Selective image encryption for Medical and Satellite Images

Panduranga H T [#1], NaveenKumar S K [*2]
[# *]Dept. of Studies in Electronics, University of Mysore
Hemagangothri PG Center, Hassan, Hassan, Karnataka, India
[1] ht_pandu@yahoo.co.in
[2]nave12@gmail.com

***Abstract*— Information security plays a very important role in fast growing information and communication technology. Few applications like medical image security and satellite image security needs to secure only selected portion of the image. This paper describes a concept of selective image encryption in two ways. First method divides the image in to sub blocks, then selected blocks are applied to encryption process. Second method automatically detects the positions of objects, and then selected objects are applied to encryption process. Morphological techniques are used to detect the positions of the objects in given images. These two approaches are specifically developed to encrypt the portion of an image in medical images and satellite image.**

Keyword- Region of Interest, partial image encryption, visible encryption

I. INTRODUCTION

With fast growing information and communication technology there is a huge demand for information security. Image is two dimensional data which carries more information. Encryption is one way to scramble the information, so that unauthorized person cannot understand that information. A major recent trend is to minimize the computational requirements for secure multimedia distribution by "*selective encryption*" where only parts of the data are encrypted. This paper describes an image encryption technique specifically for satellite and medical images. Selective encryption is a recent approach to reduce the computational requirements for huge volumes of multimedia data in distribution network with different client device capabilities.

In selective encryption some content of the image is encrypted. It reduces the execution time because it encrypts only a part of the image. Consequently, selective encryption is sometimes called partial encryption. This algorithm provides security to the image and in the same time, some part of the image is visible. One of the use of this algorithm is in medical field, now a days the doctors are consulting the other doctors abroad, this algorithm can really help those. The medical image data is different from other visual data for multimedia applications. Since the lossy data cause some negative misdiagnosis.

Nidhi et.al [1], proposed a selective encryption technique in wavelet domain for conditional access systems. This encryption is applied only to a subset of multimedia data stream rather than the multimedia data in its entirety to save the computational time and computational resources. thus controlling the transparency of the multimedia data at the time of encryption. Gaurav Bhatnagar [2], presented a simple selective encryption technique based on Saw-Tooth space filling curve, pixels of interest, non-linear chaotic map and singular value decomposition. The core idea of this algorithm is to scramble the pixel positions by the means of Saw-Tooth space filling curve followed by the selection of significant pixels using pixels of interest method. Then the diffusion process is done on the significant pixels using a secret image key obtained from non-linear chaotic map and singular value decomposition. Priyanka Agrawal and Manisha Rajpoot [3] explained a concept where important part of the image that can efficiently achieve by conceptually selecting the part of the image which is further used in its normal mode of operation for encryption. Once encryption is done, the encrypted data is sent along with remaining original part of the message, ensuring its secured transmission and distribution over public networks. The main idea behind the present work is to select the part of the image by the arranging the bit stream in grid form and choosing the diagonal of the grid. Zahia Brahimi et.al [4] presented 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 we introduce the permutation of code blocks 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. This method don't introduce superfluous JPEG2000 markers in the protected code stream, i.e, its format is compliant to JPEG2000 code stream one . Tao Xiang et.al [5] most existing selective image encryption schemes are designed based on image compression algorithms, and thus they are codec specific. As different bit planes of an image contribute differently to visualization effect, a selective gray-level image encryption scheme is proposed in this paper. In this scheme, only a portion of significant bits of each pixel is encrypted by the key stream generated from a one-way coupled map lattice that

exhibits good chaotic dynamics even after discretization . Marc Van Droogenbroeck and Raphaël Benedett, [6] presented a selective encryption of compressed image and they used JPEG compression, the Huffman coder aggregates zero coefficients into runs of zeros and uses symbols that combine the run of zeros with magnitude categories for the non-zero coefficients that terminate the runs. These symbols are assigned 8-bit code words by the Huffman coder. The code words precede the appended bits that specify the sign and magnitude of the non-zero coefficients. In the proposed scheme, the appended bits corresponding to a selected number of AC coefficients are encrypted. The DC coefficients are left unencrypted because, it is argued, they carry important visible information and are highly predictable. Roman Pfarrhofer and Andreas Uhl [7] explained the concept of the gray scale image is decomposed into its 8 bit planes and the most significant bit planes are encrypted. After a number of experiments, it is observed that (1) the encryption of the 4 most significant bit plane is not secure enough, (2) selectively encrypting 2 bit planes is sufficient if severe alienation of the image data is acceptable, and (3) encryption of 4 bit planes provides high confidentiality (4) for selective encryption only the lowest resolution of 5 layers may be encrypted . We have proposed an hybrid approach that involves rearranging the mapping image according to SCAN patterns and selecting a pixel value of rearranged mapping image based on the mapping function. The basic idea of this technique lies in converting the pixel value of original image into a row and column values of mapping image[8].

Rest of the paper is as follows. Section two describes the concept of selective encryption. Section three describes the partial and visible encryption. The proposed methods along with results are discussed in section four. Conclusion of the proposed technique is done in section five.

II. SELECTIVE IMAGE ENCRYPTION

As the name indicates that, the encryption is not applied to entire data but it is applied to selected data only. Here encryption process is applied only to selected portion of an image based on the region of interest leading to reduce the time for encryption. Selection of region of interest is done manually or automatically based on the application. This paper describes both manual and automatic selection of the region of interest in an image for encryption. Figure 1(a) shows manual selection of region of interest area and Fig.1 (b) shows the automatic selection of region of interest area.

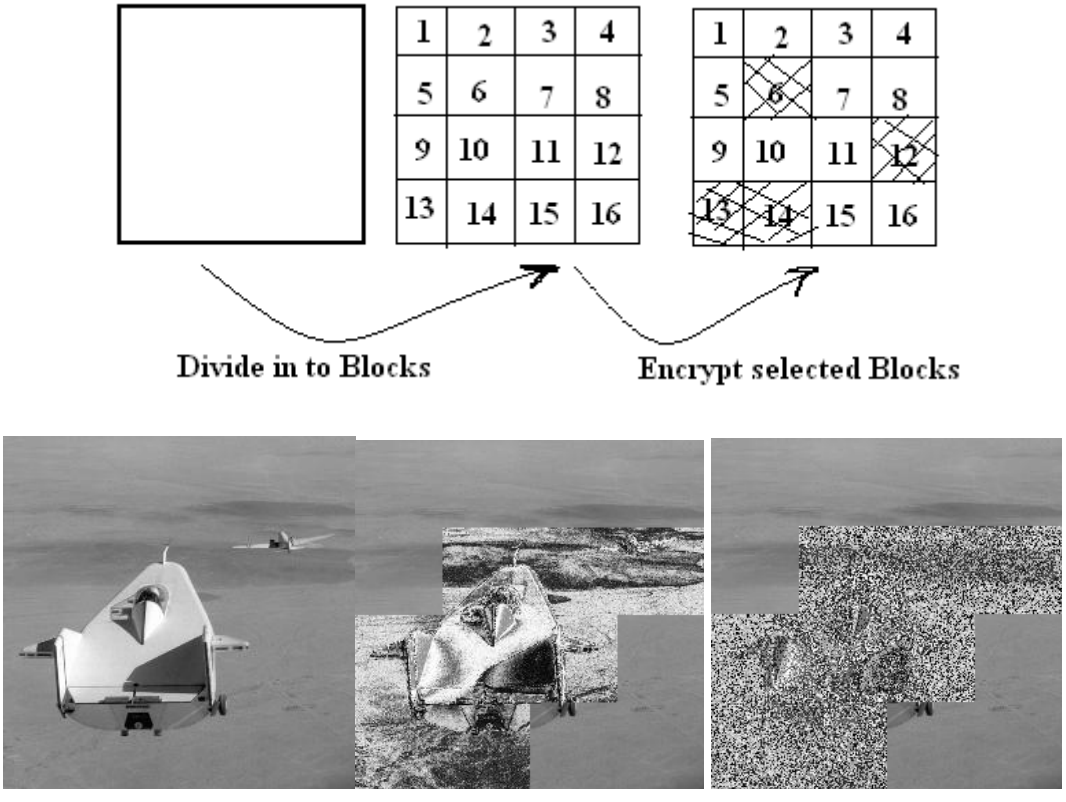


Fig. 1. (a). Manually selection of block to be encrypted.

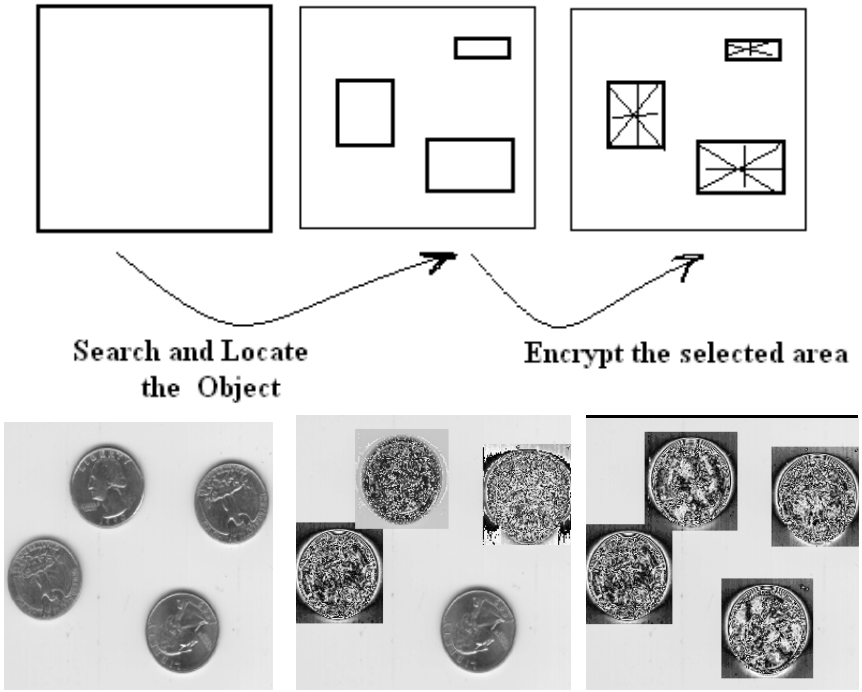
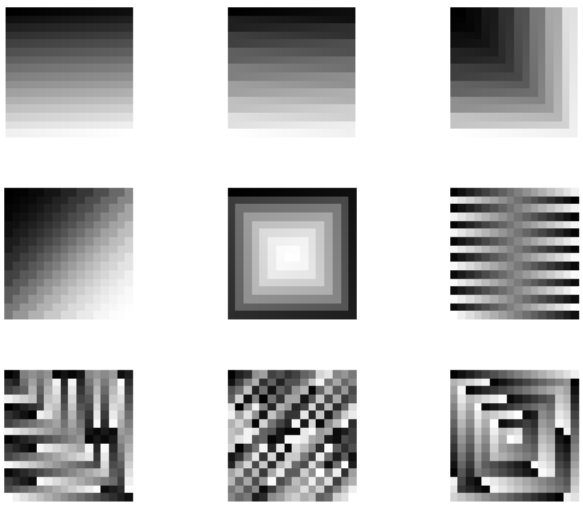


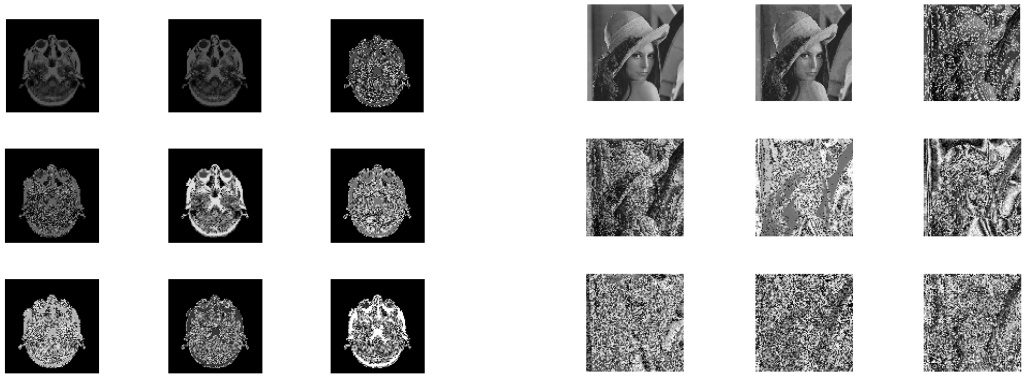
Fig. 1(b). Automatic selection of region of interest area to be encrypted.

III. PARTIAL AND VISIBLE ENCRYPTION

In medical and satellite application small amount of encryption is enough to secure the image instead of complete encryption. This way of encryption leads to partial or visible encryption. In partial or visible encryption observer can predict the original image but, accuracy of original image and predicted image depends on the amount of visibility, encryption and amount of information in an encrypted image. This paper uses a mapping technique for visible encryption. We use the method in reference [8] to perform the partial image encryption. From Fig.2 we can understand the concept of partial and visible encryption.



2(a) Mapping Images



2(b)Encrypted images
Fig.2. Partial and visible encrypted images

IV. PROPOSED SELECTIVE ENCRYPTION METHOD

This paper describes the concept of selective image encryption in two ways. Figure 3 shows the first method for selective image encryption. Here image to be encrypted is first divided in to sub blocks and then fed in to encryption block. Block selection is to be done 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. Figure 4 shows the second method for selective image encryption. Here region of interest is located using morphological operation and selected regions are encrypted using map images.

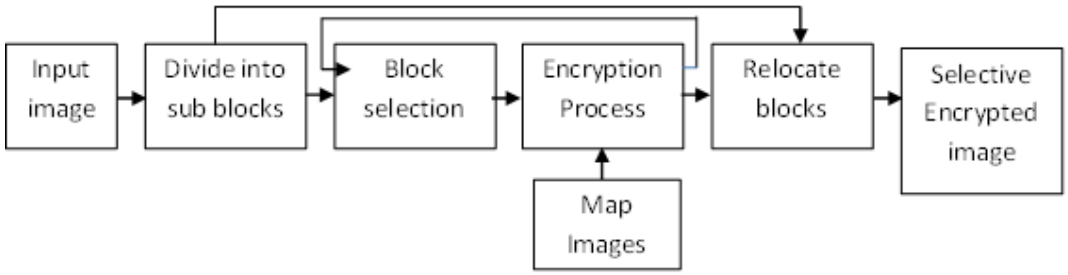


Fig. 3. Block diagram of proposed selective image encryption using sub-blocks.

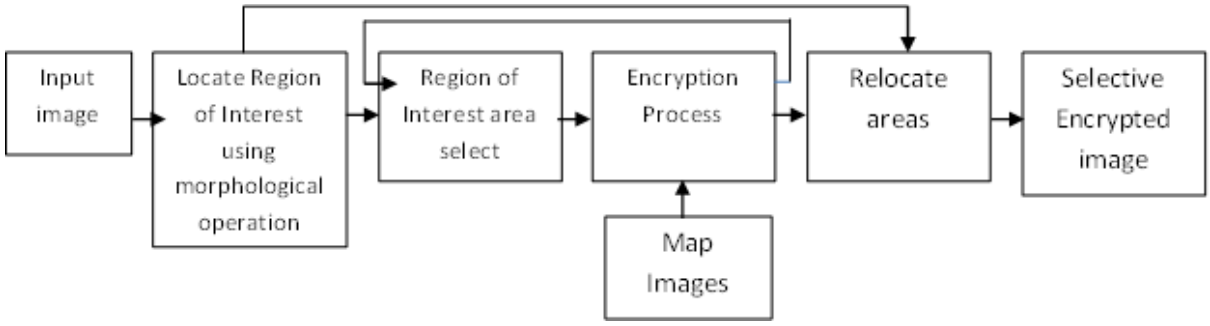


Fig. 4. Block diagram of proposed selective image encryption based on region of interest.

V. RESULTS AND DISCUSSION

Fig. 5 shows input image and resultant encrypted images for different mapping images using proposed selective encryption based on sub-blocks. From these resultant images we can observe that sub-block based selective image encryption is enough to secure the important information in an image.

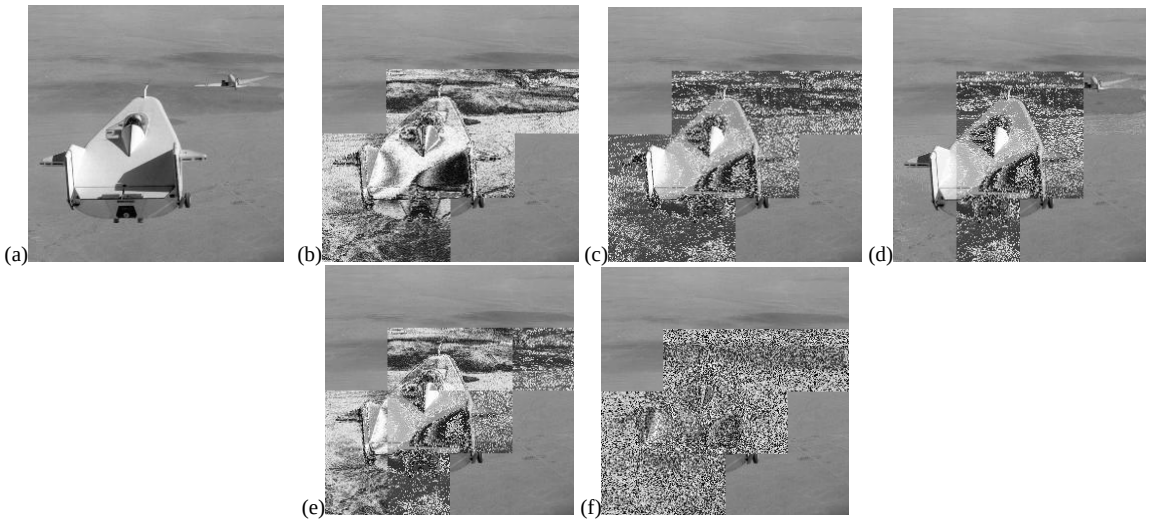


Fig. 5. Resultant encrypted images obtained from proposed method using sub-block with different map-images.

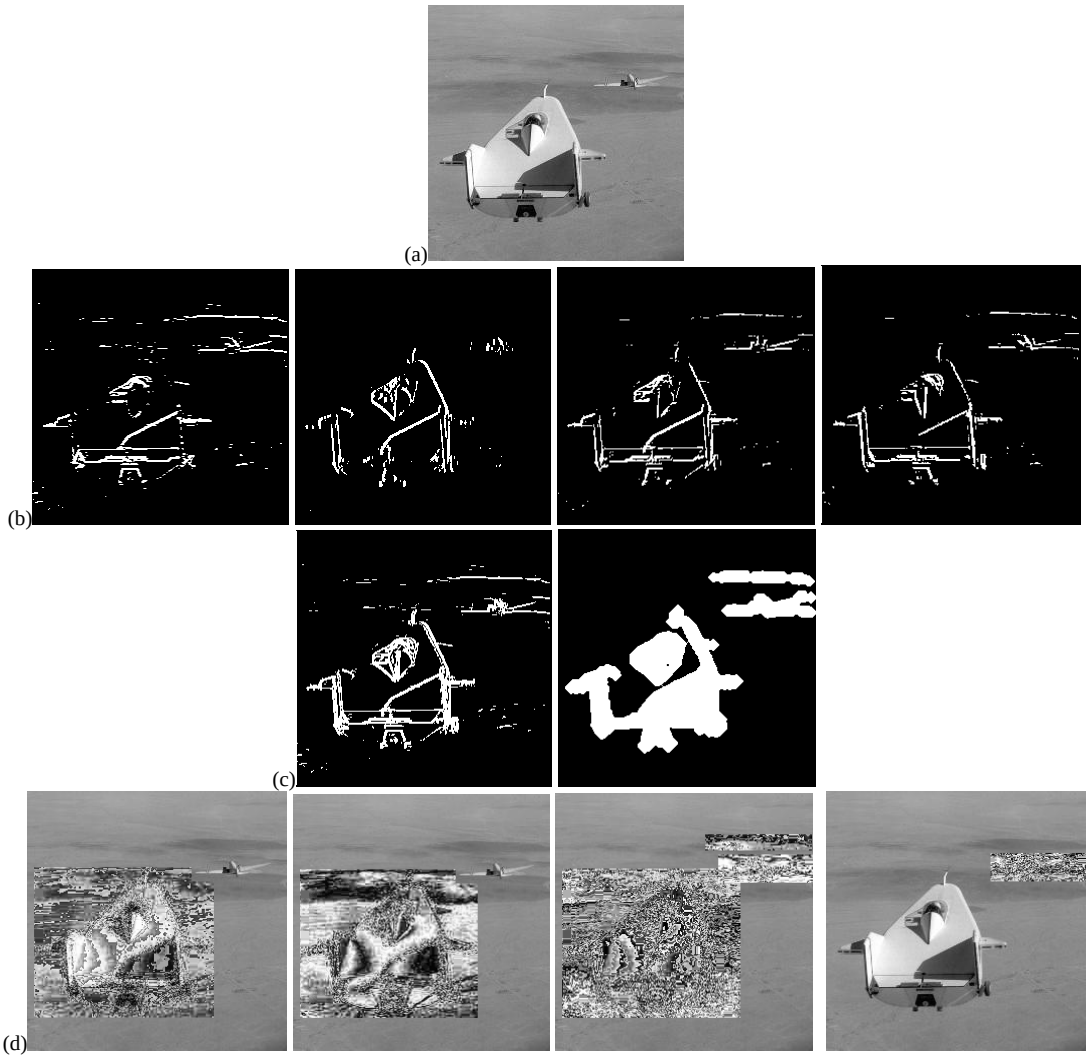


Fig. 6. (a) jet image (b) horizontal, vertical and diagonal edge images of jet (c) combined edge image and locating region of interest areas in jet image (d) selective encrypted images

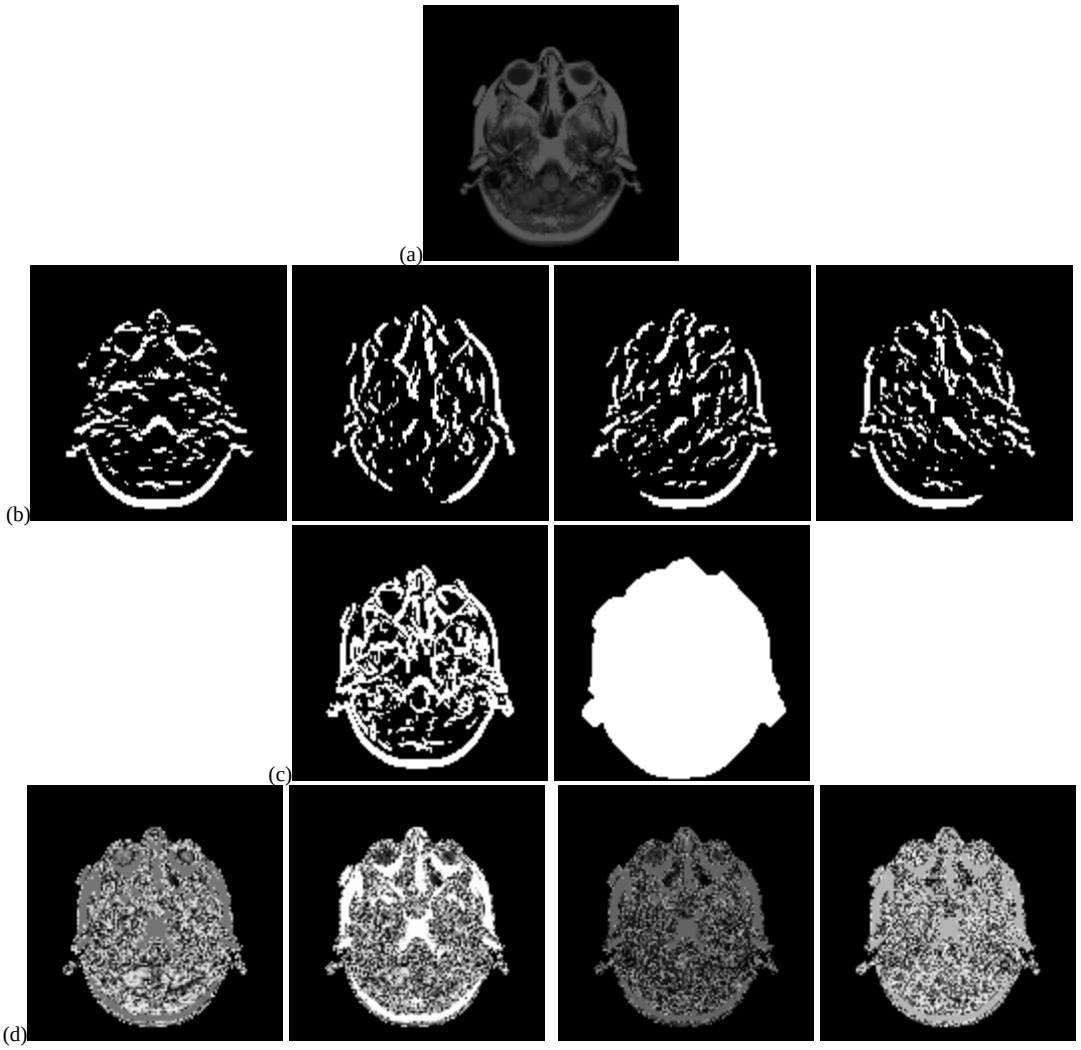


Fig.7. (a) mri image (b) horizontal, vertical and diagonal edge images of mri (c) combined edge image and locating region of interest area in mri image (d) selective encrypted images.

Fig. 6(a,b,c) and 7(a,b,c) shows input image, resultant images of edge detection and morphological operation. Figure 6(d) shows resultant encrypted images based on region of interest for different mapping images. From these results we can observe that by using region of interest based selective image encryption technique we can select and encrypt the intended region and unselect the unwanted region. In figure 6 we observe that three different regions are detected after morphological operation. Out of these three different regions we can select and encrypt one or more regions. In figure 7 we observe that only one region of interest is detected and encrypted.

VI. CONCLUSION

In this paper we presented a selective image encryption approach for medical and satellite images. First approaches for selective encryption are 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. These two approaches are very much suitable for specific applications like medical image encryption and satellite image encryption.

ACKNOWLEDGMENT

The work described in this paper is supported by a grant from the *University Grants Commission*, New Delhi, India.

REFERENCES

[1] Nidhi S Kulkarni, Balasubramanian Raman, and Indra Gupta, “Selective encryption of multimedia images”, NSC 2008, December 17-19, 2008.

[2] Gaurav Bhatnagar , Q.M. Jonathan Wu, Selective image encryption based on pixels of interest and singular value decomposition, Digital Signal Processing 22 (2012) 648–663.

[3] Priyanka Agrawal and Manisha Rajpoot A Fast and Secure Selective Encryption Scheme using Grid Division Method, IJCA vol.51 no.4,pp 29-33, Aug -2012.
[4] Zahia Brahimi, Hamid Bessalah, A. Tarabet, M. K. Kholladi, Selective Encryption Techniques of JPEG2000 Codestream for Medical Images Transmission, WSEAS Transactions on Circuits and Systems Issue 7, Volume 7, July 2008
[5] Tao Xiang, Kwok-wo Wong, and Xiaofeng Liao, Selective image encryption using a spatiotemporal chaotic system, American Institute of Physics 2007.
[6] Marc Van Droogenbroeck and Raphaël Benedett, Techniques for a selective encryption of uncompressed and compressed images, Proceedings of ACIVS 2002 (Advanced Concepts for Intelligent Vision Systems), Ghent, Belgium, September 9-11, 2002
[7] Roman Pfarrhofer and Andreas Uhl, Selective Image Encryption Using JBIG, IFIP International Federation for Information Processing 2005.
[8] Panduranga H T, Naveen kumar S K, Hybrid Approach to Transmit a Secrete Image, 978-1-4244-9581-8/11/ IEEE 2011.