

Research Article

Classification of Novel Selected Region of Interest for Color Image Encryption

^{1,2}Lahieb Mohammed Jawad and ¹Ghazali Sulong

¹UTM-IRDA Digital Media Center (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia

²Department of Network Engineering, College of Information Engineering, Al-Nahrain University, Baghdad, Iraq

Abstract: Securing digital image in exchanging huge multimedia data over internet with limited bandwidth is a significant and sensitive issue. Selective image encryption being an effective method for reducing the amount of encrypted data can achieve adequate security enhancement. Determining and selecting the region of interest in digital color images is challenging for selective image encryption due to their complex structure and distinct regions of varying importance. We propose a new feature in acquiring and selecting Region of Interest (ROI) for the color images to develop a selective encryption scheme. The hybrid domain is used to encrypt regions based on chaotic map approach which automatically generates secret key. This new attribute is a vitality facet representing the noteworthy part of the color image. The security performance of selective image encryption is found to enhance considerably based on the rates of encrypted area selection. Computation is performed using MATLAB R2008a codes on eight images (Lena, Pepper, Splash, Airplane, House, Tiffany, Baboon and Sailboat) each of size 512*512 pixels obtained from standard USC-SIPI Image Database. A block size of 128*128 pixels with threshold levels 0.0017 and 0.48 are employed. Results are analyzed and compared with edge detection method using the same algorithm. Encrypted area, entropy and correlation coefficients performances reveal that the proposed scheme achieves good alternative in the confined region of interest, fulfills the desired confidentiality and protects image privacy.

Keywords: Block cipher, chaotic map, hybrid domain, ROI, selective image encryption, vitality feature

INTRODUCTION

Lately, the exponential escalation in multimedia technology and exhaustive exploitations of internet in transmitting and storing gigantic amount of digital data with limited bandwidth and small storage capacity posed substantial threat towards data security and safety. Images being the widely used multimedia information in assorted fields of applications demand secured transmission (Rehman *et al.*, 2014). Image Encryption (IE) is an established technique that is used to keep image safety. The rationale of developing a precise IE scheme is to modify the original image by encoding it in such a way so that it appears non-understandable for unauthorized users. In short, the idea of encryption is to ensure the utter secrecy via data conversion into a form called a ciphertext. Usually, IE requires vast amount of processing requirements which is ever-demanding for an efficient solution (Ullah *et al.*, 2013). Consequently, efforts are dedicated to remarkably reduce the encrypted digital contents via the Selective Image Encryption (SIE) that only encrypts a part of the image (Puech *et al.*, 2013).

The fundamental concept of SIE is based on analyzing and identifying the significant and insignificant image regions followed by the encryption of significant areas (Hoang and Tran, 2014; Metzler and Agaian, 2010). In fact, occurrence of a tiny error in the significant part causes substantial change in the image. Conversely, slight modifications in the insignificant part does not induce much effect on the image (Bhatnagar and Jonathan Wu, 2012). Moreover, the encrypted parts in SIE scheme must be independent of the unencrypted parts (Suresh and Madhavan, 2012). Figure 1 illustrates the general architecture of SIE system consisting of two main phases such as selected and encrypted ROI.

The successful implementation of selective encryption relies on the sizeable reduction in the amount of encrypted area producing satisfactory security level. Subsequently, different encryption algorithm in spatial and frequency domains are developed (Jawad and Sulong, 2013). Nevertheless, ROI based algorithm are limited in determining the correct region of interest because each image use different criteria for determining ROI (Dutta and Chaudhuri, 2009). Therefore, feature extraction that decides the ROI

Corresponding Author: Lahieb Mohammed Jawad, UTM-IRDA Digital Media Center (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia

This work is licensed under a Creative Commons Attribution 4.0 International License (URL: <http://creativecommons.org/licenses/by/4.0/>).

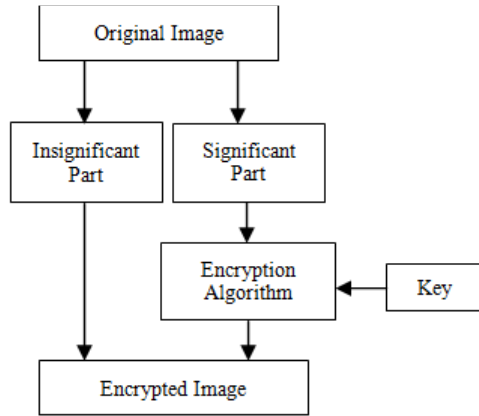


Fig. 1: The architecture of SEI scheme

requires further improvement. Furthermore, most of the SIE techniques based on the encrypted area as significant region fail to satisfy the requirements for high security level (Steffi and Sharma, 2011; Puech *et al.*, 2013).

Meanwhile, chaotic map based methods have emerged as excellent candidate because they incorporate superior features in terms of speed and computing power thereby possess obvious advantages over traditional cipher (Zhang *et al.*, 2013a). Besides, the performance of chaos-based encryption have some shortcoming when implemented to practical situations (Hong and Tram, 2014; Abd El-Latif *et al.*, 2014). Therefore, the combinational domain is regarded as best approach to be implemented in SIE for improving the security level of IE algorithm. Secret key in encryption algorithm play a vital role towards security level enhancement. Strong encryption algorithm with weak secret key achieves low security level for IE. Therefore, generation of strong secret key with good distribution are prerequisite for high quality encrypted image (Wang and Wang, 2013; Apoorva and Kumar, 2013; Yue, 2012; Benlcouiri *et al.*, 2014).

Our interest is to select and determine the ROI for color image encryption via new texture features that identify the correct ROI. Based on multi-threshold value selection, the new classification of ROI is developed. The hybrid domain is used to encrypt regions. Secret keys are automatically generated based on combination of chaotic map methods.

Shortcomings of existing approaches: Undoubtedly, data storage security and transformation is a very sensitive issue because of limited processing power, low bandwidth and small data storage space. Consequently, there is a tradeoff between the amount of encrypted data and computational resources. Indeed, selective encryption being used in various applications can reduce the overhead involved in data transmission over secured channels (Ravishankar and Venkateshmurthy, 2006). Therefore, it is customary to emphasize the past researches on the ROI selection for SIE. The traditional techniques based on the manual selection of ROI (Panduranga and Naveenkumar, 2013; Kumar and Pateriya, 2012) are not good in terms of safety. Conversely, automatic ROI detection is considered to be famous for applying in different SEI algorithms (Ullah *et al.*, 2013). Previously, three main approaches are widely applied to improve the automatic determination of ROI due to its image sensitiveness. Figure 2 illustrates all the existing approaches for ROI selection used in SIE.

The edge detection (Ullah *et al.*, 2013; Taneja *et al.*, 2011; Shekhar *et al.*, 2012; Khashan *et al.*, 2014; Zhang *et al.*, 2013b; Evans and Liu, 2006) approach tries to locate the sharp intensity transitions in an image by identifying the positions where either magnitude of the first derivative of intensity is greater than a specified threshold or the second derivative of intensity has a zero crossing. Prewitt edge detector inherently performs averaging of neighboring pixel values, provides good smoothing operation and reduces the image noise. The choice of 3*3 filter mask in Prewitt edge detection of images is preferable because it can estimate the

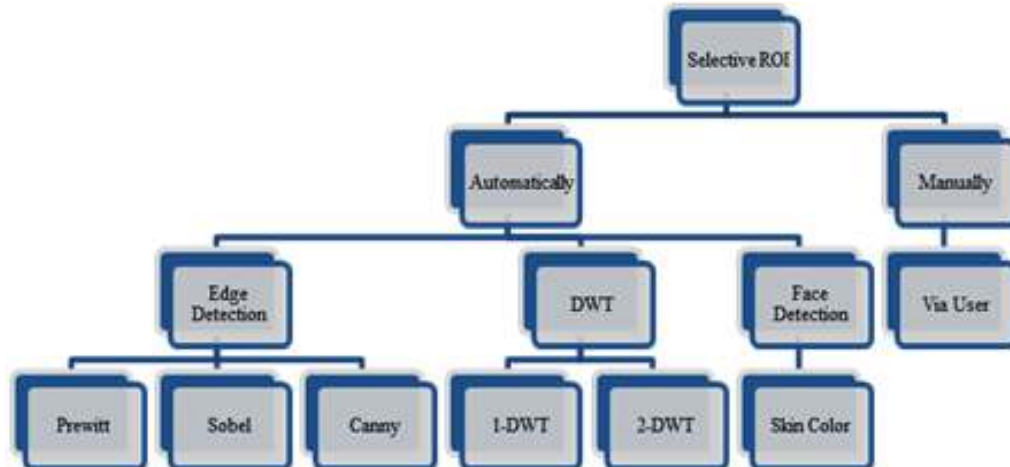


Fig. 2: Main approaches of ROI selection for SIE

magnitude and orientation of an edge accurately (Taneja *et al.*, 2011; Rad *et al.*, 2013). This technique determines region based on number of edges in each block while seldom the high number of edge in block encloses the sensitive area (ROI).

Alternatively, in frequency domain approach the wavelet transformation (Spinsante and Gambi, 2009; Pande and Zambreno, 2012; Pan *et al.*, 2010; Abd El-Latif *et al.*, 2012) is used to determine the sensitive part of an image. Generally, Discrete Wavelet Transforms (DWT) being mathematical tool can examine an image in frequency domains. In this method, the image is decomposed into 4 parts with directional frequencies such as Low horizontal and Low vertical (LL1), Low Horizontal and high vertical (LH1), high Horizontal and Low vertical (HL1) and high Horizontal and High vertical (HH1). These 4 parts correspond to 4 wavelet coefficient matrices. The Lower frequency bands (LL1)

possesses the most energy (information). Therefore, one can utilize this information by dividing an image into a low and a high frequency part using appropriate low-and high-pass filters. Once the frequency separation is completed, the low and high frequency parts concentrate the energy. Most of the energy located in the LL-sub band contains a small-scale version of the original image. The other three sub bands contain the detailed information related to vertical, horizontal and diagonal edges. The high-frequency part without owning any energy can be discarded or coded at a lower bit rate (Rad *et al.*, 2013; Pande and Zambreno, 2012; Abd El-Latif *et al.*, 2012; Flayh *et al.*, 2009; Yu *et al.*, 2010; Vilardy *et al.*, 2011). This approach still determines a sharpest area and not the important area in an image. Accordingly, the IE security level in the frequency domain is not sufficient. Each one of has to fulfill the requirements of partial IE as depicted in Fig. 3. The face


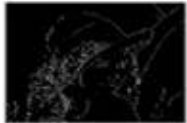






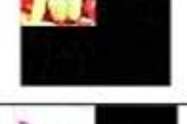








Images	Edge detection Approach	1-DWT Approach	2-DWT Approach
			
			
			
			
			
			
			
			

Fig. 3: Existing approaches for ROI selection

detection method determines it via skin color (Ravishankar and Venkateshmurthy, 2006; Khashan *et al.*, 2014; Hong and Jung, 2006; Riaz *et al.*, 2012; Rodriguesa *et al.*, 2006).

Preliminary work: In SIE, a section of the original image must be selected prior to the encryption process (Metzler and Aghaian, 2010). Hence, segmentation is the process of partitioning an image into semantically interpretable regions. It divides the image into a set of non-overlapping regions in terms of constituents or objects. Segmentation of SIE is one of the most intricate tasks in image processing (Sasikala and Mad, 2014; Kamble, 2013). These parts normally correspond to something that humans can easily separate and view as individual objects because computers cannot intelligently recognize objects. The segmentation process is based on various features contained in the image including its color information, boundaries, or segments. The level of details to which the subdivisions are carried out depend on the problem being solved (Baldevbhai and Anand, 2012). For accurate and efficient SIE the vitality features, wavelet transformation and logistic, piecewise and Arnold cat maps play paramount role (Ren *et al.*, 2013).

Vitality features: Vitality features are used to improve ROI determinism. Vitality also called Liveness Detection is a set of the biometric measures that contain recognizable features such as fingerprint, iris and face ... etc. Skin vitality is used to extract features depending on the human skin smoothness. It is always less than the artificial masks and even the softest skin has some roughness as shown in Fig. 4 (Singh *et al.*, 2012). These features are recorded using efficient vitality detection method and extracted from face image. Following vitality features, ROI in color image can be detected based on the picture roughness and smoothness. In our work the extracted features are employed to classify the image contents via roughness evaluation of each block in the color image by specifying if this block contains an important data or not.

Generally, blocks with high roughness signify the possession of sensitive data and those with low roughness contains insensitive data. However, the

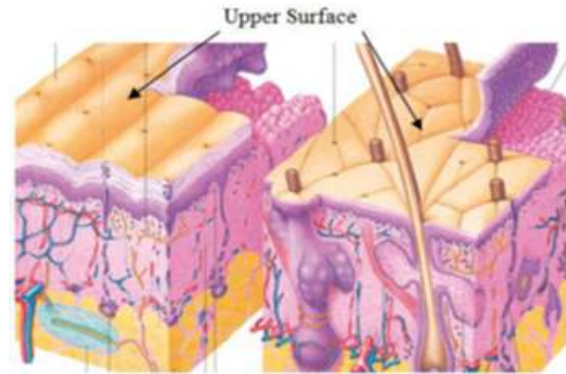


Fig. 4: The validity features of smooth (left) and rough (right) skin

reverse is true in our dataset meaning that the blocks with high smoothness represent sensitive data and vice versa. Therefore, roughness improvement remains essential for specific representation of ROI. Figure 5 displays the ROI for some dataset via smoothness region.

The modern encryption technique SIE is based on information separation process into perceptually sensitive and insensitive data following special criteria. The security level of this method depends on the selection of ROI and the encryption method used. It is essential to strengthen the security performances of SIE to protect the image from intruder and attain a reasonable security (Kulkarni, 2012). Highly precise segmentation improvement is achieved with low computation complexity through roughness measurement of vitality features using smoothing function. The principle goal of smoothing function is to find the probability distribution of the ratio when the series $\{x_i\}$ obeys Gaussian distribution. The coefficient of interest of a sequence acts as a general indicator of the roughness (or smoothness). Thus, the noncircular definition is the more natural because the series that is otherwise smooth should not usually be penalized for a difference between its values. The circular (roughness) coefficient yields (Bloomfield, 2000; Kirchgässner and Jürgen, 2007):

$$Roughness = \frac{Diff_i}{\delta}$$

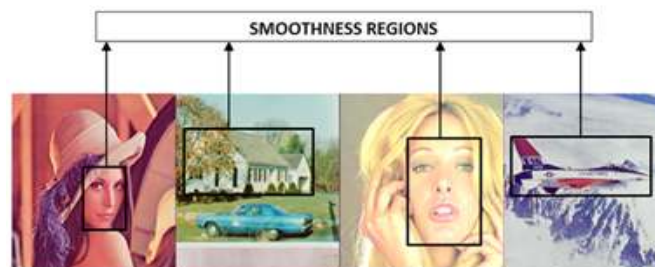


Fig. 5: The smooth region of four different color images representing ROI

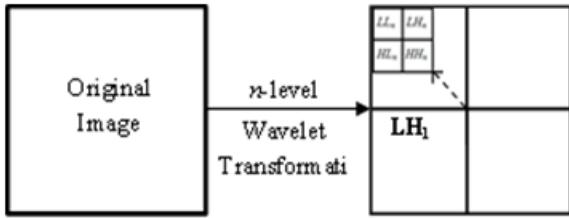


Fig. 6: Image decomposition into (3n+1) sub-bands via n-level wavelet transform

The variance ∂ is expressed as (Rosner, 2010):

$$\partial = \sum_{i=1}^{N-1} (x_i - \bar{x})^2$$

The arithmetic mean (\bar{x}) referred as the average rate is defined as (Rosner, 2010):

$$\bar{x} = \sum_{i=1}^N \left(\frac{x_i}{N}\right)$$

with,

$$Diff = \sum_{i=1}^{N-1} (x_i - x_{i-1})^2$$

where, x is the sequence values of $i = 1..N$ and N is the total number of values. The roughness coefficient is applied on color image to improve the ROI determination. Blocks with low value is determined as ROI otherwise remain insensitive.

Discrete wavelet transformation: Wavelet Transform being one of the most powerful mathematical tools in digital signal processing simultaneously examines an image in the time and frequency domains. The image components are decomposed into n different levels using DWT where each level consists of four sub-bands. These decomposition levels contain a low-resolution smooth image (LL_n) and a number of detailed information ($HL_n, LH_n, HH_n, HL_{n-1}, LH_{n-1}, HH_{n-1}, \dots, HL_1, LH_1, HH_1$) as shown in Fig. 6 (Flayh *et al.*, 2009; Chen and Wu, 2002; San and Nirmala, 2014).

Chaotic map methods: One dimensional logistic map can be represented as (Taneja *et al.*, 2011):

$$x_{i+1} = \mu x_i (1 - x_i)$$

where, $0 \leq x_i \leq 1$. The parameter μ and x_0 together form the encryption key. The logistic map exhibits high sensitivity to initial conditions for $3.57 < \mu < 4$. This map is extensively used by cryptographic community to generate a pseudorandom sequence due to its high sensitivity and chaotic behavior. Whilst, Arnold cat map is used to scramble the image by employing shearing and wrapping operation. The representation of

Arnold map for a matrix of size $N*N$ is given by Makris and Antoniou (2012):

$$\begin{aligned} \begin{pmatrix} x' \\ y' \end{pmatrix} &= Q \begin{pmatrix} x \\ y \end{pmatrix} \text{mod}(N1) \\ &= \begin{bmatrix} 1 & p \\ p & pq + 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod}(N1) \end{aligned}$$

where, p and q are positive integers acting as Cat map control parameters. Here (x, y) and (x', y') are the old and the new pixels positions, respectively with $N1$, the total number of pixels in the image ($N*N$). After some iteration the Arnold cat map yields a completely distorted image without any increase in its size. The periodic property of this map ensures that the image is transformed back to its original form. Due to this periodic property the Arnold scrambled image is encrypted by logistic output in the proposed technique. Finally, the family of chaotic maps named as piecewise linear chaotic maps or PWLCM. This is a class of discrete dynamical systems which are always chaotic for all the values of control parameters. The PWLCM is used to generate automatic secret expressed as Rhouma *et al.* (2009):

$$X_{i+t} = \begin{cases} \frac{X_i}{m} & 0 \leq X_i < m \\ \frac{X_i - m}{1 - m} & m \leq X_i \leq 1 \end{cases}$$

where, x_i and m are the iterative value and the system parameter symbolizes is the total number of blocks in the image, respectively. To obtain random and non-periodic numbers m is restricted in the range of 0 to 1 (Ardabili, 2012).

PROPOSED METHODOLOGY

Firstly, the image is divided into $n*n$ blocks and the new feature is extracted to determine ROI based on rough and smooth characteristics. The blocks are classified into rough, smooth and very smooth regions which correspond to the low, high and medium sensitivity level, respectively. Secondly, t secret keys are automatically generated based on PWLCM and logistic map with one initial key K_0 . Lastly, three models are used to encrypt regions based on its classification group.

First model is the Encryption Algorithm 1. It is implemented for high sensitivity level group using confusion diffusion chaotic map methods in spatial domain. The second model is the Encryption Algorithm 2 which encrypts the medium sensitivity level group using 1-level DWT with chaotic map methods. Last one is the Encryption Algorithm 3 which is executed for low sensitivity group via shuffling region using Arnold cat map for $P1$ iterations in 1-level DWT.

Now we turn our attention on selective image encryption in hybrid domain. The proposed method is comprised of three main phases. The first phase determines and selects the ROI, the second one generates automatic secret key and the final one implements strong encryption algorithm using chaotic map techniques. Figure 7 to 9 represent the new selection techniques, the method of secret key generation and encryption process, respectively. These three phases are highlighted hereunder.

Determining and selecting ROI: Various steps for the proposed algorithm for extracting dominant region from a given input RGB image (IM) of size $N*N$ is listed as:

Step 1: Convert RGB input image into YCbCr color space image and store in IMI .

Step 2: Determine the total number of blocks in image using $W = (N/M)^2$.

Step 3: Divide both images IM and IMI into W blocks denoted by BIM and $BIMI$ each of size $M * M$.

Step 4: Generate secret keys automatically with the initial input K_0 and W .

Step 5: Find the roughness value for each block of IMI .

Step 5.1: Evaluate the (\bar{x}) for each block using Eq. (3) and store the result in $MEAN_i$.

Step 5.2: Evaluate the (σ) of each block using Eq. (2) and store the result in Vi .

Step 5.3: Evaluate the $(Diff)$ using Eq. (4) and store result in DFi .

Step 5.4: Evaluate the (Roughness) of each block using Eq. (1) and store result in Ri .

Step 6: Identify significant and insignificant blocks.

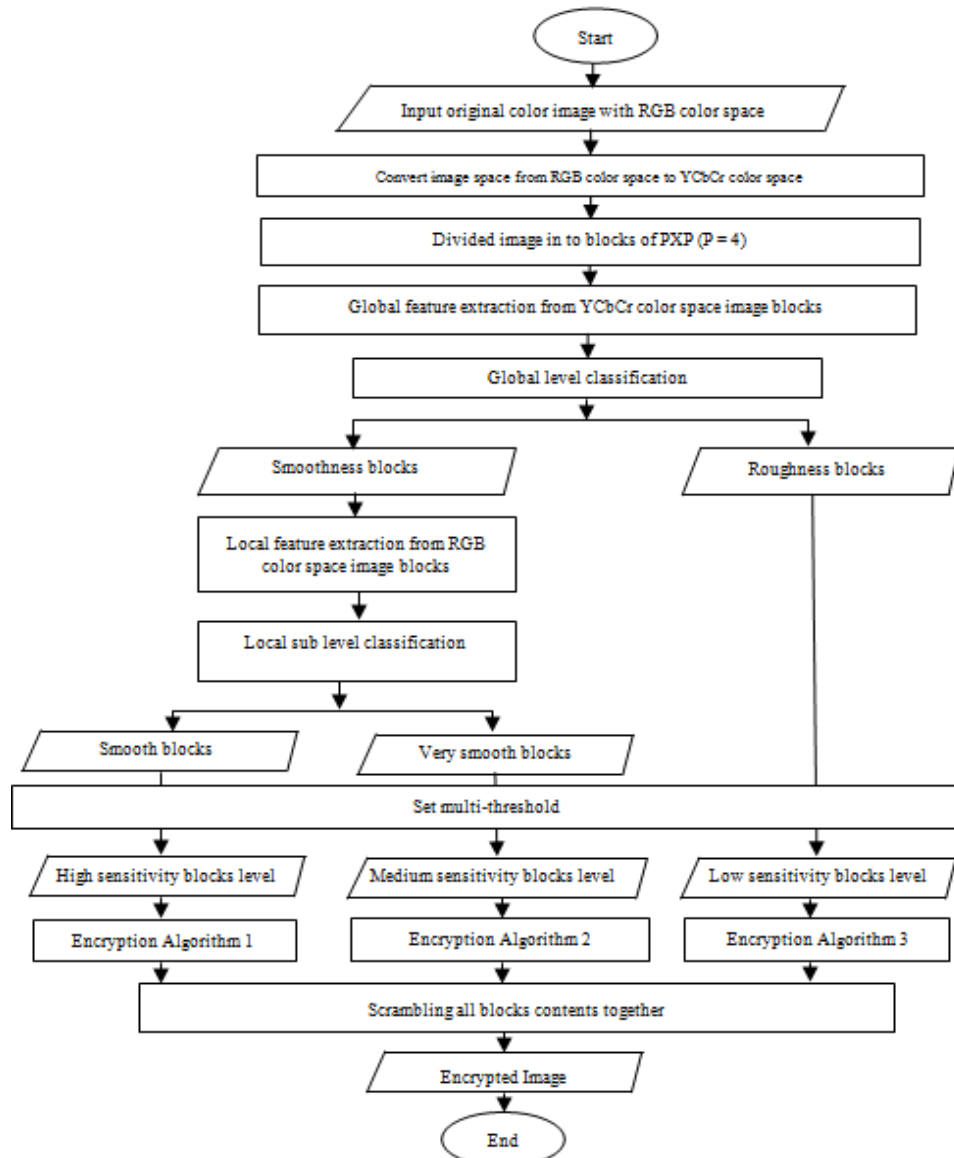


Fig. 7: Block diagram for the selection and classification of ROI

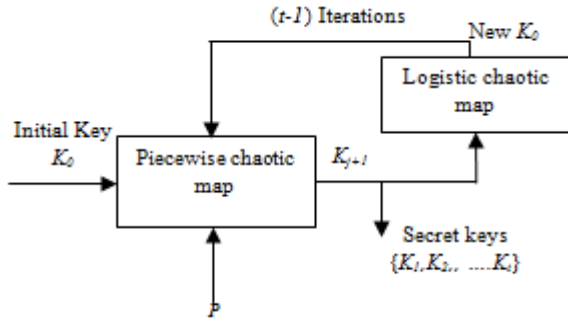


Fig. 8: Block diagram for automatic secret keys generation

Step 6.1: Set the threshold of image using user-defined $Q1$ that decides the threshold level and is given by:

$$Eth = Q1 * \sum_{i=1}^W (\frac{Roughness_i}{W}),$$

$Q1$ is taken as 0.017

Step 6.2: Generate a binary significant vector ($BSVi$) of size $1*W$, where each vector element corresponds to a block in the input image IMI . A '1' in the $BSVi$ reflects the corresponding block in input image as significant blocks, while others are insignificant (roughness) blocks,
 -if $Ri < Eth$ then
 -set $BSVi = 1$ (smoothness block content)
 otherwise- $BSVi = 0$ (roughness block content)

Step 7: Determine the smoothness region from the significant blocks in IM image.

Step 7.1: Evaluate the (\bar{x}) for each significant block using Eq. (3) and store the result in $SMEANI$

Step 7.2: Evaluate the (∂) of each significant block using Eq. (2) and store the result in SVi .

Step 7.3: Evaluate the (Diff) for each significant block using Eq. (4) and store the result in $SDFi$.

Step 7.4: Evaluate the (Roughness) of each significant block using Eq. (1) and store the result in SRI .

Step 8: Identify smoothness for very smooth blocks.

Step 8.1: Set the threshold of image IM following user-defined $Q2$ that decides the threshold level ($Q2$ is taken as 0.48):

$$SEth = Q2 * \sum_{i=1}^{SW} (\frac{Roughness_i}{SW})$$

Step 8.2: Generate a new binary significant vector ($BSVi$) of size $1*W$, where each vector element corresponds to a block in the input image IM . Set all $BSVi$ with '0' as roughness, then check each significant block and set '1' in the $BSVi$ for the smoothness block and set '2' to $BSVi$ for very smooth block
 -if $SRI < SEth$ then
 -set $BSVi = 1$ (smoothness block content).
 otherwise- $BSVi = 2$ (very smooth block content).

Step 9: if $BSVi = '2'$ then:

Roughness blocks are encrypted with module 3
 Else
 If $BSVi = '1'$ then
 Smoothness blocks are encrypted with module 1
 Otherwise
 Very smooth blocks are encrypted with module 2

Generating automatic secret keys: In this step the generated initial secret key is used in encryption steps. An input parameter for generating secret key is considered with the one initial input secret key ($K0$). Then, based on the value of $K0$ a set of secret keys is generated using a combination between logistic and

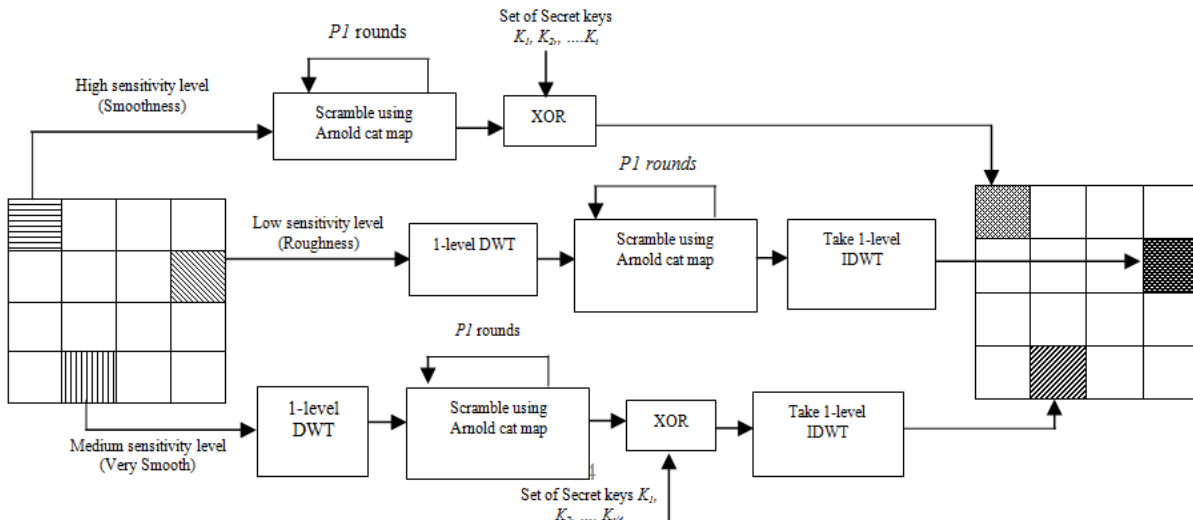


Fig. 9: Block diagram for encryption process

Original Images	Roughness/Smoothness	Sensitivity Level	Encrypted Image
			
			
			
			
			
			
			
			

Fig. 10: ROI selection and encrypted images

piecewise chaotic map methods. Furthermore, the total number of secret keys remains the same with number of blocks. The piecewise chaotic map method is used to generate these set (Ardabili, 2012). Figure 8 depicts the block diagram for the automatic secret key generation. The input is the initial secret key K_0 ranges between 0 and 1 with $0 < P \leq 4$ and t is the total number of secret keys generated to obtain the final output $\{K_1, K_2, \dots, K_t\}$.

Encryption algorithm: Figure 7 illustrates the proposed combinational domain encryption approach. This phase concerns with the implementation of the protected important blocks based on the classification together with the set of secret key generation. All blocks that contain high sensitivity level of color image are protected with safety chaotic map in the spatial domain (Encryption Algorithm 1). Meanwhile, blocks that are classified as the medium sensitivity level are encrypted in 1-DWT domain using chaotic map methods. Finally, the blocks with low sensitivity level are shuffled using Arnold cat map in 1-DWT. Figure 9 displays in detail the encryption algorithm for each region.

In Encryption Algorithm 1 module, the blocks which are classified as high sensitivity level with smoothness region are encrypted using the chaotic map method in spatial domain. At the first step, the block is scrambled using Arnold cat map for $P1$ iterations before XOR-ing it with set of pre-generated secret keys. Whilst, using Encryption Algorithm 2 module, the blocks which are classified as medium sensitivity level with very smooth regions are encrypted in 1-DWT domain based on the chaotic map method. Firstly, the block is scrambled using Arnold cat map in the $P1$ iterations before XOR-ing it with set of pre-generated secret keys and making inverse 1-DWT of the block at the end. The last Encryption Algorithm module focused on the changing pixel positions without changing their values. The Arnold chaotic map is used for scrambling pixels in 1-DWT for $P1$ iterations. Finally, the block of 1-DWT is inverted.

RESULTS AND DISCUSSION

Several experiments were performed to measure the encrypted area for selective image in determining their security level. All simulations were conducted using a 32-bit operating system, 1.70 GHz CPU of 4 GB main memory to ensure the proficiency of the proposed algorithm. The MATLAB R2008a codes were used and eight well-known color images Lena, Pepper, Splash, Airplane, House, Tiffany, Baboon and Sailboat were acquired from the USC-SIPI Image Database (<http://sipi.usc.edu/dataset>) with corresponding secret key set 0.4, 0.866, 0.4, 0.3, 0.3, 0.002, 0.3 and 0.7, respectively. Each color images of size 512*512 pixels

Table 1: Encrypted area and entropy values of all dataset images

Sample images	Initial key	Encrypted area (%)	Entropy
Lena	0.400	25.00	7.30
Pepper	0.866	43.75	7.70
Splash	0.400	43.75	7.61
Airplane	0.300	50.00	7.78
House	0.300	50.00	7.79
Tiffany	0.002	50.00	7.72
Baboon	0.300	56.25	7.88
Sailboat	0.700	56.25	7.82

Table 2: CCs of encrypted images

Sample images	Horizontal CC	Vertical CC	Diagonal CC	Avg. CC
Lena	+0.00152	-0.02260	-0.00246	-0.00784
Pepper	+0.01579	+0.00371	-0.00574	+0.00458
Splash	+0.00266	+0.00149	-0.00564	-0.00049
Airplane	+0.00380	-0.00068	-0.00418	-0.00035
House	+0.03477	-0.02802	-0.00405	+0.00089
Tiffany	+0.00534	-0.00018	-0.00668	-0.00050
Baboon	+0.00480	+0.01426	-0.02032	-0.00042
Sailboat	-0.01988	+0.00878	+0.00991	-0.00039

Avg.: Average

were selected with the block size of 128*128 pixels, the threshold levels were $T1 = 0.0017$ and $T2 = 0.48$. The performance analysis of selective image encryption in hybrid domain with chaotic maps was performed by measuring the encrypted area, entropy, Correlation Coefficients (CCs) and Histogram.

Figure 10 shows the selection and classification of ROI of the original image for all data set images as mentioned. Base on the image classification blocks in Fig. 10, the rates of encrypted area and entropy values were computed and summarized in Table 1. The histograms of three channels for four sample images are displayed in Fig. 11. The calculated CCs for all data set images are enlisted in Table 2. Moreover, Fig. 12 displays the achieved very good distribution of the automatic 120 secret keys which are randomly generated in the range of 0 to 255.

Test is carried out on the histogram of enciphered image to demonstrate that our proposed algorithm achieves strong resistance to statistical attacks. The histograms of all the color images are compared with their corresponding ciphered image. Four typical examples are found to have different encrypted area rates. The histogram (Fig. 11) of all four original images exhibits large spikes but the cipher images show uniform base of rates in the encrypted area. It is clear that the histogram of the encrypted image is significantly different from the respective original image without any statistical resemblance to the plain image with high encrypted area. Moreover, the encrypted area as shown in Fig. 13 is found to vary for all images based on the significant blocks that are used for encryption.

Table 1 clearly reveals that all the dataset images possess high entropy. The correlation coefficient for each image varies. This variation is primarily attributed to the different rates of encrypted area used to encrypt

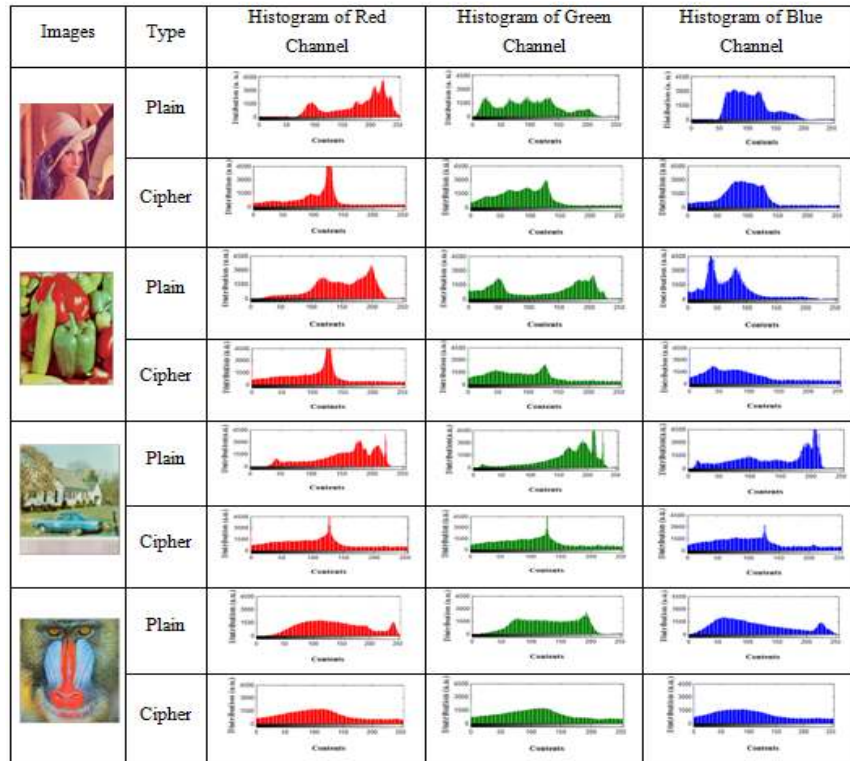


Fig. 11: Histogram of original and encrypted images

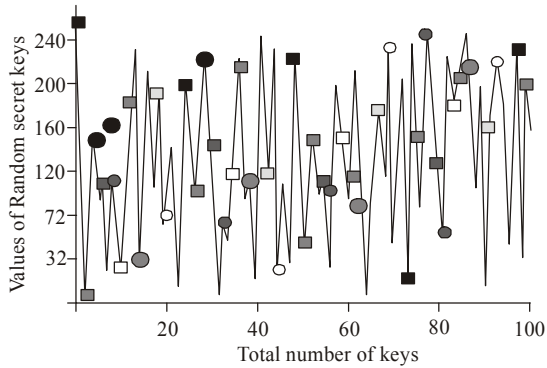


Fig. 12: Distribution of secret key set

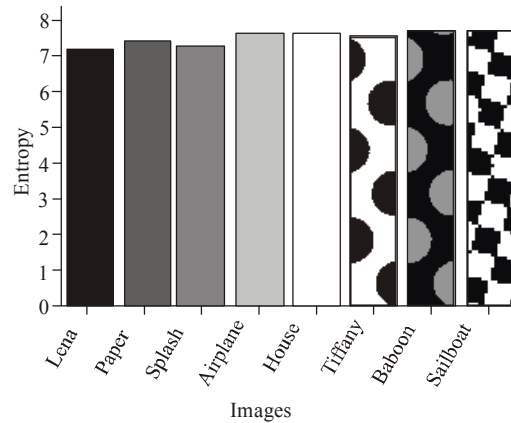


Fig. 14: Entropy values of all dataset images

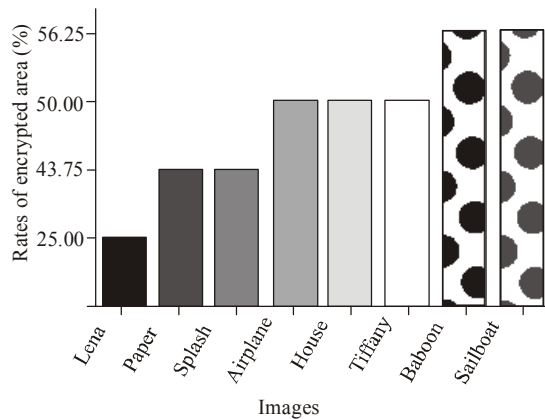


Fig. 13: Rates of encrypted area

each image and the random selection of horizontal, vertical and diagonal vectors containing the pairs of pixels. Moreover, all entropy values (Fig. 14) remain at the same level implying that all data set encrypted image cannot be broken by threat. The correlation coefficients for all dataset images in all three directions are found to be close to 0 as illustrated in Fig. 15. The absence of any similarity between the original image and the encrypted image are evident. Consequently, the entropy increases with the increase of encrypted area and the correlation coefficient is close to 0. Therefore, the values of entropy and average CCs for all images demonstrate that the proposed selective image

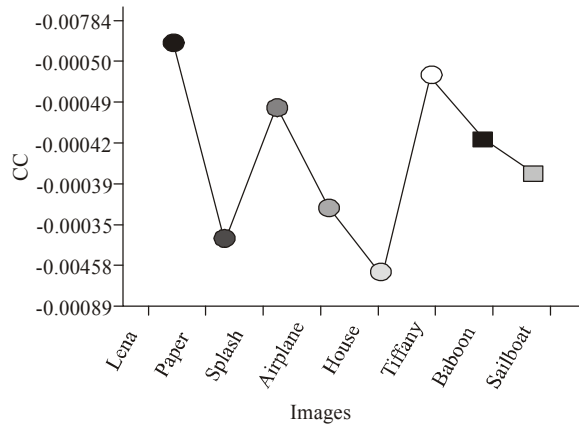


Fig. 15: Average CCs of all dataset images

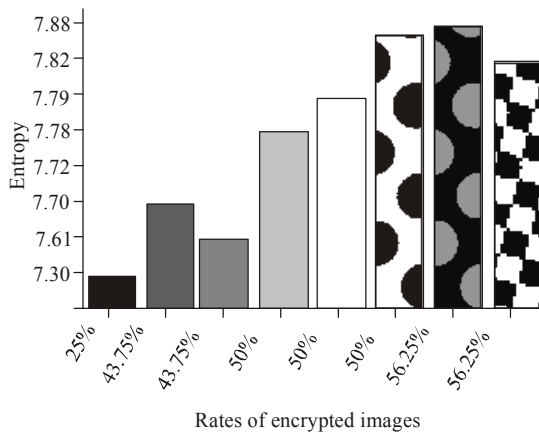


Fig. 16: Security level versus encrypted area

Table 3: Encrypted area from proposed method versus previous work

Sample images	Proposed method encrypted area (%)	Edge detection method encrypted area (%)
Lena	25.00	43.75
Pepper	43.75	56.25
Splash	43.75	50.00
Airplane	50.00	43.75
House	50.00	31.25
Tiffany	50.00	37.50
Baboon	56.25	43.75
Sailboat	56.25	50.00

Table 4: Entropy values from proposed method versus previous works

Sample images	Proposed method	Edge detection-based method
Lena	7.30	7.27
Pepper	7.70	7.73
Splash	7.61	7.35
Airplane	7.78	6.48
House	7.79	6.95
Tiffany	7.72	6.03
Baboon	7.88	7.62
Sailboat	7.82	7.57

encryption with more than 25% encrypted area rate are free from any statistical attack. Indeed, the rate of encrypted area in the whole image is directly correlated to the security level as depicted in Fig. 16.

Table 5: Average CC for proposed method versus previous work

Sample images	Proposed method	Edge detection-based method
Lena	-0.00784	-0.00884
Pepper	+0.00458	+0.00846
Splash	-0.00049	-0.00055
Airplane	-0.00035	-0.00062
House	+0.00089	+0.00509
Tiffany	-0.00050	-0.00056
Baboon	-0.00042	-0.00616
Sailboat	-0.00039	-0.00216

Comparative analysis: The performances of our proposed selective ROI method is compared with the previous studies using edge detection method (Taneja *et al.*, 2011; Khashan *et al.*, 2014). The entropy and encrypted area rates are used in this comparison for the same dataset in color scales for security improvement. The encrypted areas of the ciphered images are computed for each algorithm and the results are furnished in Table 3. It clearly displays the distinction between our method and previous methods in terms of the rates of the encrypted areas. Furthermore, Table 4 exhibits the achievement of highest entropy possibility implies minimal threat. In the present case, no one can break the cipher without knowing the secret key compare to the previous method. Although, the encrypted area of the proposed method is lesser than previous method but the higher entropy values for Lena and Splash image indicate that the mean the security performances of proposed method is improved. Furthermore, the average CC of our method is also close to 0 compare to the previous work as enlisted in Table 5. Thus, the comparison reveals that the new method achieves best security performance.

CONCLUSION

SIE is demonstrated to be one of the most promising solutions to reduce the protected area. A novel solution for selective encryption to achieve image protection effectively with correct significant ROI is proposed. Simulation is carried using MATLAB codes on eight images each of size 512*512 pixels acquired from standard USC-SIPI Image Database. A block size of 128*128 pixels with threshold levels 0.0017 and 0.48 are employed. Unique texture features are used to determine ROI with new classification for selecting ROI. Different level of encryption is performed depending upon selection of ROI which enhanced the overall security performance. The automatic secret keys are generated by combining chaotic maps method and only one initial secret key is used to get set of others. The implemented encryption involves the selection of ROI, vitality features manipulation and Prewitte edge detection method. The development and implementation of SIE based on percentage of encryption area. The vitality features are used to determine the ROI based on the performances of the

rough and smooth areas for color image with a multi-threshold value. The blocks with smooth and very smooth area represented the most important and medium important parts, respectively. The roughness area was attributed to the unimportant parts. The blocks were classified according to the sensitivity level such as low, medium and high. Each level used new model for encrypting the block contents. Our approach achieved best encrypted area with suitable security performances compared to the previous reports. We assert that the proposed algorithm can be used in encrypting any color image obtained from satellite and medical areas because both of them need selected ROI before being encrypted with greater security from transferring into unauthorized hands.

ACKNOWLEDGMENT

Lahieb is grateful to the Ministry of Higher Education and Scientific Research, Iraq for providing sponsorship to continue her PhD.

REFERENCES

- Abd El-Latif, A.A., X. Niu and M. Amin, 2012. A new image cipher in time and frequency domains. *Opt. Commun.*, 285(21): 4241-4251.
- Abd El-Latif, A.A., L. Li, N. Wang, J.L. Peng, Z. Shi and X. Niu, 2014. A new image encryption scheme for secure digital images based on combination of polynomial chaotic maps. *Res. J. Appl. Sci. Eng. Technol.*, 4(4): 322-328.
- Apoorva and Y. Kumar, 2013. Comparative study of different symmetric key cryptography algorithms. *Int. J. Appl. Innov. Eng. Manage.*, 2(7): 204-206.
- Ardabili, M., 2012. A novel image encryption approach based on chaotic piecewise map. *J. Theor. Phys. Cryptogr.*, 1: 37-40.
- Baldevbhai, P.J. and R.S. Anand, 2012. Review of graph, medical and color image base segmentation techniques. *J. Electr. Electron. Eng.*, 1(1): 1-19.
- Benlcouiri, Y., M. Benabdellah, M.C. Ismaili and A. Azizi, 2014. A new approach of crypto-compression on MPEG format. *Res. J. Appl. Sci. Eng. Technol.*, 7(18): 3791-3796.
- Bhatnagar, G. and Q.M. Jonathan Wu, 2012. Selective image encryption based on pixels of interest and singular value decomposition. *Digit. Signal Process.*, 22(4): 648-663.
- Bloomfield, P., 2000. *Fourier Analysis of Time Series: An Introduction*. 2nd Edn., John Wiley and Sons Inc., Hoboken, NJ.
- Chen, S. and C. Wu, 2002. An architecture of 2-D 3-level lifting-based discrete wavelet transform. *Proceeding of the VLSI Des. CAD Symposium*, 1: 351-354.
- Dutta, S. and B.B. Chaudhuri, 2009. A color edge detection algorithm in RGB color space. *Proceeding of the 3rd International Conference on Advances in Recent Technologies in Communication and Computing*, pp: 337-340.
- Evans, A.N. and X.U. Liu, 2006. A morphological gradient approach to color edge detection. *IEEE T. Image Process.*, 15(6): 1454-1463.
- Flayh, N.A., R. Parveen and S.I. Ahson, 2009. Wavelet based partial image encryption. *Proceeding of the International Multimedia, Signal Processing and Communication Technologies (IMPACT '09)*. Aligarh, pp: 32-35.
- Hoang, T.M. and D. Tran, 2014. Cryptanalysis and security improvement for selective image encryption. *Eur. Phys. J. Spec. Topics*, 223(8): 1635-1646.
- Hong, K. and K. Jung, 2006. Partial encryption of digital contents using face detection algorithm. *Proceeding of 9th Pacific Rim International Conference on Artificial Intelligence*, Guilin, China, pp: 632-640.
- Hong, T.M. and D. Tram, 2014. Cryptanalysis for selective image encryption. *Eur. Phys. J. Spec. Topics*, 223(8): 1635-1646.
- Jawad, L.M. and G.B. Sulong, 2013. A review of color image encryption techniques. *Int. J. Comput. Sci. Issues*, 10(6): 266-275.
- Kamble, P.D., 2013. A study of edge detection and image segmentation by using thresholding. *Int. J. Comput. Sci. Inform. Technol.*, 1(1): 44-46.
- Khashan, O.A., A.M. Zin and E.A. Sundararajan, 2014. Performance study of selective encryption in comparison to full encryption for still visual images. *J. Zhejiang Univ., Sci. Comput. Electr.*, 15(6): 435-444.
- Kirchgässner, G. and W. Jürgen, 2007. *Introduction to Modern Time Series Analysis*. 2nd Edn., Springer, Berlin, Heidelberg, New York.
- Kulkarni, N., 2012. Color thresholding method for image segmentation of natural images. *Int. J. Image Graph. Sign. Proc.*, 4(1): 28-34.
- Kumar, P. and P.K. Pateriya, 2012. RC4 enrichment algorithm approach for selective image encryption. *Int. J. Comput. Sci. Commun. Netw.*, 2(2): 181-189.
- Makris, G. and I. Antoniou, 2012. Cryptography with chaos. *Proceeding of 5th International Conference of Chaotic Modeling and Simulation*. Athens, Greece, pp: 309-318.
- Metzler, R.E.L. and S.S. Agaian, 2010. Selective region encryption using a fast shape adaptive transform. *Proceeding of IEEE International Conference on System Man and Cybernetics*. Istanbul, pp: 1763-1770.

- Pan, F., C. Wang and X. Chen, 2010. An image encryption scheme based on image complexity. Proceeding of the IEEE International Conference on Information Theory and Information Security. Beijing, China, pp: 462-465.
- Pande, A. and J. Zambreno, 2012. The secure wavelet transform. *J. Real Time Image Proc.*, 7(2): 131-142.
- Panduranga, H.T. and S.K. Naveenkumar, 2013. Selective image encryption for medical and satellite images. *Int. J. Eng. Technol.*, 5(1): 115-121.
- Puech, W., A.G. Bors and J.M. Rodrigues, 2013. Protection of Colour Images by Selective Encryption. In: Fernandez-Maloigne, C. (Ed.), *Advanced Color Image Processing and Analysis*. Springer Publisher, New York, pp: 397-421.
- Rad, R.M., A. Attar and R.E. Atani, 2013. A comprehensive layer based encryption method for visual data. *Int. J. Signal Process. Image Process. Pattern Recogn.*, 6(1): 37-48.
- Ravishankar, K.C. and M.G. Venkateshmurthy, 2006. Region based selective image encryption. Proceeding of the International Conference on Computing and Informatics. Kuala Lumpur, pp: 1-6.
- Rehman, A.U, X. Liao, A. Kulsoom and S.A. Abbas, 2014. Selective encryption for gray images based on chaos and DNA complementary rules. *Multimed. Tools Appl.*, 2014: 1-23.
- Ren, H., D. Linlin and Z. Jian, 2013. Image encryption algorithm based on chaos mapping and the sequence transformation. *Res. J. Appl. Sci. Eng. Technol.*, 5(22): 5308-5313.
- Rhouma, R., D. Arroyo and S. Belghith, 2009. A new color image cryptosystem based on a piecewise linear chaotic map. Proceeding of the 6th International Multi-Conference on Systems, Signals and Devices and Conference on Power Electronical Ssems. Djerba, Tunisia, pp: 1-6.
- Riaz, F., S. Hameed, I. Shafi, R. Kausar and A. Ahmed, 2012. Enhanced image encryption techniques using modified advanced encryption standard. *Comm. Com. Inf. Sc.*, 281: 385-396.
- Rodriguesa, J.M., W. Puecha, A.G. Borsb, C. Science and Y. Yoo, 2006. Selective encryption of human skin in JPEG images. Proceeding of the IEEE International Conference on Image Processing. Atlanta, GA, pp: 1981-1984.
- Rosner, B., 2010. *Fundamentals of Biostatistics*. 7th Edn., Harvard University, Boston, USA.
- San, A. and K. Nirmala, 2014. A gray texture classification using wavelet and curvelet coefficients. *Res. J. Appl. Sci. Eng. Technol.*, 7(24): 5258-5263.
- Sasikala, D. and M. Mad, 2014. Identification of carotid asymptomatic plaque using texture and orientation features for health care. *Res. J. Appl. Sci. Eng. Technol.*, 8(1): 56-63.
- Shekhar, S., H. Srivastava and M.K. Dutta, 2012. An efficient adaptive encryption algorithm for digital images. *Int. J. Comput. Electr. Eng.*, 4(3): 380-383.
- Singh, A., S. Tiwari and S.K. Singh, 2012. Vitality detection in face images using second order gradient. *Int. J. Comput. Appl. Inf. Technol.*, 1(2): 96-101.
- Spinsante, S. and E. Gambi, 2009. Selective encryption for efficient and secure transmission of compressed space images. Proceeding of the International Workshop on Satellite and Space Communications. Tuscany, Italy, pp: 9-11.
- Steffi, M.A.A. and D. Sharma, 2011. Comparative study of partial encryption of images and video. *Int. J. Mod. Eng. Res.*, 1(1): 179-185.
- Suresh, V. and C.E.V. Madhavan, 2012. Image encryption with space-filling curves. *Defence Sci. J.*, 62(1): 46-50.
- Taneja, N., B. Raman and I. Gupta, 2011. Combinational domain encryption for still visual data. *Multimed. Tools Appl.*, 59(3): 775-793.
- Ullah, I., W. Iqbal and A. Masood, 2013. Selective region based images encryption. Proceeding of the 2nd National Conference on Information Assurance. Rawalpindi, pp: 125-128.
- Vilardy, J.M., J. Useche, C.O. Torres and L. Mattos, 2011. Image encryption using the fractional wavelet transform. *J. Phys. Conf. Ser.*, 274(1): 1-7.
- Wang, X. and Q. Wang, 2013. A novel image encryption algorithm based on dynamic s-boxes constructed by chaos. *Nonlinear Dynam.*, 75(3): 567-576.
- Yu, Z., Z. Zhe, Y. Haibing, P. Wenjie and Z. Yunpeng, 2010. A chaos-based image encryption algorithm using wavelet transform. Proceeding of the 2nd International Conference on Advanced Computer Control. Shenyang, pp: 217-222.
- Yue, M., 2012. Based on negative selection algorithm to generate long-period pseudo-random sequence. *Res. J. Appl. Sci. Eng. Technol.*, 4(14): 2167-2170.
- Zhang, W., K. Wong, H. Yu and Z. Zhu, 2013a. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. *Commun. Nonlinear Sci.*, 18(3): 584-600.
- Zhang, Y., D. Xiao, W. Wen and Y. Tian, 2013b. Edge-based lightweight image encryption using chaos-based reversible hidden transform and multiple-order discrete fractional cosine transform. *Opt. Laser Technol.*, 54(30): 1-6.