Journal of Zhejiang University-SCIENCE C (Computers & Electronics)
ISSN 1869-1951 (Print); ISSN 1869-196X (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Performance study of selective encryption in comparison to full encryption for still visual images

Osama A. KHASHAN, Abdullah M. ZIN, Elankovan A. SUNDARARAJAN

(*Centre for Software Technology and Management, Faculty of Information Science and Technology,
National University of Malaysia (UKM), Bangi 43600, Selangor, Malaysia*)

E-mail: o_khashan@yahoo.com; amz@ftsm.ukm.my; elan@ftsm.ukm.my

Received Sept. 18, 2013; Revision accepted Jan. 22, 2014; Crosschecked May 4, 2014

Abstract: Securing digital images is becoming an important concern in today's information security due to the extensive use of secure images that are either transmitted over a network or stored on disks. Image encryption is the most effective way to fulfil confidentiality and protect the privacy of images. Nevertheless, owing to the large size and complex structure of digital images, the computational overhead and processing time needed to carry out full image encryption prove to be limiting factors that inhibit it of being used more heavily in real time. To solve this problem, many recent studies use the selective encryption approach to encrypt significant parts of images with a hope to reduce the encryption overhead. However, it is necessary to realistically evaluate its performance compared to full encryption. In this paper, we study the performance and efficiency of image segmentation methods used in the selective encryption approach, such as edges and face detection methods, in determining the most important parts of visual images. Experiments were performed to analyse the computational results obtained by selective image encryption compared to full image encryption using symmetric encryption algorithms. Experiment results have proven that the selective encryption approach based on edge and face detection can significantly reduce the time of encrypting still visual images as compared to full encryption. Thus, this approach can be considered a good alternative in the implementation of real-time applications that require adequate security levels.

Key words: Selective image encryption, Edge detection, Face detection
doi:10.1631/jzus.C1300262 **Document code:** A **CLC number:** TP309

1 Introduction

Recently, the rapid growth in multimedia technology and the rapid increase of Internet use have introduced a great number of users to generate, transmit, and store a huge amount of digital images with private information. Unfortunately, numerous potential threats violate the privacy of the content, in both storage and transmission domains. In accordance with these growing threats, the security of digital images has become a major challenge in the digital age.

One of the most effective approaches to deter malicious attacks while preserving confidentiality and achieving access control of digital images is through encryption. Nevertheless, the huge size, complex structure, and statistical properties of digital images make the computational overhead and processing time involved during encryption and decryption a major bottleneck, especially for real-time applications.

Several encryption schemes have been proposed with respect to the approach in construction for both storage and transmission domains, which are generally categorized into full encryption and selective (or partial) encryption schemes. Encryption operation involves implementing encryption methods to entire or partial image information using either standard block ciphers like AES and DES, or stream ciphers. Furthermore, several random position permutation algorithms (Li *et al.*, 2008; Li and Lo, 2011; Zhang *et* *al.*, 2013a) and chaotic based cryptosystems (Liu and Wang, 2010; Bhatnagar and Wu, 2012; Zhang *et al.*, 2013b) have been used to encrypt entire or partial image data.

However, the security level provided by the random position permutation schemes is frail under the known-text attack and several decryption methods have been proposed to recover the corresponding original image (Zhao *et al.*, 2004). On the other hand, the main constraint of chaos based encryption schemes is that the finite accuracy of numerical calculations can lead to an arbitrary change of major chaos properties such as the external parameters or initial conditions. Furthermore, most of chaos cryptosystems have shown some weaknesses against one or more attack types. Although their performance is generally high, their security is unlikely to compete with the security levels provided by standard ciphers (Amigó *et al.*, 2007; Kulkarni *et al.*, 2009).

Selective image encryption is a current research trend being investigated to minimize the encryption time of digital images. It does not strive for maximum security, but trades off security for computational complexity. It involves representing the most meaningful parts of an image. Consequently, the encryption process is carried out on the most significant bits, pixels, or blocks using three major encryption techniques: value substitution, scrambling positions, or a combination.

Typically, full and selective image encryption schemes depend on whether the image is compressed or uncompressed. The original image is viewed as a 2D array of pixels. Full image encryption is realized by treating the 2D array of pixels as a 1D textual bit stream. Therefore, any conventional cryptographic technique can be applied directly to encrypt the entire bit stream or the entire compressed encoded bit stream.

When selective encryption is applied on still visual image data, visual inspection methods are carried out first to determine the most meaningful optical parts of the image, according to various aspects, such as boundaries or object backgrounds, followed by encryption; other parts of the image are left unencrypted. On the other hand, selective image encryption schemes in the compression domain are accomplished mainly in respect to compression execution. Here, selective encryption can be carried out before compression on raw image data or during image compression stages, in addition to the partial encryption of a compressed encoded bit stream (Kulkarni *et al.*, 2009). Accordingly, to meet the selective encryption schemes in the compression domain, many studies have looked into how to overcome the security and computational complexity problems of selective encryption of digital images at different compression stages.

In this paper, the feasibility and performance of selective image encryption of the pixels domain are studied, and the results are compared with those of full encryption for still visual colour images. Here, only two methods are studied, namely edge and face detection methods, to identify the semantic parts of an image, since the maximum information of an image is presented in the image edges and human faces. This process aims to select and use the edge or face detection methods with minimum computational costs. Subsequently, all the indicated significant pixels will be transparently encrypted using a fast symmetric encryption algorithm.

2 Overview

2.1 Methods for selective image encryption

Selective image encryption before compression can be realized in the spatial domain by decomposing the image into bit-planes. Consequently, encryption is accomplished by encrypting a subset of the most significant bit-planes, according to Podesser *et al.* (2002), Norcen *et al.* (2003), and Subba Rao *et al.* (2006), since the significant bit-planes have higher adjacent correlations and carry more perceptual information. Another method presented by Droogenbroeck and Benedett (2002) encrypts a subset of the least significant bit-planes, because they appear more random and encrypting them can add noise to an image. Nevertheless, applying a selective encryption approach before compression can significantly affect the statistical and structural properties of an image. Moreover, it generates extra overhead during compression and hence results in severe limitations in image compressibility (Lian and Chen, 2013).

Selective image encryption schemes can be obtained during the compression stages. A JPEG image is the most standard compression scheme used to represent an image to greatly save the storage space and the transmission band of the images. Therefore, it has been widely explored in research for protection (Zhang and Zhang, 2013).

Most selective encryption schemes for JPEG images encrypt a selected number of DC or AC coefficients when the image is transformed into the frequency domain using discrete cosine transform (DCT) (Droogenbroeck and Benedett, 2002; Stutz and Uhl, 2006; Krikor *et al.*, 2009). Selective encryption can be applied to the DCT coefficients during the vector quantization phase (Chen *et al.*, 1998). Moreover, encryption can be combined with the entropy-coding phase into a single step (Puech *et al.*, 2013; Zhang *et al.*, 2013c), hence reducing the computational time and maintaining format compliance and compression rates. In addition, other coding-based selective encryption schemes have been proposed for wavelet-based image compression for JPEG2000 (Martin *et al.*, 2005; Flayh *et al.*, 2009), or by using an embedded bit stream, like SPIHT (Zhang and Wang, 2013), or for quadtree based image compression (Cheng and Li, 2000).

As a matter of fact, selecting an appropriate partial encryption scheme is an important step in selective encryption in order to reduce computational time and resource consumption, while maintaining security of the digital image. However, an inappropriate choice can lead to a computational overhead similar to that of full encryption, which provides a superior security level. This is due to the higher computation involved during parsing of the significant parts of a digital image, followed by encryption.

2.2 Edge detection approaches

Edge maps play a significant role in the image-processing domain. They are used for image enhancement, segmentation, and recognition. Edge detection is a basic process of image segmentation; it recognises the boundaries or contour features in locations where significant changes occur, such as changes in intensity, colour, or texture. Several studies have been devoted to exploiting the edge detection features in the selective encryption domain.

Most existing selective encryption schemes are based on the edge detection approach, such as those proposed by Zhou *et al.* (2009), Shekhar *et al.* (2012), Khashan and Zin (2013), and Zhang *et al.* (2013b). These approaches similarly split an image into non-overlapping pixel blocks. The detection output is a binary image with only two values (1 or 0) for each pixel, with 1 reflecting a significant pixel and 0 the opposite. Consequently, the blocks that contain edges greater than a specified threshold are identified for subsequent encryption using different encryption ciphers, for both the spatial and transmission domains. Although the level of security in each scheme is based on the encryption cipher used to encrypt the indicated significant parts on an image, it generally provides an acceptable perceptual security level. However, very few of the presented schemes have proved the performance efficiency of the combination of edge detection and encryption operations, or compared it with a full encryption approach.

A variety of edge detectors are available, each employing different techniques for detecting edges in digital images. After studying different edge detection methods, it was found that the Prewitt edge detector (Prewitt, 1970) has the simplest implementation and requires the least computational cost. The inherent property of the Prewitt edge detector is an averaging of neighbouring pixels. A 3×3 filter mask is used in the Prewitt edge detector. The edge detection provides good smoothing as well as an ability to reduce image noise (Maini and Sohal, 2006). Thus, the Prewitt edge detector is an accurate method of estimating the magnitude and orientation of edges in images.

2.3 Face detection approaches

Human faces possess more important semantic information than other parts of images. The face detection approach is based on identifying the location of human faces on digital images, regardless of size or position. Several face detection methods are currently available. Some of these methods use simple cues to predict human faces, such as colour, flesh tones, or contours, whereas other methods use more complex techniques, such as templates, filters, or neural networks (Tolba *et al.*, 2006). However, the methods are all based on analysing the image pixels to carry out face detection. Therefore, the required normalized operations against the pixel values, such as scaling, rotating, and moving, make these methods suffer from high processing overheads. Viola and Jones (2001) have proposed a highly accurate and more computationally efficient technique for object recognition. It is called Haar classifier object detection, and is based on Haar-like features. This technique rapidly detects objects, including human faces, but is not based on pixels.

The implementations of the Haar classifier, such as OpenCV (OpenCV, 2013), provide different object classifiers using different datasets. A sub-window containing a scaled size from the original image scans the entire image in order to obtain the candidate object, i.e., a human face. It uses a cascade of stages. In each stage, the algorithm looks for all Haar-like features and encodes the contrasts exhibited by the target object and its special relationships, and then classifies the object using the Haar feature classifier. When one of these features is found, the next stage of detection is processed, until all detection stages have run and the target object, i.e., a human face, is detected. Since the Haar detection framework has the best performance in both accuracy and speed, it is widely used by other studies on face detection, and has been chosen for this work to detect faces followed by encryption.

3 Cryptographic operations

In this study, we use methods similar to those employed in previous selective image encryption schemes based on edge and face detection approaches followed by encryption. The cryptographic operations of full images, as well as selective image encryption, are based on using symmetric encryption ciphers. This takes a fixed length plaintext block of pixels or bits and then transforms it after a set of complicated operations into a ciphered block of the same length. The Blowfish algorithm is selected as a symmetric encryption cipher in the output feedback (OFB) mode with a 128-bit key. Blowfish has good performance and is considered one of the fastest symmetric encryption algorithms (Verma *et al.*, 2011). In the OFB mode a block cipher is transformed into a synchronous stream cipher. It has good performance and high security levels, and maintains the ability to hide all features of an image (El-Fishawy and Abu Zaid, 2007).

Typically, the encryption process is more complicated and has a higher computational overhead than the decryption process. This is because the visual inspection methods used during the encryption process, i.e., edge and face detection methods, consume more processing time to identify the significant parts of an image. These operations are not required in the decryption process, but restricted to extracting the location of the encrypted regions followed by decryption.

3.1 Edge based image encryption

Fig. 1 illustrates the steps carried out on an original image to identify the significant blocks, followed by encryption of these detected blocks.

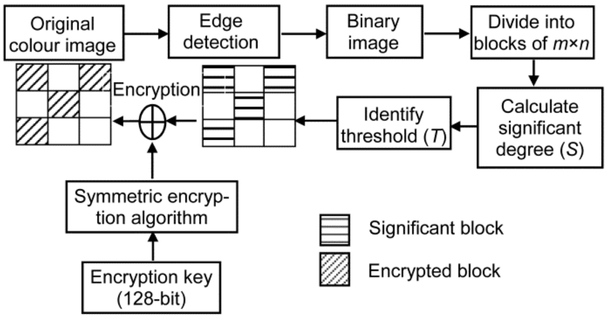

Fig. 1 Block diagram for edge based image encryption

Consider that G represents the original colour image of size M×N.

1. The original image (G) is detected using the Prewitt edge detector. This yields a binary image that has the same size as the original image, but with only two values, 1 or 0, for each pixel. A value of 1 indicates an edge at the same location of a corresponding pixel in the original image, whereas 0 indicates no edge. Figs. 2a and 2b show the original Lena image and the output of the Prewitt edge detector, respectively.

2. The detected images and the original images are similarly divided into non-overlapping blocks of pixels. Each block has a size of m×n, and $P=M\times N/(m\times n)$ is the total number of blocks in the image.

3. A calculation is made of the significant degree (S) for each detected block (B) by counting the total number of detected pixels (Q) in each detected block $B_{i,j}$ using $S_{i,j}=Q_{i,j}/P$, where $B_{i,j}$ is the exact coordinate of the block location on the image.

4. The threshold level T is detected, $0\leq T\leq 1$. Thus, for each block, $S_{i,j}\geq T$ indicates it is significant,

and $S_{i,j}<T$ indicates it is insignificant. Here, a binary index key array (I_{key}) is used to indicate the index of the significant and insignificant blocks in an image into an array sized $1\times P$. The element '1' reflects that the corresponding block is significant, whereas '0' means the opposite.

5. Next, significant blocks are encrypted based on the I_{key} in sequence using the Blowfish encryption algorithm. The encryption key and the initialization vector are of 128-bit length, and both are generated randomly. On the other hand, the insignificant blocks are left as are without encryption.

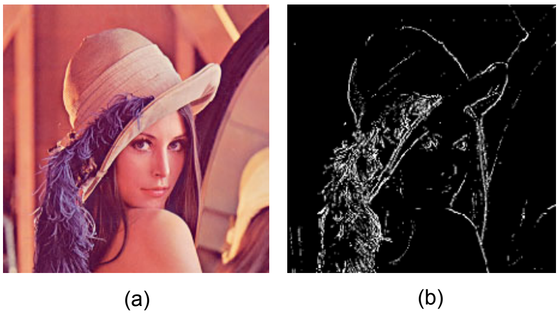

Fig. 2 Edge detected output using the Prewitt detector
(a) Original Lena image; (b) Edge detected Lena

3.2 Face based image encryption

Several previous studies have used the pixel-based approach to detect the human face region in digital images. As pixels require frequent reanalysis for scaling and precision, more processing time is needed. Therefore, to derive more exact face detection in significantly less computation time, the OpenCV Haar cascade classifier is used. For detecting and encrypting image faces, the following steps are performed:

1. The original input colour image (G) of size $M\times N$ is first determined and then loaded to the cvHaarDetectObject.

2. A sub-window classifier (SB) is then defined with a suitable size $m\times n$ based on the minimum face size in the image (G).

3. Next, the classifier SB window is used to search across the entire image (G) by checking every location to find human faces of different sizes. Here, the scan procedure is repeated many times to find the larger faces by increasing the size of SB until all faces in the image are detected or rejected otherwise.

4. When a face object is found by the classifier SB, the coordinates of that detected face position as a rectangle of pixels will be retrieved and stored in a list (l).

5. Finally, all the defined faces regions in the list (l) will be encrypted into another ciphered bit string that has the same region length. The encryption is performed using the Blowfish cipher in OFB mode, with a randomly generated 128-bit key.

In full encryption, all image information is encrypted by considering the entire image as a single block of pixels. Each pixel is extracted in sequence and converted into a byte stream. All the internal operations of the Blowfish algorithm are carried out to transform the plain image data into other cipher text in a bit string of the same length. On the other hand, decryption is the reverse process using the same secret key, which results in similar processing time and resource consumption.

4 Experimental results

Several experiments were performed to measure the execution time for selective image encryption, which combines encryption operation with face or edge detection methods, as well as the performance of full image encryption. All experiments were conducted in the same environment, with a 32-bit operating system, Intel Core 2 Duo 2.1 GHz CPU, and 4 GB main memory. Also, several typical colour bitmap images of various sizes were used.

First, full encryption was carried out for various test images of different sizes using Blowfish-OFB. Table 1 shows the computational encryption time for various test images.

The performance of the edge based image encryption was assessed and compared by the computational time involved through the different processes during the selective encryption operation. Fig. 3 shows the edge based encryption output of Lena and Airplane test images of size 512×512 using a block size of B=8×8 and a threshold value of T=0.05.

Typically, decreasing the T value effectively increases the number of detected blocks for encryption. When T is approaching 1, the number of detected blocks is close to zero. Fig. 4 shows the correlation between different T values and the percentage of significant pixels of all detected blocks, for subsequent encryptions of the Lena image of size 512×512 using B=8×8 as a default size. When T=0.01, the percentage of encrypted blocks is 48%, whereas when T=0.25, only 5% of blocks on the image are encrypted.

Table 1 The computational time of full encryption for different test images

Image	Size	Full encryption time (ms)
Lena	256×256	272.5
Airplane	512×512	1099.8
Baboon	512×512	1113.4
Barbara	512×412	911.3
Couple	256×256	273.5
Jelly Beans	256×256	273.4
Peppers	512×512	1092.6
Tiffany	512×512	1100.7
Group	400×300	503.3
Child	256×197	211.4
Friends	259×194	210.3
Model in black dress	512×768	1676.6

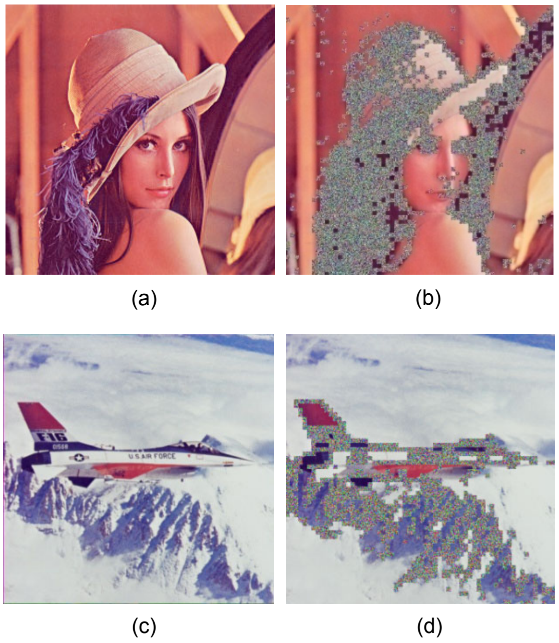

Fig. 3 Selective encryption based on edge detection output

(a) and (c) are the original Lena and Airplane images of size 512×512, respectively; (b) and (d) are the edges based encrypted images, respectively (B=8×8 and T=0.05)

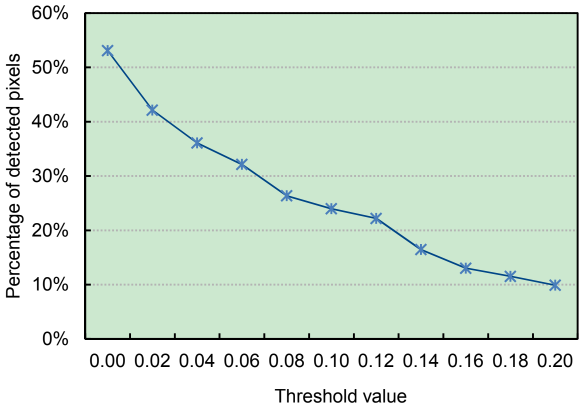

Fig. 4 The correlation between the changing T value and the percentage of the detected pixels for encrypting the Lena image of size 512×512 with a default B of 8×8

The different processes carried out during edge image encryption were analysed, and the computational time involved in each process was calculated. The Lena image of size 512×512 and B=8×8 was used using various T values. Fig. 5 shows the plot of elapsed time for the processes executed during edge image encryption, namely the detection, extraction, and encryption processes.

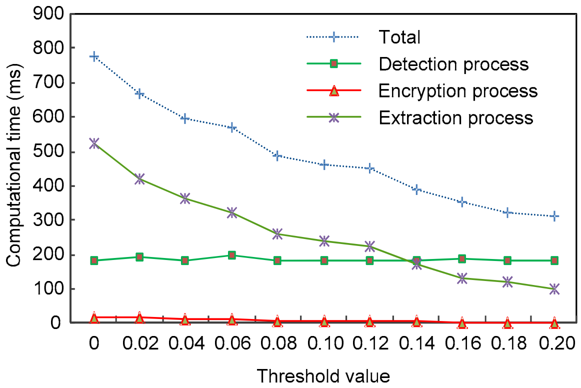

Fig. 5 Comparison of computational time for different execution processes during edge-based selective encryption for Lena of size 512×512 using various T values

Detection time is the time required to detect the edges of an image. Extraction time is the time needed to extract a 2D array of pixels and convert it into a 1D array byte stream. Encryption time is the time required to transform plain blocks into other cipher text blocks of bit string. There are more processes involved that also take time, such as the movement process in which blocks and pixels in the nested loops operations are moved, in addition to the time required for I/O disk operations. Total processing time is the total time taken for all processes to obtain the image encrypted.

The evaluation results show that the encryption process requires the minimum elapsed time, which is decreased gradually with an increased T value. It takes a little less than 3% of the total processing time when T is close to zero. The extraction process requires the maximum computational time. The time needed decreases linearly as T increases, due to the decreased number of detected pixels needed for encryption.

On the other hand, the elapsed time for detecting edges on an image is almost the same for all T values. The elapsed time of other processes, such as the movement process and I/O disk operations, is a little more than 6% of the total time for all T values.

A comparison of edge-based image encryption was performed on various colour images of various sizes to determine the percentage of the detection process and the encryption process time among the total time. Table 2 shows the results obtained from different test images using B=8×8 and T=0.1 as default values.

The performance of face-based encryption was analysed to evaluate the computational time involved in the different processes during selective encryption. Fig. 6 shows the original Lena and Group test images and the encrypted counterparts.

A Lena image of size 256×256 was used; the face was detected and encrypted using various sub-window sizes. Fig. 7 shows the elapsed time for different processes executed during the operation. The encryption process has a minimum elapsed time not exceeding 2% for all sub-window sizes.

Table 2 Results of selective encryption based on edge detection for different test images (T=0.1, B=8×8)

Image	Size	Percentage of detected pixels (%)	Total time* (ms)	Detection time (ms)	Percentage of detection time (%)	Encryption time (ms)	Percentage of encryption time (%)
Lena	512×512	23.97	467.57	183.93	39.34	8.86	1.89
Airplane	512×512	28.02	516.01	190.62	36.94	10.21	1.98
Baboon	512×512	80.29	1085.42	196.39	18.09	29.03	2.67
Barbara	512×412	54.64	652.02	158.52	24.31	16.21	2.49
Couple	256×256	27.83	129.48	48.69	37.60	2.62	2.02
House	256×256	37.40	153.61	46.80	30.47	3.48	2.27
Jelly Beans	256×256	22.46	110.81	46.71	42.15	2.05	1.85
Peppers	512×512	23.63	464.34	189.50	40.81	8.62	1.86
Tiffany	512×512	26.54	495.97	188.76	38.06	9.74	1.96

* Total time includes the times taken by all execution processes to obtain the image encrypted, such as detection, encryption, movement, and I/O

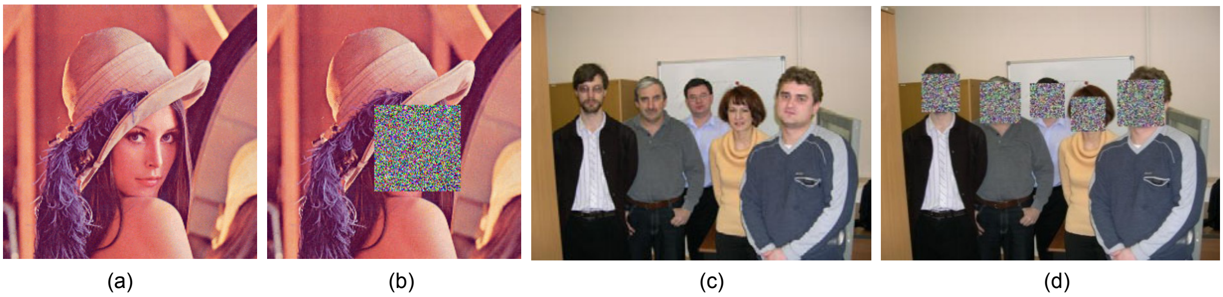

Fig. 6 Selective encryption based on face detection for Lena and Group test images
(a) Original Lena image; (b) Face encrypted Lena; (c) Original Group image; (d) Face encrypted Group

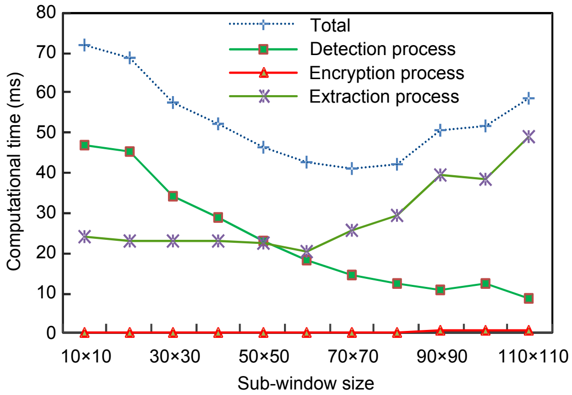

Fig. 7 Comparison of computational time for different execution processes during face based selective encryption for the Lena image of size 256×256 using various sub-window sizes

A drastic decrease in the computational time for the detection process was observed with the increase of the sub-window size; in contrast, the computational time for the extraction process increased. This is due to the increasing number of pixels on the sub-window which scans a larger area from the image, and hence decreases the number of scan times, whereas the number of pixels converted into a byte stream increases during the extraction process.

To ascertain the efficiency of face based encryption, a computational time analysis was performed on different test images using a 40×40 sub-window. Table 3 lists the results obtained for the face detection and encryption processes in addition to the total time for different test images.

A comparison of computational time was performed on the Lena test image of various sizes by implementing complete and selective image encryption using different encryption methods. Full image encryption was performed using the entire image as a single block of pixels. The encryption was implemented after converting the block of pixels into a stream of bytes. Selective image encryption is performed by implementing a random selection of image blocks for encryption according to a certain percentage, in addition to the implementation of edge and face based image encryption methods. Fig. 8 shows the computational elapsed time for the different encryption methods.

The evaluation results show a significant difference in the computational time observed between full image encryption and other selective encryption methods. The analysis indicates that selective encryption methods, which use a combination of encryption and visual inspection techniques, still encrypt a smaller number of pixels compared to the encryption using a random selection of specified percentage values based on a convergent value of computational time. However, former methods still offer a higher security level because the entire data of

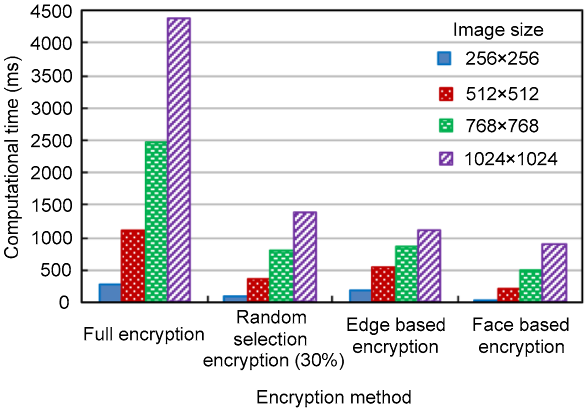

Fig. 8 Comparison of the computational time for encrypting the Lena image of various sizes using different encryption methods (*T*=0.05, *B*=8×8, 40×40 sub-window)

Table 3 Results of selective encryption based on face detection for different test images with a 40×40 sub-window

Image	Size	Percentage of detected pixels (%)	Total time (ms)	Detection time (ms)	Percentage of detection time (%)	Encryption time (ms)	Percentage of encryption time (%)
Lena	256×256	11.55	49.10	28.68	58.41	0.330	0.672
Group	400×300	8.93	74.03	40.11	54.18	0.522	0.705
Tiffany	512×512	29.69	348.85	116.49	33.39	3.126	0.896
Girl	256×256	9.28	45.89	26.90	58.62	0.276	0.601
Child	256×197	23.13	59.05	22.56	38.20	0.528	0.894
Friends	259×194	30.17	70.45	24.04	34.12	0.700	0.994
Model in black dress	512×768	1.24	205.16	189.49	92.36	0.235	0.115

the image does not have equal importance; these methods can restrict encryption to image data that has a relatively high importance level.

5 Conclusions

This paper provides an extensive analysis of selective image encryption based on edge and face detection methods using the Blowfish symmetric cipher. Most studies in this domain use pixels based permutation with chaos-based techniques and other random permutation methods. However, while such encryption schemes are efficient, the security levels are unlikely to compete with those provided by standard ciphers, which are less affected by attacks.

Thus, selective encryption of visual images based on symmetric ciphers is a more acceptable trade-off between security and performance. Experimental tests demonstrate the computational time taken by the different processes executed during image encryption using a symmetric cipher. The results obtained reflect a significant reduction of computational time for selective encryption methods on still visual images compared to full encryption. Such selective encryption based on these methods is suitable for applications requiring short computation time and satisfactory security levels.

References

Amigó, J.M., Kocarev, L., Szczepanski, J., 2007. Theory and practice of chaotic cryptography. *Phys. Lett. A*, **366**(3): 211-216. [doi:10.1016/j.physleta.2007.02.021]

Bhatnagar, G., Wu, Q.M., 2012. Selective image encryption based on pixels of interest and singular value decomposition. *Dig. Signal Process.*, **22**:648-663. [doi:10.1016/j.dsp.2012.02.005]

Chen, T.S., Chang, C.C., Hwang, M.S., 1998. A virtual image cryptosystem based upon vector quantization. *IEEE Trans. Image Process.*, **7**(10):1485-1488. [doi:10.1109/83.718488]

Cheng, H., Li, X., 2000. Partial encryption of compressed images and videos. *IEEE Trans. Signal Process.*, **48**(8): 2439-2451. [doi:10.1109/78.852023]

Droogenbroeck, M.V., Benedett, R., 2002. Techniques for a selective encryption of uncompressed and compressed images. Proc. Advanced Concepts for Intelligent Vision Systems, p.90-97.

El-Fishawy, N., Abu Zaid, O.M., 2007. Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms. *Int. J. Network Secur.*, **5**(3):241-251.

Flayh, N.A., Parveen, R., Ahson, S.I., 2009. Wavelet based partial image encryption. Proc. Int. Multimedia, Signal Processing and Communication Technologies, p.32-35. [doi:10.1109/MSPCT.2009.5164167]

Khashan, O.A., Zin, A.M., 2013. An efficient adaptive of transparent spatial digital image encryption. Proc. 4th Int. Conf. on Electrical Engineering and Informatics, p.288-297. [doi:10.1016/j.protcy.2013.12.193]

Krikor, L., Baba, S., Arif, T., *et al.*, 2009. Image encryption using DCT and stream cipher. *Eur. J. Sci. Res.*, **32**(1): 48-58.

Kulkarni , N.S., Raman, B., Gupta, I., 2009. Multimedia encryption: a brief overview. Recent Advances in Multimedia Signal Processing and Communications Studies in Computational Intelligence. *In*: Grgic, M., Delac, K., Ghanbari, M. (Eds.), Studies in Computational Intelligence, Springer Heidelberg, **231**:417-449.

Li, C., Lo, K., 2011. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Process.*, **91**(4):949-954. [doi:10.1016/j.sigpro.2010.09.014]

Li, S., Li, C., Chen, G., *et al.*, 2008. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. *Signal Process. Image Commun.*, **23**(3):212-223. [doi:10.1016/j.image.2008.01.003]

Lian, S., Chen, X., 2013. On the design of partial encryption scheme for multimedia content. *Math. Comput. Model.*, **57**(11-12):2613-2624. [doi:10.1016/j.mcm.2011.06.007]

Liu, H.J., Wang, X.Y., 2010. Color image encryption based on one-time keys and robust chaotic maps. *Comput. Math. Appl.*, **59**(10):3320-3327. [doi:10.1016/j.camwa.2010.03.017]

Maini, R., Sohal, J.S., 2006. Performance evaluation of Prewitt edge detector for noisy images. *Int. J. Graph. Vis. Image Process.*, **6**(3):39-46.

Martin, K., Lukac, R., Plataniotis, K., 2005. Efficient encryption of wavelet-based coded color images. *Pattern Recogn.*, **38**(7):1111-1115. [doi:10.1016/j.patcog.2005.01.002]

Norcen, R., Podesser, M., Pommer, A., *et al.*, 2003. Confidential storage and transmission of medical image data. *Comput. Biol. Med.*, **33**(3):277-292. [doi:10.1016/S0010-4825(02)00094-X]

OpenCV, 2013. Open Source Computer Vision Library. Available from http://opencv.org/.

Podesser, M., Schmidt, H.P., Uhl, A., 2002. Selective bitplane encryption for secure transmission of image data in mobile environments. Proc. 5th Nordic Signal Processing Symp., p.1034-1037.

Prewitt, J.M.S., 1970. Object Enhancement and Extraction: Picture Processing and Psychopictorics. Academic Press Inc., USA, p.75-150.

Puech, W., Bors, A.G., Rodrigues, J.M., 2013. Protection of colour images by selective encryption. *Adv. Color Image Process. Anal.*, p.397-421. [doi:10.1007/978-1-4419-

6190-7_12]

Shekhar, S., Srivastava, H., Dutta, M.K., 2012. An efficient adaptive encryption algorithm for digital images. *Int. J. Comput. Electr. Eng.*, **4**(3):380-383. [doi:10.7763/IJCEE.2012.V4.516]

Stutz, T., Uhl, A., 2006. Transparent image encryption using progressive JPEG. *LNCS*, **4176**:286-298. [doi:10.1007/11836810_21]

Subba Rao, Y.V., Mitra, A., Mahadeva Prasanna, S.R., 2006. A partial image encryption method with pseudo random sequences. *LNCS*, **4332**:315-325. [doi:10.1007/11961635_22]

Tolba, A.S., El-Baz, A.H., El-Harby, A.A., 2006. Face recognition: a literature review. *Int. J. Signal Process.*, **2**(2):88-103.

Verma, O.P., Agarwal, R., Dafouti, D., *et al.*, 2011. Performance analysis of data encryption algorithms. 3rd IEEE Int. Conf. on Electronics Computer Technology, p.399-403. [doi:10.1109/ICETECH.2011.5942029]

Viola, P., Jones, M., 2001. Rapid object detection using a boosted cascade of simple features. IEEE Computer Society Conf. on Computer Vision and Pattern Recognition, p.511-518. [doi:10.1109/CVPR.2001.990517]

Zhang, D., Zhang, F., 2013. Chaotic encryption and decryption of JPEG image. *Optik-Int. J. Light Electron Opt.*, **125**(2):717-720. [doi:10.1016/j.ijleo.2013.07.069]

Zhang, X., Wang, X., 2013. Chaos-based partial encryption of SPIHT coded color images. *Signal Process.*, **93**(9):2422-2431. [doi:10.1016/j.sigpro.2013.03.017]

Zhang, Y., Xiao, D., Wen, W., *et al.*, 2013a. Vulnerability to chosen-plaintext attack of a general optical encryption model with the architecture of scrambling-then-double random phase encoding. *Opt. Lett.*, **38**(21):4506-4509. [doi:10.1364/OL.38.004506]

Zhang, Y., Xiao, D., Wen, W., *et al.*, 2013b. Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. *Opt. Laser Technol.*, **54**:1-6. [doi:10.1016/j.optlastec.2013.04.029]

Zhang, Y., Xiao, D., Liu, H., *et al.*, 2013c. GLS coding based security solution to JPEG with the structure of aggregated compression and encryption. *Commun. Nonl. Sci. Numer. Simul.*, **19**(5):1366-1374. [doi:10.1016/j.cnsns.2013.09.019]

Zhao, X.Y., Chen, G., Zhang, D., *et al.*, 2004. Decryption of pure-position permutation algorithms. *J. Zhejiang Univ. Sci.*, **5**(7):803-809. [doi:10.1631/jzus.2004.0803]

Zhou, Y., Panetta, K., Agaian, S., 2009. A lossless encryption method for medical images using edge maps. 31st Annual Int. Conf. on IEEE Engineering in Medicine & Biology Society, p.3707-3710. [doi:10.1109/IEMBS.2009.5334799]