A Review on Different Approaches of Selective Image Encryption for Compressed and Uncompressed Images

Anshu Devangan¹ Omprakash Dewangan²

¹²Rungta College of Engineering and Technology Bhilai, (CG), India

Abstract— Due to rich growth of multimedia application it becomes essential to secure and compress the multimedia data. Digital distribution network is a medium used to transfer the multimedia data. It is obvious to provide security against these multimedia data for unauthorized access or use. This is achieved by applying encryption. The encryption is a mathematical process which converts an original message into unintelligible message. There are a lot of encryption rules which can be applied to secure the data before it is stored or transmitted. Security is must for the military images, medical images, satellite images, corporate business images, geographical images (in research) etc. These images are nowadays collected and stored on electronic computers and transmitted across network to other computers or smart phones. A suitable security mechanism is required for such type of confidential digital images. A digital image is made up of various picture elements (pixels). Each of which is a perfect combination of red, green and blue colors and is interpreted as a two dimensional array for gray scale plain. Image encryption techniques try to change the image view from which the original image cannot easily guessed by applying the decryption techniques.

There are various schemes that have been designed for securing digital images which are based on transposition, substitution, combination of transposition and substitution and chaos-based. Transposition simply shuffles the pixels position whereas substitution substitutes the data values with the help of a fixed system like lookup table. For better security the combination of these two schemes can be used also we can use double transposition by applying the transposition twice. Chaos-based schemes are also uses transposition and substitution for data values but with the help of chaotic functions or chaotic (extremely disorganized) maps and are considered to be more promising. The main property of chaos is its sensitivity to initial conditions makes them suitable for real time multimedia transmission.

The properties of chaos include deterministic dynamics, unpredictable behavior and non-linear transform. Newly proposed image encryption techniques also enhance the security level by introducing more than one chaotic scheme for image encryption algorithms.

Many image encryption algorithms have been proposed such as AES, DES, 3DES, blowfish, rijndael, RC4, RC5 etc. These algorithms can be broadly classified as symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography is further divided into block ciphers and stream ciphers and can be used for multimedia security. Traditional encryption schemes like Advanced Encryption Standard (AES) and Data Encryption Standard (DES) provides good security because of good key size but they are time taking schemes and very complex because of multiple processing rounds involved in it hence they are outdated now. These image encryption schemes can be compared with the help of performance parameters like compression friendliness, visual degradation, tunability, encryption ratio, format compliance, cryptographic security etc.

The selective encryption or partial encryption methods provide increased security level because the intruder cannot guess which type of selection criteria is applied. The basic cryptographic algorithms can also used for selective encryption. The criteria of selecting the parts of images for encryption can be different. Different types of encryption and compression methodologies can be used together. The image compression and encryption can be performed in one of the following three ways, first, compression followed by encryption (CE), second, encryption followed by compression (EC) and third, joint compression and encryption.

Key words: Selective Image Encryption, DCT, RC4, AES, Cryptography, DES

I. INTRODUCTION

With the growth of applications exchanging digital images over network, security of images has become an important area of concern. Image security mechanisms are invented to protect the image from various types of active and passive attacks while it is being sent over communication network. To make the image secure from unauthorized access and for the integrity of data we must encrypt the data before it is stored or transmitted. Security is must for the military images, medical images, satellite images, corporate business images, geographical images (in research) etc. These images are nowadays collected and stored on electronic computers and transmitted across network to other computers or smart phones. A suitable security mechanism is required for such type of confidential digital images. A digital image is made up of various picture elements (pixels). Each of which is a perfect combination of red, green and blue colors and is interpreted as a two dimensional array for gray scale plain. Image encryption techniques try to change the image view from which the original image cannot easily guessed by applying the decryption techniques.

Analysis and Cryptanalysis of a Selective Encryption Method for JPEG Images

In this approach author combines JPEG compression and the selective encryption during the Huffman coding stage of JPEG. In the CFB mode, the previously encrypted block is used to encrypt and to decrypt the current one. The proposed SE is applied in the entropy encoding stage during the creation of the Huffman vector. The three stages of the proposed algorithm are: the construction of the plaintext, the encryption of plaintext to create and the substitution of the original Huffman vector with the encrypted information.

The encryption is performed in the Huffman coding stage of the JPEG algorithm using the AES encryption algorithm in the CFB mode. The proposed encryption method does not affect the compression rate and the JPEG bit stream compliance. The selective encryption (SE) is performed only on the Huffman vector bits that correspond
to the AC coefficients as provided by the DCT block of JPEG. The proposed methodology is applied for ensuring the protection of images. Only authorized users that possess the key can decrypt the entire encrypted image sequences. The proposed method has the advantage of portability on mobile devices, which currently embed the JPEG image compression algorithm, which corresponds to their low computational requirements [4].

B. Selective Image Encryption Using DCT with Stream Cipher

This paper [5] presents a new effective method for selective image encryption that employs DCT for compression and RC4 stream cipher for encryption. DCT is a very commonly used compression technique where the image is decomposed into 4x4 or 8x8 blocks. The blocks are then transformed from the spatial domain to the frequency domain by the DCT. In order to generate coefficient sequence ordered from the low spatial domain frequencies to the higher spatial domain frequencies DCT block is scanned in zigzag order. Then the DCT coefficients correlated to the lower frequencies of the image block are encrypted using the RC4 Stream Cipher. The image details are situated in the lower frequencies and the human is most sensitive to the lower frequencies than to the higher frequencies so that only some selective DCT coefficient related to lower frequencies are selected for encryption. Before decrypting the image the IDCT and block shuffling is performed respectively.

The proposed encryption method uses the Selective Encryption approach in which only the DC coefficients and some selective AC coefficients are encrypted because the DC coefficients carry important visual information, and it is difficult to predict the selective AC coefficients. Rest of the AC coefficients are not encrypted, this give a high level of security. In order to make the algorithm more effective and secure an extra security has been added as shuffling the blocks of encrypted image.

RC4 is a good, widely used, fast, simple and secure encryption algorithm. Due to the selective encryption approach with RC4 this methodology takes less time for encryption and decryption hence concluded as a fast methodology. Idea of block shuffling makes the algorithm more secure.

C. Analysis and Implementation of Selective Image Encryption Technique using Matlab

In this paper [6] the basic idea is provided by the author that how to implement and analyses the selective image encryption technique using matlab. The proposed selective encryption scheme starts with compressing the input image. After that a message is embedded with the compressed image and encrypted using the key. The exact reverse process is performed at the receiving end. The author shows that at the receiving end if someone how does not have the key can only decompress the image and get an altered image. The steps involved in the complete proposed technique are input the image, save the R, G, B pattern matrix in a variable, pixel value replacement by another value generated by any random number generator, XOR the random number with the input image pixels, get the output as encrypted image.

D. Selective Image Encryption for Medical and Satellite Images

In this paper [7] the author says that the selective image encryption can be performed in two ways: manually or automatically. According to this the two types of selective encryption methodologies are described for medical and satellite images. In the first method image to be encrypted is first divided into sub blocks and then fed into encryption block. Block selection is to be done manually before encryption. Encryption block has two inputs one is selected block and second is map image. Using map-based encryption technique selected blocks are partially encrypted. Complete encryption of selected blocks is also possible and each block can use separate map-image. In the second method for selective image encryption region of interest is located using morphological operation and selected regions are encrypted using map images and rest of the process is similar as in first method. First approach for selective encryption is very useful when the area or region of interest is known. Second approach for selective encryption is useful when focused objects are present in an image, so that it is possible to detect and select the region of interest in that image.

E. Selective Encryption Techniques of JPEG2000 Code stream for Medical Images Transmission

An efficient selective encryption should possess the basic properties like compressibility equivalent, complexity equivalent, backward compatible and computationally secure.

In this paper two novel selective encryption image schemes based on JPEG2000 are proposed. The first one encrypts only the code-blocks corresponding to some sensitive precincts. In order to improve the security level author introduce the permutation of codeblocks contributing in the selected precincts. The idea of combining permutation and selective encryption is used in order to minimize the amount of processed data encryption while ensuring the best possible degradation through the permutation.

For selectively encrypting the JPEG 2000 bitstream format compliance should be achieved. The aim is to operate directly on the bitstream without any decoding. The discrimination of packet data from packet headers in the bitstream can be achieved by using two special markers “Start of Packet: SOP” and “End of Packet Header: EPH”. The packet header is located between the subsequent SOP and EPH and the packet data may be located between EPH and the subsequent SOP. The two schemes are; first, selected codeblocks permutation and encryption and second, codeblocks encryption combined to packets header permutation.

In first scheme the formatter receives non encrypted and encrypted packets and works to reconstruct a compliant partially permuted/encrypted codestream. The block packets processing is used to only encrypt codeblocks or to permute and encrypt them. The permutation of codeblocks contributing in the selected precincts is introduced to improve the security level [8].

In second scheme the JPEG2000 codestream input to the selection precincts block where sensitive precincts are selected. The remaining codestream and the selected packets are input to the packets analyser. All packets headers are
separated from the bodies packets and a cyclic permutation of all the header packets are performed and encryption is performed on only bodies of selected packets. At last the header packets, selected bodies packets and remaining bodies packets are combined to form the encrypted image.

F. RC4 Enrichment Algorithm Approach for Selective Image Encryption

In this paper [9] author introduces the RC4 enrichment algorithm derived from the standard RC4 algorithm to make the algorithm stronger and to avoid various attacks. The procedure of selection of specific portion of images is based on the selection algorithm. The paper uses two algorithm one for selection of image part and second for encryption of the image. First of all the selection algorithm is applied to the original image. The steps involved in the selection algorithm are input the original image, choose the way of selection, call the array file and store the image, select the art of the image, store the image. The selection algorithm selects the sensitive parts of image for encryption and the image matrix is created. Then encryption is applied using the RC4 enrichment algorithm. Decryption process is the exact reverse of the encryption process. Finally the decrypted image is combined with the non selective parts of image.

G. Selective Encryption Algorithm for GIS Vector Map using Geometric Objects

In this paper [10] the proposed algorithm is concerned with security of GIS vector maps in DCT domain. A vector map data is the combination of attribute information, display information and geographic information. The attribute information and display information are stored as text and the geographic information is stored as geometrical object like polyline and polygon. The vector map is decomposed into layers. Layers containing text are goes for vector encryption and layers containing polylines and polygons are goes for selective encryption. All the layers are then combined to form the encrypted vector map.

In the process of selective encryption objects are considered as a 1D vector. The basic steps of selective encryption for each layer are objects clustering, finding of maximum number of vertices of an object among objects in a layer, random coefficients generation, verticalization, 1D-DCT, DC values encryption and inverse 1D-DCT. Clustering is performed to identify objects by groups. Each layer contains different number of DC values. The selection of clustering algorithm and the number of groups are the user’s choice. Selective decryption steps are objects clustering, finding of maximum number of vertices of an object among objects in a layer, random coefficient generation, 1D-DCT, DC values decryption, inverse 1D-DCT and inverse verticalization.

H. A Fast Partial Image Encryption Scheme with Wavelet Transform and RC4

Wavelets are mathematical functions that cut up data into different frequency components. Wavelet algorithms process data at different scales or resolutions. The wavelet transform carries out a special form of analysis by shifting the original signal from the time domain into the time–frequency, or, in this context, time–scale domain [11].

In the proposed method very first the four types of coefficient matrices are generated: horizontal matrix (ch), vertical matrix (cv), diagonal matrix (cd) and approximation matrix (ca). The ch, cv and cd matrices are not encrypted and shuffled to provide high level of security. The ca matrix contains the lowest frequency sub-band and goes for encryption. The ca coefficients are simply XORed with RC4 keystream. The final encrypted image is obtained by performing inverse DWT of encrypted ca matrix and shuffled ch, cv and cd matrices.

I. Multiple Selective Regions Image Cryptography on Modified RC4 Stream Cipher

Normally cryptography begins with taking an image as an input and then applying the required algorithm encrypting the image that is called encrypted image. But for selected image encryption first we need to specify the regions we are going to encrypt. Then the encryption algorithm works. With the help of the algorithm the selected parts of the image is being encrypted and the other parts remains the same. After the end of this process we got the encrypted image. By applying the same algorithm we again decrypt the selected regions. After the end of this step we again got the original image back [12].

In the proposed methodology the selected sensitive part and non-selected part of the image is separated first. Sensitive part of the image is converted into image matrix and then encrypted using modified RC4 algorithm. The decrypted image is added to the non-selected part of the image to get the original image.

J. Selective Image Encryption with Diffusion and Confusion Mechanism

In this paper [13] the proposed methodology includes two approaches; the selective encryption is combined with the chaotic encryption. The image encryption starts from image conversion i.e. from RGB color model to the YCbCr color model. The Y component image is selectively encrypted and shuffled iteratively using 2D Arnold Cat Map and Cr and Cb components are row-column wise scrambled. Image encryption performs by diffusion or substitutes the shuffled image of Y component and scrambling Cb, Cr components through changing the value of each of Y, Cb, and Cr pixels through XOR operation with the sequence key values dedicated for each component.

K. Selective Image Encryption using One Way Hash Technique

The proposed methodology extends the SHA-2 (secure hash algorithm) and enhances the strengths of it. The basic steps involved are hash key generation, processing of image, binary image conversion, extension of key, pixel substitution and decryption. First of all a password obtained by the user is applied to SHA-512 logic to produce a message digest of binary string of length 512. The hash value is then converted into a matrix and resized. The result is then transformed by DCT followed by FFT and then XORed with the image bit stream. The result is then converted into grayscale values and then reshaped to form the ciphered image. The result of this is the new ciphered image obtained by pixel substitution (shuffling of rows) on the randomized image.
L. Selective Image Encryption Using DCT with AES Cipher

The proposed method based on the idea of decomposing the image into 8x8 blocks, these blocks are transformed from the spatial domain to frequency domain by the DCT. Then, the DCT coefficients related to the higher frequencies of the image block are encrypted using the AES cipher. The concept behind encrypting only some selective DCT coefficients based on the fact that the image details are situated in the higher frequencies. In fact the image encryption algorithm obtains higher security when DCT coefficients related to the lower frequencies are encrypted than those related to higher frequencies [15]. The basic steps involved are DCT, decomposing of image into blocks, DCT on each block, encryption, IDCT on each block and IDCT.

III. CONCLUSION

The aim of the paper is to study the various methods and understanding the principle involved in different steps of selective image encryption. Selective image encryption is applied on image for compression and secure transmission of multimedia data over insecure communication channel. Compression is applied so that file takes less space whereas encryption is applied to secure the data from unauthorized access.

REFERENCES


