Region Based Selective Image Encryption

K. C. Ravishankar, M.G. Venkateshmurthy
Department of Computer Science and Engineering,
Malnad College of Engineering, Hassan, Karnataka, India
E-mail: kcrshankar@gmail.com , muthu_gowri@yahoo.co.in

***Abstract*-Image security has found a great need in many applications where the information (in the form of image) is to be protected from unauthorized access. Encrypting the image makes this possible. Several schemes for image encryption have been proposed. These schemes produce randomness in the image so that the content is not visible. Encryption and decryption consume a considerable amount of time. So there is a need for an efficient algorithm. In this paper, a region based selective image encryption technique is proposed which provides the facilities of selective encryption and selective reconstruction of images. Simulation results are presented and a comparative analysis of the proposed technique with the conventional methods is discussed. Also, the efficiency considerations and advantages of the new technique over the conventional methods are highlighted.**

I. Introduction

In recent days, image security has found a place in many applications like internet banking transactions, military image database and communication, document storage systems, and medical imaging systems. Image encryption has gained a lot of focus in the field of image processing. The very fact that the data has to be encrypted to maintain the secrecy involved in it makes it very attractive for a detailed study. Encryption was first being studied and applied for all kinds of information in the same way. This is no longer sufficient. Image encryption differs from data encryption. Different representations of information like text, images, audio, video, etc, have to be treated individually in a specific manner so that features specific to each of them are analyzed and appropriate techniques are applied. Application of text encryption techniques on images may not completely hide all the image features and hence, proper encryption of images can not be achieved. The image features can be used to provide a greater level of security. Robust image encryption algorithms are required to make the images sturdy against possible attacks.

Large amount of processing is involved in image encryption. This demands for an efficient algorithm that reduces the overhead involved in encrypting the image. This problem can be handled in many ways. One way is to look in to the image for the presence of information that is more sensitive which needs protection, and to encrypt only such parts. In many applications there is no need to encrypt the whole image, for e.g., in a bank draft/ cheque, only the signature, the amount and the seal of the bank need to be protected. In other applications, whole of the image may be encrypted but only a part of it needs to be deciphered.

The concept of region based selective image encryption finds use in time-critical applications wherein security is also a concern such as, internet banking transactions, military image database and communication and medical imaging systems. Special and reliable security in transmission of digital images is needed in many applications, such as pay-TV, confidential video conferencing and corporate communications. Looking at the requirements of the hour and the existing techniques, the idea of region based selective image encryption finds a prominent place in the field of image security.

II. Previous Work

Some of the existing techniques of image encryption and how they motivate the technique proposed in this paper have been presented in this section.

A. Encryption Techniques

Encryption techniques are generally categorized into

- Position permutation techniques
- Value transformation techniques, and
- Combination of both.

Position Permutation:

The chaotic key based image encryption technique (CKBA technique) proposed by Yen and Guo [1] presents an algorithm that uses *position permutation* to reorder individual pixels of an image so that the original information is not visible. The concept of chaotic image encryption is based on a chaotic system that generates a binary sequence which is a function of the key. This binary sequence is used to rearrange the pixels of the image by rotating the pixels row-wise, column-wise, along the diagonal and anti-diagonal directions. The value of the bit in the sequence decides the direction of rotation.

In this technique, the entire image is encrypted and decrypted each time, which is a big overhead in case of storage and retrieval of a large set of images in an image database or transmission of images over an insecure channel. Also the loss of even a small part of the encrypted image results in greater distortion in the decrypted image. This is because of the fact that the part of the encrypted image which is distorted constitutes pixels that will be scattered in the decrypted image.

1-424-0220-4/06/$20.00 ©2006 IEEE.

Value Transformation:

A new chaotic neural signal security system proposed by J C Yen and J I Guo [4] uses *value transformation* technique. The weights and biases of the network are set according to a binary sequence generated from a chaotic system, for encryption or decryption of each signal element.

Combination:

Position permutation and value transformation can be combined. For example, the Space Filling Algorithm uses space-filling curves for pixel permutation and large period pseudo-random number generators for pixel value substitution. The algorithm uses a variable-length key (at least 64 bits long), and satisfies properties such as confusion, diffusion and the strict avalanche criterion.

B. Selective Encryption

The idea of selective encryption is being followed in various applications. This is used mainly to reduce the overhead involved in data transmission over secure channels. The paper by Marc Van Droogenbroeck and Raphael Benedett [2] presents a technique for selective encryption of compressed and uncompressed images. The selective encryption technique is depicted in Fig. 1:

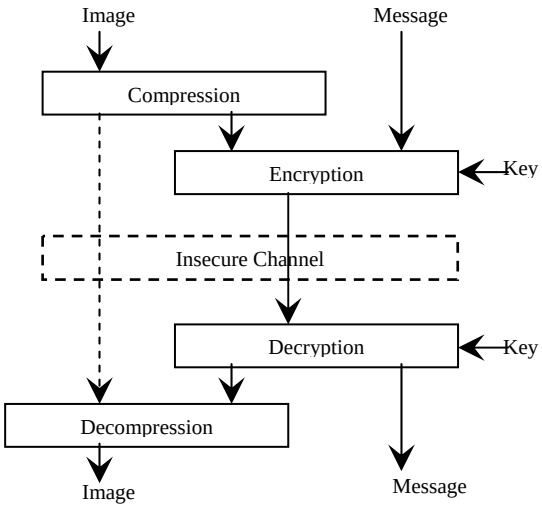

Fig. 1. Selective encryption mechanism.

The general selective encryption works as follows. The image is first compressed (if needed). The algorithm only encrypts part of the bit-stream with a well proven ciphering technique; incidentally a message (a watermark) is added during this process. To guarantee a full compatibility with any decoder, the bit-stream should only be altered at places where it does not compromise the compliance to the original format. This principle is sometimes referred to as *format compliance*. With the decryption key, the receiver decrypts the bit-stream, and decompresses the image. In principle, there should be no difference between the original image and the image that has been encrypted and decrypted. However there might be slight, though invisible, difference if a watermark message has been inserted in the image.

III. Proposed Region Based Selective Image Encryption

The proposed Region Based Selective Image Encryption technique is a new approach to image encryption. The main idea is to follow a selective approach for both encryption and decryption. The model for region based selective image encryption is shown in Fig. 2.

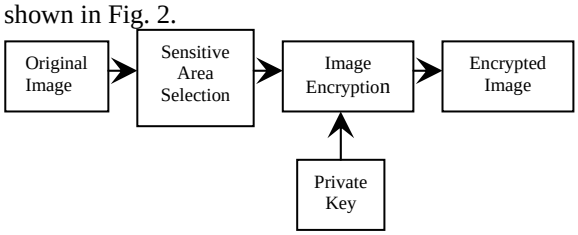

Fig. 2. Schematic of Region Based Selective Image Encryption

A. Encryption Process

The encryption process is shown in Fig. 3. The original image is first processed for feature extraction that involves identification of sensitive areas, which are marked. The image is then segmented into regions of a given block size. Then, all the regions that contain the sensitive area (partly or fully) are encrypted and other regions are left as they are. The regions (both encrypted and non-encrypted) are permuted.

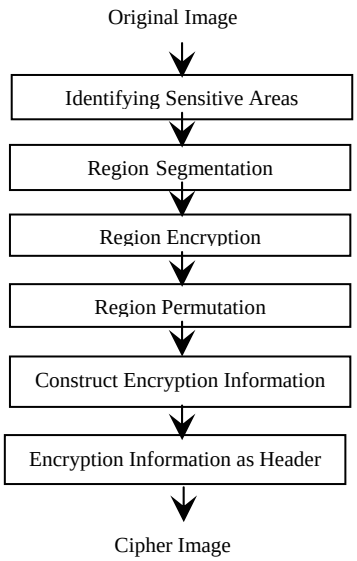

Fig. 3. Schematic of Region Based Selective Image Encryption Technique

Different block sizes are considered for region segmentation. Various algorithms are used for encryption and permutation. All these parameters form the encryption information. The encryption information is added to the cipher image.

Identify sensitive areas:

With the perspective of selective encryption of images, the image has to be first searched for the presence of sensitive regions and also looked for the regions that can be left out of encryption process. Here the user can mark the sensitive regions. Once the required regions are identified, further processing can be done.

Region Segmentation

Consider an image $I = p_1, p_2, p_3 \ldots p_K$ of size $K=2^n$ and $K=m$ x m for some integers m and n, where p_i represents the i^{th} pixel of the image.

The whole image is divided into regions based on:

1. *Number of blocks*: The number of blocks N_b is determined such that: $N_b = 2^q \; x \; 2^q$ for some integer $q>0$ where $N_b<K$.
2. *Block size*: The size of a block B_s is determined such that: $B_s=2^q$ and $B_s<m$, for some integer $q>0$

The segmentation is represented using a square matrix containing a total of N_b number of elements. Each element of this matrix holds the index of a region in the image. This representative matrix is used for performing the operations on regions. The blocks obtained by the above operations represent the regions. Each region is considered separately for encryption.

Region Permutation

Region permutation deals with scrambling the regions of the image in a definite manner. This is done in order to induce disorderliness in the visibility of the image. By doing permutation, the regions are trans-positioned to new locations. The algorithms employed for this purpose need to be efficient to induce enough randomness and simple enough to retrace back. Several of the techniques known for matrix permutation are applied to the image as the regions are represented in a matrix form. Following algorithms are used for permuting the regions.

- *RC Permutation*: Regions are numbered in a chosen order, e.g. row-wise. They are then reordered using transposition techniques. The reordering sequence is decided by the key. If the regions are numbered row-wise, they are collected column-wise according to the key. Otherwise if they are numbered column-wise, they are collected row-wise. For example,

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Key - 3142 ⇒

2	6	10	14
4	8	12	16
1	5	9	13
3	7	11	15

Fig. 4. Original and Permuted Matrix

Doing so will mix the cells. But still there exists some statistical relationship between them. This can be diluted by repeatedly applying the permutation.

- *Z-Permutation*: In this method of permutation, the cells of matrix are collected along the diagonal or anti-diagonal direction. The Fig. 5 illustrates the action.

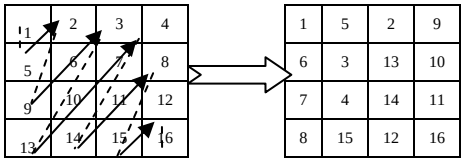

Fig. 5. Original and Permuted Matrix

- *Random Sequence*: A random sequence is generated from *1* to *n*, where *n* is the number of regions, such that all the numbers from *1* to *n* occur exactly once. The random sequence is a function of the key and sufficiently unique i.e. the wrap around space is large.
- *Chaotic Reordering*: The chaotic system itself can be used to permute the regions instead of individual pixels. Here the region is considered as a single unit instead of pixels. The key is used for generating the chaotic binary sequence.

Such transpositions are applied repeatedly to get a permuted sequence of regions. The reordering of the regions has the advantage that it makes it difficult to find the original position of the region in the encrypted image, thereby making cryptanalysis difficult. For permuting the regions, permutation algorithms are applied on the matrix that represents the region segmentation. At the end, the resultant image is constructed by looking at the indices in the representative matrix.

Region Encryption

The regions obtained are considered separately for encryption. Only the regions that contain the selected area are encrypted. Various well known algorithms are used for encrypting the regions. The encrypted regions are permuted with the unencrypted regions using region permutation algorithms to provide one more level of security.

Construction of Encryption Information Key

When multiple regions are selected and encrypted, the information regarding the region segmentation, permutation, and encryption has to be maintained in order to help in the reconstruction of the image contents. Encrypted images are usually transmitted or stored in electronic form. In case of electronic transmission, the encrypted image is sent as a file. Hence the key information can be attached or embedded in the image file itself. But keeping it in plain causes security concern. To counter this problem, the information is encrypted using a suitable algorithm like DES and appended to the image file. Also, different regions in an image may be encrypted using different keys. For this, a general model of information construction is devised. Following are the parameters that need to be maintained:

- Region id
- Block size
- Region permutation algorithm index
- Region Encryption algorithm index
- Co-ordinates and Size of Encrypted area in case of selective encryption

All these parameters are to be combined suitably and efficiently. The term *suitably* refers to ease of setting and accessing the required parameters and the term *efficiently* refers to using minimum possible space for storing the parameters. This can be implemented by the following model:

- The resultant information is a string representation of the *Long* value.
- A *Long* value can account for 8 bytes i.e. 64 bits.
- Appropriate number of bits is reserved to store a particular parameter.

63-56	55-45	44-34	33-23	22-12	11-8	7-4	3-0
id	h	w	sx	sy	REA_i	RPA_i	b

Fig. 6. Encryption information key

id- Selected region id
sx- Starting x coordinator
sy- Starting y coordinator
RPA_i- Region Permutation Algorithm index
h-Height of the region
w-Width of the region
REA_i- Region Encryption Algorithm index
b-Block size

- Bit operations are used for setting and accessing the required bits. The information is inferred from the value of the bits.

B. Decryption Process

The decryption process starts with the extraction of encryption information which is in the header. The parameters are retrieved and the encryption mechanism is determined. The image is partially or fully decrypted. In case of partial/ selective decryption, the user selects the areas of the image to be decrypted. Only those regions are decrypted.

Retrieving the Encryption Information

The encryption information needs to be obtained before proceeding with decryption. It is obtained from the *Encryption Information* that was constructed by the encrypter.

Selective Reconstruction

The user is allowed to select the part of the image that is to be reconstructed. Such a facility may be useful in cases where the user needs only some particular information. For e.g., a signature authentication system may need to decrypt the area containing the signature. The encrypted image contains the regions in a scrambled fashion. This scrambling has to be reversed. This is done by applying the inverse permutation using the shared key. The block size and algorithm information are obtained from the encryption information. The coordinates of the selected area are used to find out the encrypted regions that fall in the selected area, for decryption.

C Advantages of Selective Region Based Image Encryption

The advantages of the proposed technique are as follows:

- The region based approach for encryption of the images is faster with appropriate block-size.
- Selective encryption approach reduces the overhead of encrypting the non-sensitive areas.
- Loss of information is less, as errors are localized to the regions which are associated with the areas that are affected by noise.
- The region based approach enables selective decryption of images.
- Selective decryption reduces the overhead involved in decrypting the unwanted regions and hence makes the decryption faster.
- It is possible to encrypt different parts of the image using different keys (multiple encryptions).
- The algorithm can be parallelized for higher performance.

IV Complexity Analysis

The complexity and performance of the proposed Selective Region Based algorithms and comparison with the conventional techniques is discussed in the following sections.

A. Encryption Process

The performance of each component of the encryption process is discussed separately.

- *Identifying sensitive areas:* It involves the user selecting the required regions to be encrypted. The encryption process is concerned with encrypting only the pixels that fall under the enclosing rectangle of the selected region. The complexity calculation narrows down from the size of whole image to the size of the enclosing rectangle. So the time complexity can be represented as:

$$T_{sel} \ \alpha \ W_{sel} \, x \, H_{sel}$$

Where,
W_{sel} is the width of the selected area,
H_{sel} is the height of the selected area.
$W_{sel} \, x \, H_{sel}$ represents the number of pixels in the selected area.
The encryption time is proportional to the number of pixels encrypted. For multiple selections, the sum of encryption times of selected areas is the total encryption time. This total encryption time is less compared to the encryption time involving the whole image.

- *Region Segmentation*: This step deals with dividing the whole image into N_b number of blocks (regions). The task involves creating new buffers for regions, copying the pixel values to the region buffers, and other related processing. It can be observed that the time required to segment a given image is based on N_b. So, the segmentation time T_s can be represented as: $T_s \ \alpha \ N_b$

- *Region Permutation*: This step deals with scrambling the regions of the image in a definite order. Permutation algorithms are applied on representative matrix which contains N_b elements. Each element represents the corresponding region in the original image. This representation makes the task of applying region permutation algorithms easy. After the completion of permutation, the representative matrix is scrambled. The scrambling reflects the scrambling of regions. The regions are arranged according to the representative matrix to form the final scrambled image. The processing depends on the algorithm chosen for permutation. The total number of operations is proportional to number of blocks N_b. The permutation time T_p can be represented as: $T_p \ \alpha \ N_b$
- *Region Encryption*: The regions are individually considered for encryption. The processing depends on the algorithm chosen for encryption. The encryption algorithms operate on all the pixels in the region. The encryption time T_e can be expressed as:

  $$T_e \ \alpha \ N_b \, x \, B_s^2$$

  Where, B_s^2 represents the number pixels in a region of block size B_s.

B. Decryption Process

Selective *reconstruction*: This involves decrypting only the selected number of regions, N_{sr}. The decryption time T_d can be expressed as:

$$T_d \ \alpha \ N_{sr} \, x \, B_s^2$$

Where, B_s^2 represents the number pixels in a region of block size B_s.

Prior to decryption, the scrambling of the representative matrix has to be done in order to locate the regions that fall under the selected area. Hence, the permutation time T_d. is also added to the total decryption time

As seen in the above discussion, the encryption time depends on the segmentation i.e. the Number of blocks(N_b), or the Block size (B_s).

V. Experimental Results

The proposed technique has been applied to a number of sample images. The sample images chosen for the experiments are square images of the order $m \, x \, m$, where $m = 2^n$.

The original image of size 512 x 512 is shown below:

Fig. 7. Original (Lenna) image

Fig. 8 shows encrypted images of the above original for different block sizes. The image is encrypted using chaotic key algorithm. These images, on decryption, matched the information in the original image perfectly.

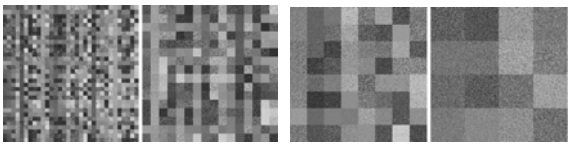

Fig. 8. Encrypted images of Lenna for block sizes 16, 32, 64, 128

- *Selective Encryption*: Fig. 9(a) shows an image marked for selective encryption. The portion of the image that falls under the bounding rectangle is the candidate for encryption. Fig. 9(b) shows the result of applying selective encryption.

a b

Fig. 9. a. Image marked for selective encryption
b. Result of selective encryption

- *Selective reconstruction of images*: Fig. 10 shows an encrypted image marked for selective reconstruction. Regions that enclose the marked part are shown by the bounding rectangle. Fig. 11 shows the result of applying selective reconstruction

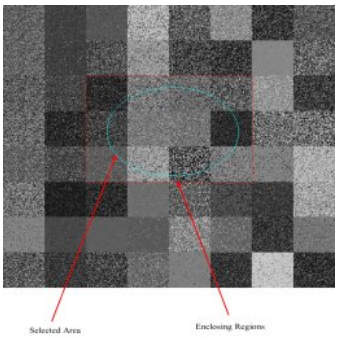

Fig. 10. Regions marked for selective decryption

Fig. 11. Result of applying selective decryption

Table 1 shows the result of the experiment. The chaotic algorithm was applied for both region permutation and region encryption. The block size was varied and the time count was noted. The values

are obtained by taking the average over repetitive tests.

TABLE 1
ENCRYPTION TIMES FOR DIFFERENT BLOCK SIZES

Block Size	Time Taken (in units)
1	344
2	315
4	198
8	171
16	131
32	141
64	159
128	171
256	180
512	189

The values in Table 1 are plotted as in Fig. 12. The graph clearly shows the dependence of encryption time over the block size. For comparison, the behavior of chaotic algorithm, applied to whole image, is also shown.

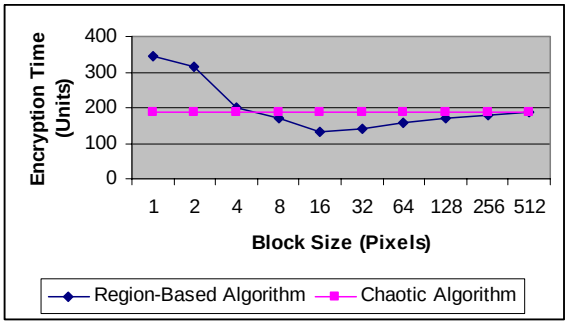

Fig. 12: Behavior of Encryption time on Block Size

As observed in the graph, the curve initially dips down as the block size is decreased and then rises when continued further. The optimal point is the one where the curve has its minima. In the graph, it is for block size 16. So, an optimal value for block size has to be chosen for region segmentation.

VI. CONCLUSIONS

Here, it is pointed out that the conventional methods that act on whole images are not efficient. The problems faced by the conventional encryption schemes are identified. The new approach to image encryption and reconstruction tries to solve these problems. The proposed technique segments the image into regions of fixed size. These regions act as units for processing the image. Selective Encryption makes it possible to encrypt only a part of the image leaving the rest of the image unaltered. Here, the regions covering the part of the image are considered for encryption. Selective Reconstruction deals with decrypting only a part of the encrypted image. Both the methods give a fair amount of reduction in the encryption time. In case of Selective Encryption, the sensitive regions are marked by the user. Experiments were conducted on a number of sample images and the simulation results are analyzed. A comparative analysis is made to prove the effectiveness of the proposed technique.

The proposed selective region based image encryption technique also has an added advantage. Once the segmentation and permutation of regions is completed, the regions are encrypted independently. Encryption of one region is in no way concerned with encryption of other regions. The processes are mutually exclusive. This fact can be carried further to speed up the encryption process. Parallelism in encrypting the regions can be exploited to further enhance the performance. On a uniprocessor system, threading can be used.

In this paper, grayscale images only have been considered. The technique can be extended to colour images. Artificial Intelligence techniques can be applied for recognizing sensitive contents of an image.

REFERENCES

[1] Jui-Cheng Yen and Jiun-In Guo, "A New Chaotic Image Encryption Algorithm", *IEEE Int. Conf. Circuits and Systems*, 2000, Vol. 4, pp. 49-52.

[2] Marc Van Droogenbroeck and Raphael Benedett, "Techniques for a selective encryption of uncompressed and compressed image" , *ACIVS 2002 Proceedings*, September 9-11, 2002.

[3] Marc Schneider and Shih-Fu Chang, "A Robust Content Based Digital Signature for Image Authentication", Columbia University, Image and Advanced Television Laboratory, New York.

[4] J.C. Yen and J.I. Guo, "The Design and Realization of a Chaotic Neural Signal Security System", *Pattern Recognition and Image Analysis*, 2002, Vol. 12, No. 1, pp. 70-79.

[5] Shujun Li and Xuan Zheng, "Cryptanalysis of a Chaotic Image Encryption Method" *Proceedings of 2002 IEEE International Symposium on Circuits and Systems (ISCAS 2002), vol. II pp. 708-711, 2002.*

[6] Nam-Deuk Kim and Alastair Reed, "Content-based Digital Watermarking using Contrast and Directionality" *PICS 2002,Portland, Oregon, pp. 232-236, 2002;.*

[7] Peng Chang and John Krumm, "Object Recognition with Color Co-occurrence Histograms", *IEEE Conference on Computer Vision and Pattern Recognition, Fort Collins, CO*, June 23-25, 1999.

[8] Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing", second edition, Pearson Education, 2003.