data needs large volumes of storage space and transmission bandwidth, so the current technology is unable to handle technically. One of the potential solutions to this problem is to compress the data so that the storage space and communication time can be reduced. By using image compression can store the image in compressed manner and can be transmitted faster.
4. RESULT AND DISCUSSION

The application generates key for the user to create a key (integer number) that will be served as the secret key for both encryption and decryption. The warning alerts the user if key generation by system failed due to unforeseen circumstances.

ADVANTAGES

- Pixels are converted to bits.
- No attacker can tamper the contents
- Completely unreadable by human
- Pixel values are masked.
- Image content is not altered during the process

The images are encrypted so that except the licensed user nobody can distribute or sell the image and also prevents from modification of the image. For example academic websites have figures related to study. So encryption of those images prevents from distribution. The images are secured to maintain confidentiality of important data. For example photos of terrorists should not be available to the public. While uploading and downloading images from sites the images are encrypted to prevent from being manipulated by any third party. Because personal images are always prone to attack by malicious users. The encryption of image prevents users from sharing the pictures from one media to another. For example to prevent the stills of yet to release films might be encrypted to prevent from distribution. In web pages that contain sensitive data, images have to be encrypted. Secret or confidential information has to be shared with a wide variety of people who cannot be predicted, and who may occur singly, or in groups. If a hacker tries to save the contents the contents of the image should become unreadable.

Since employee data may include his and his family photos it is important to keep them in encrypted format. So that it benefits the employee as well as the organization. Photos of the recent events or sensitive news may be distributed or be stolen by other sites. So images may be kept encrypted in such scenarios as shown in Fig.3.
Constructed on the integer value $M$ and the Threshold value $T$, compression ratio of new input images are intended. When an encoded image is decomposed within additional levels, more records are involved in compression. Therefore the table 1 shows the PSNR performance is better and PSNR value of different images in shown in Fig.4.

<table>
<thead>
<tr>
<th>Input image</th>
<th>Integer value ($M$)</th>
<th>PSNR value (db)</th>
</tr>
</thead>
<tbody>
<tr>
<td>512X512</td>
<td>24</td>
<td>37.78</td>
</tr>
<tr>
<td>Image 2</td>
<td>24</td>
<td>37.87</td>
</tr>
<tr>
<td>Image 3</td>
<td>24</td>
<td>37.98</td>
</tr>
<tr>
<td>Image 4</td>
<td>24</td>
<td>37.8</td>
</tr>
<tr>
<td>Image 5</td>
<td>24</td>
<td>37.99</td>
</tr>
</tbody>
</table>
Figure 4. PSNR value Vs Integer value for different gray scale images

5 CONCLUSION

This paper has proposed a novel scheme of scalable coding for encrypted images. The original image is encrypted by 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. The produced output was bit streams. 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, the principal content with higher resolution can be obtained when more bit streams are received.

REFERENCE


http://www.iaeme.com/IJMET/index.asp

153

editor@iaeme.com
Encryption and Decryption of Gray Scale Images Using Scalable Coding Mechanism


