Indian Journal of Science and Technology, *Vol 8(27), DOI:10.17485/ijst/2015/v8i27/71241, October 2015*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Survey on Emerging Challenges in Selective Color Image Encryption Techniques

Lahieb Mohammed Jawad[1,2]* and Ghazali Sulong[1]

[1]UTM-IRDA Digital Media Center (MaGIC-X), Faculty of Computing, Universiti Teknologi Malaysia, Skudai - 81310, Johor, Malaysia; lahieb1978@gmail.com, ghazali@utmspace.edu.my
[2]Network Engineering Department, Collage of Information Engineering, Al-Nahrain University, Baghdad, Iraq

Abstract

Background/Objectives: Selective image encryption is the best modern approach for reducing the amount of encrypted area. The objective of this paper is to study the strength and limitationof the modern approach. **Methods**: This survey has mainly focuses on reviewing modern approaches in literature on selective encryption and classifies them into three categories based on region of interest selection, image encryption techniques and key managements. Therefore, their strengths and limitations are identified in order to establish possible solution for the future of selective encryption research. **Findings:** This survey comprehensively determine the limitations and strengths of the selective image encryption technique based on the fact that this approach saves cost and time via reducing the size of encrypted region. The literature of the different methods is analyzed based on each category. It derived the remaining gaps for selective image encryption approach; a big gap in selective image encryption is on how to split image into significant and insignificant region. Moreover, there is still gap in the security results of traditional encryption algorithm for modern approach and the key space size is also one of an important factor in obtaining high security level for any encryption algorithm. **Improvements:** This survey identifies the major limitation of its strategies as encryption of certain regions in an image does not guarantee security. Moreover, the traditional encryption algorithms still need security improvements.

Keywords: Block Selection, Image Encryption Domain, Key Management, Region of Interest, Selective Image Encryption, Stream Selection

1. Introduction

Due to the rapid demand for image data in real-time, encryption or decryption can be time consuming, therefore, will require careful consideration into its processes for effective information sharing[1,2]. The time required to be expended on information sharing is basically addressed from two perspectives: encryption and transfer time. In order to avoid spending a lot of time in image encryption, a number of methods have been proposed in literature, one of which is the selective encryption (partial encryption) method[3,4].

The selective (modern) encryption approach dissimilar to the full (traditional) encryption approaches secures just critical regions in an original image, as clarify in Figure 1. The principle goal of the modern encryption strategy is that it can give similarly, security and complexity requirements without tradeoffs. The benefits of the modern encryption strategy are essentially in real-time applications, where privacy is vital and tremendous measure of information becomes an integral factor. In essence, selective encryption is more practical in the real-time and main inquiry is how to reduce the complexity requirements with assurance information security[5,6].

*Author for correspondence

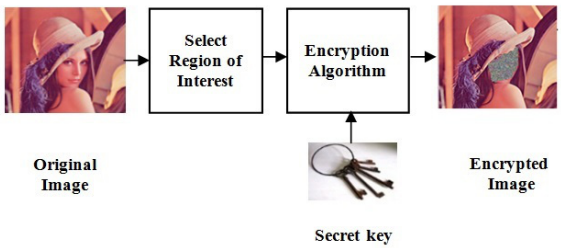

Figure 1. An overview of selective image encryption approach.

Due to the arsenal of works in selective encryption this paper focuses on surveying modern works in selective image encryption. The rest of this paper is organized as follows. In section 2, some preliminaries of encryption concept are discussed. The next section discusses the challenges of selective image encryption in the various types. While, section 4 summarizes the remaining issues and finally, section 5 is the conclusion.

2. Preliminaries

The main concepts of encryption and decryption are explains in this section including the principles of encryption and decryption, types of encryption key, the definition of block and stream cipher, and the description of image encryption algorithms types.

2.1 Principles of Encryption and Decryption

The encrypting systems are also known as ciphers. A cipher helps in transforming the plaintexts to ciphertexts and also helps in recovering the plaintexts from ciphertexts under control of the key. Here, the transforming operation and the recovering operation are named encryption and decryption, respectively. The key is necessary to decryption, because without the key, the plaintext cannot be recovered correctly. The original data is known as plaintext. The encrypted data is known as ciphertext. The plaintext and ciphertext is denoted by P and C. On the other hand, the decipher side used the input C with the secret key to get P[7].

2.2 Encryption Key

Generally, secret key is the compulsory condition for encrypted data. Both, the strength of the encryption algorithm and secrecy of the key is used in the security performance. The key remains independent of the plaintext. Hence, the same plaintext encrypts to different ciphertext with different keys, and in this way, both processes are impossible without the use of the correct key.

The secret key can be divided into two types such as public key (Asymmetric key) and symmetric key (private key). Public Key Cryptography (PKC) is also called asymmetric cryptography. It uses one key to encrypt and the other to decrypt. The encryption key is called a public key. It is an intelligible and can be distributed to all parties. Whereas, the decrypt key which is called a private key. It is understandable only to the receiver. Thus, both secret keys are created by each user. If one is used for encryption then the other is used for decryption[8]. Figure 2, indicates about the Encryption and decryption ingredients for both symmetric and Asymmetric key algorithms.

In symmetric key cryptography, to perform an encryption and decryption, the same secret keys are used. This key is only known to the sender and receiver for maintaining the integrity of the message. The primary demerit of the symmetric key algorithms is that the key should always remain secret. Thus for this purpose, the key should be kept in high protection and security which requires the sender to transmit the key to the recipient in a more secured way. Symmetric encryption is highly extensively used algorithm for images protection[9].

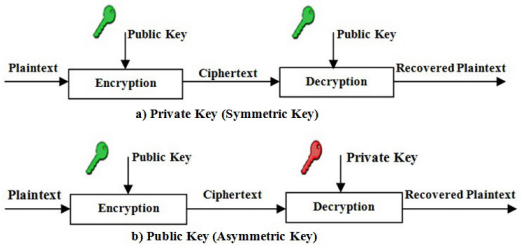

Figure 2. Types of encryption key. a) Symmetric key. b) Asymmetric key.

2.3 Block and Stream Cipher

Secret key methods can be classified in two groups, namely block and stream ciphers. A block cipher is a kind of symmetric key encryption algorithms which helps in transforming the block having fixed length of the plaintexts data to a block of ciphertexts data having same lengths. Hence, the fix length is known as the block size. Thus in numerous block ciphers, the size is 64 or 128 bits[10].

On the other hand, a stream cipher is an important class of symmetric key encryption scheme, when one byte at a

time was encrypted. Therefore, the cipher state is based on the current cipher action that is called state ciphers. Stream ciphers execute at a higher speed than block ciphers, and have lower hardware complexity. In a stream cipher, the same plaintext symbol will always be encrypted to a distinct ciphertext symbol due to different encryption transformation for each plaintext symbol. Actually, sometime the length of plain data is unknown that led the sender to use a stream cipher for encryption[11,12].

2.4 Image Encryption Algorithms

Image encryption is an important in all future multimedia Internet related application. But, such information is sent over or through a network. Thus, the protection of the transmitted image has become an important issue over a network. In fact, there are several convention encryption algorithms some implemented for block cipher and the rest for stream cipher.

The conventional algorithms under symmetric key are Data Encryption Standard (DES), Triple DES (3DES), Blowfish, Advanced Encryption Standard (AES), and many more. On the other hand, RC4 is the famous algorithm used in stream cipher[13]. Figure 3 will describe an overview of most common encryption algorithms used in conventional algorithms.

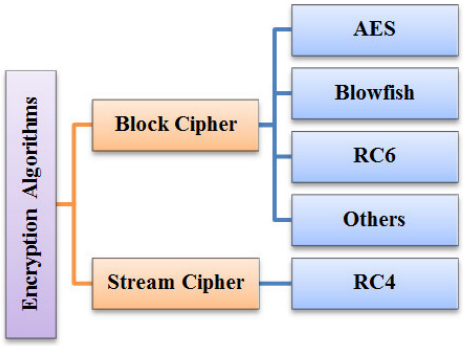

Figure 3. An overview of encryption algorithms.

3. Challenges Classification of Selective Image Encryption

To bring to understanding the intricacies of the selective encryption technique, the various approaches proposed in literatures will be presented based on the major classifications under which they are discussed. The major classifications are with respect to the region of interest selection, image encryption techniques, and key management. For each of these categories and how they contribute to selective image encryption technique is summarized in Figure 4 and discussed accordingly.

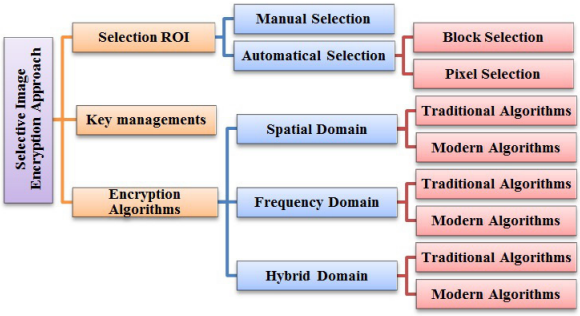

Figure 4. Categories of selective image encryption technique.

3.1 Region of Interest Selection

The encryption techniques under selective ROI are methods that encrypt only significant regions such that a portion of the original image should be chosen before protection[14]. The major prerequisite of any selective ROI technique under modern encryption is that the encrypted regions should be autonomous of the rest regions. The suggestion is that: If this condition does not hold, the protected areas can be effectively deciphered by an unapproved end client based on the correlation of the pixels of the encrypted regions to that of the pixels of unencrypted regions[15,16].

The selective ROI can be generally classified into two main techniques; manual selection and automatic selection. The manual selection is considered as the traditional technique which are exceptionally appropriate for uncommon applications, for example, medical image. It is helpful when the significant region is known, for instance, Panduranga et al.[17] proposed manual selective image encryption approaches, where the image is separated into non-overlap blocks. Each of the blocks is encoded via image mapping that is used as input data to the chose blocks. The full encryption of choosing blocks is additionally conceivable, and every block can utilize the different map. While, the dynamic selected region of interest is one of the suitable and well known methods that are implemented in different image encryption algorithms. In this study, the dynamic choice will be explained and characterized into two principal techniques (block selection and pixel Selection) which are clarified in points of interest in the accompanying subsections.

3.1.1 Block Selection

Selection of significant block is one of the famed methods that are utilized to determine ROI on the premise of particular features. A typical practice among studies for the selection of ROI is the appropriation of edge detection techniques. The edge detection operation is one of the speediest procedures for finding sharp changes that can either demonstrate lines, points or bends inside of an image. For example, let's take the Prewitt edge detector into consideration. The Prewitt edge detector has special characteristic to implement averaging of neighboring pixel values. As a useful tool for edge detection, it uses a mask filter of size 3 × 3 in estimating the magnitude and orientation of edge locations of an image[18,19]. In more recent times, Rad R M et al.[20] suggested an image encryption technique that combines several established algorithms such as, Blowfish, AES, Serpent and RC6. Their technique encrypts the sensitive blocks and the insensitive blocks are rescanned using four different pattern types. Further processes are carried out by means of edge detection in order to determine and likewise classify significant blocks from the insignificant blocks.

The frequency domain wavelet transformation approach is another approach commonly adopted. The image under transformation is firstly decomposed via wavelet transformation into several decomposition levels. These decomposition levels consist of a number of sub-bands with equal block size, which comprises of coefficients that describe all characteristics of the plain image. Therefore, the sub-band of low-frequency coefficient of wavelet transform is used to encrypt the important information of an image[21]. It has been demonstrated in[20–25] that the significant data lie in the lower frequency bands (LL1), while the remaining sub-bands contain the edge information.

Yekkala et al.[26] utilized Discrete Cosine Transform (DCT) transform and adaptable lightweight encryption procedure to encode chosen blocks that contain edges. The concept behind their selection methodology is to encode chose an area with important data by using the threshold value in individual rage, while other areas are unencrypted. Notwithstanding, by their methodology the processing time is insignificantly decreased because of the large encrypted areas. Additionally Munir[27] used DCT for deciding encrypted area after convert RGB color space to HSV, and the choice block is encrypted by means of scrambling content via cat map method.

In[28] three levels of shuffle on region blocks and coefficients of Orthogonal Polynomials Transform (OPT) domain are explained. The image is rearranged three times for each region block after partitioning the image into non-overlap blocks of 4x4 pixels, after that the blocks are mixed three times. The Zigzag sequence method is applied for every low OPT coefficients block of the image after implementation OPT for all image blocks. The blocks to be rearranged are chosen by pseudo-random sequence produced utilizing the seed sub key. At last, the blocks are split into sub-blocks and rearranged therefore; the protection is much harder to break via the intruder. The less complexity of this work is based on advantage of OPT. The OPT is known to have utilized 25% of the entire image for encryption, which is an indication that the encrypted region is independent of the unencrypted region. A summarized discussion on the several block selection techniques can be seen in Table 1.

3.1.2 Pixel Selection

The pixel selection strategy is one of the strategies that mostly adopt the selective image encryption strategy. Selecting pixels is one of the useful strategies that can be executed at all image pixels. Hence, it is reliant on the particular criteria designed to be accomplished for the segmented regions such as, edge sharping or pixel brightness. In[29] Rao et al, an image is isolated into two parts based on correlated and uncorrelated information via splitting each 8 bits of each pixel into initial four MSB (Most Significant Bit) planes and last four LSB (Least Significant Bit) planes. After that, a pseudo random arrangement of the uncorrelated information is utilized to protect the correlated information while keeping the rest information is unencrypted. Subsequently, the joint between correlated and uncorrelated information is utilized to get the last cipher image. The remarkable limitations of pixel selection are that the encrypted image usually appear noisy, thereby, the risk of perceptibility of an encrypted region becomes highly likely. More so, there is the issue of computational unpredictability.

As indicated by Droogenbroeck in[30], a visual debasement of the image can be fulfilled if the encryption is in any event between 4 to 5 Least Significant bits (LSB) planes. Therefore, the selective image encryption is proposed in this work for uncompressed and compressed images using 50%-60% rates of encrypted area. These rates have been indicated in their work to add to quickness and convenient encryption. In[31], Ou Y et al. proposed the region of interest encryption technique for medical image. Firstly, the wavelet transform is utilized

Table 1. Block selection techniques

Ref./Year	Methodology	Remarks
[18] 2013	Three phases Part1: detected significant parts using Prewitt edge detector Part2: encrypt significant part in spatial domain using Arnold cat map and Logistic map Part3: insignificant part is encrypt using Discrete Wavelet Transform (DWT)	Encrypted algorithm is very fast Good ability to resist differential attack Very little similarity between encrypted and original images High security level with large key space size. Difficult for intruder to retrieve the original image without knowing the key. ROI selection is not significant.
[20] 2013	Two phases Part1: selective sensitive block using edge detector Part2 encrypted sensitive block in sequences methods(Blowfish, AES, RC6,Serpent)	Encrypted algorithm is very fast and simple No similarity between encrypted and original image Small data leak ROI is the busy region, but not the correct significant region.
[22] 2009	method1: Three phases Part1: 3-DWT Part2: wavelet filter (Haar filter) to select sensitive information Part3: Stream Cipher method2: Three phases Part1: 3-DWT Part2: wavelet filter (Haar filter) to select sensitive information Part3: AES-PE for encryption	Stream algorithm has low security with relatively small key space size, while AES algorithm has high security level with large key space size The algorithm works well to protect image Little similarity between encrypted and original image, while AES algorithm get very little similarity between them. Encryption is very fast because relatively small area of encrypted image AES takes more time in encryption compared with stream-PE, for that reason stream is faster than AES Selective region is very small.
[26] 2007	Three phases part1: apply DCT domain for image part2: detecting blocks containing edge using threshold value	Encrypted speed is medium with large rate of encrypted area. It's difficult to retrieve the original image without having key.
[27] 2012	Three phases Part1:image is represent in HVS color space for transparency Part2: DCT is apply to detect low frequency Part3: permute only low frequency sub band using Arnold cat map	Decrypted image has medium quality The encryption algorithm is robust against noise.
[28] 2008	Two phases Part1: OPT domain is used Part2:scrambling using bit scrambling, shuffling of block coefficient and block shuffling based on orthogonal polynomial Transformation	Encrypted speed is fast Good ability to resist different attacks Large key space and highly sensitive to small changes Very little similarity between encrypted and original images Small rate of encrypted area Security on average level with low sensitivity for changing in encrypted image

in the region of interest of the original image. After that, the MSBs coefficients are encrypted via the AES in CFB (Cipher Feedback Block) mode. But, this technique gives low security because of the way that their strategy uses scrambles just a little area of 1.258%.

Zhang et al.[32] proposed selective a feature of interest based on an interested features. These features are based on the correlation among bit planes and the characteristic of bit information. Due to the superior characteristics of bit-level operations and the intrinsic bit features of the image confusion and diffusion stage. An expand-and-shrink strategy is implemented to shuffle the image based on the features selection. The results show that the proposed scheme leads to a higher security level with high

entropy of cipher image. Moreover, it is fast. But, still the selection of bit plants is based on testing several rounds.

Panduranga et al.[17] suggested selective image encryption methodology based on the map image. The image is separated into non-overlap blocks. The input image map is used for encrypting the chosen block. This methodology is extremely appropriate for unique applications, for example, medical and satellite images and it is most helpful when the region of interest is known. A summarized discussion on the several pixel selection techniques can be seen in Table 2.

3.2 Image Encryption Techniques

The Image encryption technique has been distinguished in a number of works spanning the spatial, frequency and the hybrid domain techniques. The following subsections describe most selective image encryption techniques for each domain, then Table 3, summarized discussion on the encryption schemes for each domain.

3.2.1 Spatial Domain

As indicated by Oh et al.[33] the AES algorithm was applied based on five principles; input image, partitioning size, iteration selection, programming usage improvement, and entire routine determination procedure. These criteria form is called Selective Encryption Algorithm (SEA) used for enhancing the AES algorithm via reduces the computation process by 50% with reducing the encrypted area for 35%. Thus, in view of these qualities, it can be reasoned that security level is of normal level. A multi-level ROI image encryption general construction modeling is proposed in[34] for biometric information. In their work, the multiple regions and RC4 were utilized to protect an uncompressed image. The main concept behind their system is that for an approved observer, just part of the image can be seen. Generally, just an approved individual can see the substance of the protected image; however this is fundamentally for the biometric framework. Preceding these, different ROIs are chosen for every image, which are then protected at three levels of authority utilizing RC4 and fingerprint methods.

Kumar[35] improved the RC4 algorithm and actualized it with the partial image encryption for expanded security of the RC4 against attacks. The partial image encryption system is received from two points of view: 1) for the locate region of interest, and 2) for encoding the close areas of the image. The reachable result of this approach is less security and less time about 210s via encrypted 8.192% area. Because of the little encrypted area, the security may be traded off. Brahimi et al.[36] suggested a new modern encryption method of JPEG2000, which scrambles just the code-pieces relating to some delicate territory. The modification of block code picked at the chose region is utilized to improve the security. AES symmetric encryption is utilized with CFB mode to scramble the traded code blocks. The encrypted area is reduced via shuffling and partial image encryption. The encryption proposed by[36] works with any standard encryption algorithms and requires less complexity. Case in point, while he encrypted data about 11.64% of the image, therefore less computational time is accomplished.

3.2.2 Frequency Domain

In Kulkarni et al.[37], a modern protection technique was proposed. The determination phase uses five levels of wavelet change with a specific end goal to decompose the image data by means of applying the wavelet channel. To organize the image in hierarchal structure, the low and high pass band filters are utilized so that every structure is about distinctive meaning. According to Human Visual System (HVS), the corrupted form of the input image of the proposed strategy gives an adequate level of sensitivity.. This strategy chooses the high relationship coefficient of five level sub-bands to control security and sensitiveness.

Younis[38] proposed an encryption system that is included wavelet packet transform, quantization by C-mean fuzzy, randomization image and arithmetic operation coding to two sub-band of the input image. The CMF accomplishes clustering investigation with the randomization cipher for the two level sub bans. The system in[38] has ability for protecting just 6.25%-25% of the image, which reduce the computational process to get fast process of encryption and decryption and high safety. Richard et al.[39] proposed a new partial image encryption strategy. In this strategy the block of DCT coefficient of the original image is shuffling. To separate image regions, an edge identification technique utilized. At that point, the noise is reduced via implementing the median filter to the encrypted image. Additionally, for the encryption to be accomplished, the properties of vitality compaction of a shape versatile cosine transform are connected in the DCT domain. From the work in[39], it is accounted for that just a 10% of the original image is protected and the security level is enhanced.

Table 2. Pixel selection techniques

Ref./ Year	Methodology	Remarks
[29] 2006	Two phases Part1: divided image into correlated an uncorrelated data by separating 4 MSB planes and four LSB Part2: encrypt correlated data using highly uncorrelated pseudo random sequence	Encryption speed is slow High level of security with 4 MSB plants is encrypting.
[30] 2011	Three phases Part1: select sensitive information from image Part2: Mixing image data and XOR function Part3: Least Significant bit used for encryption	Encrypted image is slow because more than half image is encrypted It is not robust against cryptanalysis attack Very high security level.
[31] 2007	Method1: Two phases Part1: five-level DWT used detecting ROI Part2:randomly inverse the first two MSBs of ROI using bit flipping Method2: Two phases Part1: five-level DWT used detecting ROI Part2:AES in CFB mode for encrypt the region	Encrypted speed is very fast with relatively small rate of encrypted area Low security with relatively small key space size method1) this method modifies few bits of each region while, method2) make use of AES with Cipher Feed Back (CFB) mode which satisfies the requirement for encryption of arbitrary data size method2) detected and encrypted only one region in each block Difficult for intruder to retrieve the original image without knowing the key.
[32] 2013	Two phases Part1: select interested feature based on pixel correlation and bit plant. Part2: shuffling interested area using expand-and-shrink strategy.	Encrypted speed is very fast. Security is high The map is not safety in transformation. Secret key is very large and not safety.
[17] 2013	Two phases Part1: select sensitive information using mapping image Part2: Encrypt selected-blocks using chaos map	Detected and encrypted multi regions This method is very useful when the area or region of interest is known. The map is not safety in transformation

Sasidharan et al.[40] suggested a quick selective image cipher strategy utilizing an RC4 algorithm and Discrete Wavelet Transform (DWT). In their suggested strategy, the protection is completed at the most reduced band utilizing the stream cipher. As per Sasidharan, the essential thought of the stream cipher to hold all the image data. Nevertheless, utilizing the stream cipher expends additional time since it ordinarily protects one byte at once. The bitwise XOR-operation is utilized to consolidate between key stream and input image, while the stream cipher is created haphazardly. Finally, the edges in the image are rearranging. It is seen from[40] that the encryption strategy utilized can decrease the encryption time following just the most minimal band of the image is protected. Likewise, a high security performance is accomplished through the rearranging procedure, which rearranges the unencrypted areas with the encrypted areas via the rearranging algorithm.

In[41] developed an optimum modern image cipher technique utilizing high vitality coefficients of the transformed image, which were chosen by utilizing the Particle Swarm Optimization (PSO) system in the daubechies domain for protection. The protected area of the image is 33% of the original image; this rate demonstrates that the protection process is very fast. In[27], an encryption strategy that applies the chaotic map method on alow sub-band of the DCT transformed image is proposed. The core concept of utilized the low sub-band of the DCT transform image is that HVS color space is more drawn to data at the lower frequencies than the high frequency data. Moreover, just curves, lines, etc. in the low sub-bands of DCT coefficients are ciphered because it include the significant data of an image.

Rodrigues et al.[42] proposed a method based on AES stream encryption utilizing Variable Length Coding (VLC) of the Huffman's vector. The image data is isolated

Table 3. Image encryption techniques

DOMAIN	Ref./ Year	Methodology	Remarks
Spatial Domain	[33] 2010	Two phases Part1: selective function Part2: AES for selected part	Encryption speed is medium with more than 35% of image is encrypted Security on the average level with this rate of encrypted area and large key space
	[34] 2007	Two phases Part1: detecting Multi ROI Part2:RC4 stream cipher for each region	High security level with large key space size and multi regions can Encryption speed is medium when multi regions are encrypted.
	[35] 2012	Two phases Part1: select sensitive information Part2: encrypt selected part using RC4	Encrypted image is very fast Low security with relatively small encrypted data
	[36] 2008	Three phases Part1: Div. Image to Blocks Part2: Permutation of blocks Part3:Encrypt block using AES in CFB mode	Encrypted speed is fast with small rate of encrypted area Secure against brute force attacks Security on the average level because the small encrypted area of image
Frequency Domain	[37] 2008	Four phases Part1: five level wavelet decomposition Part2 hierarchal structure is create with high and low pass band Part2: HVS is used for transparency Part3:Logistic map is used to shuffling table Part4:Bit shuffle and sign is used for encryption	High security level and very difficult for intruder to retrieve the original image without having the key
	[38] 2009	Three phases part1: Wavelet packet transform part2: quantization by Fuzzy C-MEAN (FCM) part3: Permutation cipher and arithmetic coding apply for 2D level of sub band.	Encryption speed is very fast with relatively small rate of encrypted area Difficult to retrieve the original image without knowing the key Security is on the average level If number of cluster increased, the encrypted speed will be slower and quality of decrypted image will be higher.
	[39] 2010	Two phases Part1: multi region differentiate using edge detection Part2:matrix multiplication with a key matrix for encrypt regions	Encrypted algorithm is very slow High key space with high sensitivity to small change on key Low security with relatively small encrypted data
	[40] 2011	Four phases Part1: DWT is apply on image Part2: RC4 Stream is used to encrypt lower frequency band Part3: key is combined with encrypted image using XOR Operation Part4: Shuffling encrypted image is used when many edge is found on an image	Secure against statistical attacks Many attackers can threat secret key. Large key space with high security level Encrypted image has very high quality.
	[41] 2012	Three phases Part1: Daubechies4 domain is apply on image Part2: PSO is used to select high coefficient Part3:IQIM is used for encryption	Encryption speed is medium because encrypted area is small Good ability to resist differential attack. High key space with high sensitivity to small change on key Security on average level with this rate of encrypted area

	[27] 2012	Three phases Part1:image is represent in HVS color space for transparency Part2: DCT is apply to detect low frequency Part3: permute only low frequency sub band using Arnold cat map	Decrypted image has medium quality The encryption algorithm is robust against noise.
	[42] 2006	Three phases Part1: applying DCT on image Part2:quantization using scan method with VLC of Huffman's vector Part3: AES in CFB mode is applied for the new sequence.	Encrypted algorithm is very fast. Large key space size. Security on the average level with small rate of encrypted area Easy for intruder to retrieve the original image without knowing the key.
Hybrid Domain	[43] 2011	Three phases Part1: detected significant parts utilizing Prewitt edge detector Part2: protect significant region in spatial domain utilizing cat and logistic maps. Part3: insignificant region is cipheed using Discrete Wavelet Transform (DWT)	Very Fast Encryption algorithm. Good ability to resist differential attack. Very little similarity between encrypted and original images High security level with large key space size Difficult for intruder to retrieve the original image without knowing the key.
	[44] 2015	Four phases Part1: detected sensitive parts using rough and smooth criteria. Part2: encrypt high sensitivity part in spatial domain using Piecewise map and logistic map. Part3: medium sensitivity part is encrypting using Discrete Wavelet Transform (DWT). Part4: low sensitivity part is shuffled the content pixels using Arnold Cat map.	Good ability to resist differential attack High security level with large key space size Difficult for intruder to retrieve the original image without knowing the key. Small encrypted data with high security level.
	[45] 2013	Two phases Part1: Phase manipulations in Fourier transform. Part2: Sign encryption is used to modify image	More threat prone Easy for intruder to retrieve the original image without knowing the key. Low security level

into non-overlap blocks of 8x8 pixels. After that, every block is changed from the spatial domain to the frequency domain utilizing Discrete Cosine Transform (DCT). Then, the quantization is implemented to the previous step result using scan method, while final step based on implementing the AES stream encryption strategy. The benefits saw of this method is that there is the likelihood of recognizing maybe a couple regions for every block of 8x8.

3.2.3 Hybrid Domain

The famous literary works that investigated the benefits of consolidating the spatial and frequency domain for successful encryption method is Taneja N et al.[43]. In their work the fractional wavelet was utilized to encode just important blocks utilizing Arnold cat map and logistic map. Firstly, the significant region in the spatial domain is encrypted while the low sub-band of insignificant regions is encrypted. The significant region is determined via the Prewitt edge detector for extracting the edges of the image. As reported in[43], a PSNR estimation of 9.3008dB is accomplished, which is a sign that the procedure guarantees better detectable quality and cryptography because of the simple processing to encode the image. From the result, it can be concluded that since encryption in the hybrid domain is independent of the original image, the encrypted region is difficult to alter.

In[44], Jawad and Sulong proposed 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 achaotic map approach which automatically generates secret key. The criteria of select and determine the ROI for color image encryption is based on a new texture features

that identify the correct ROI. Based on multi-threshold value selection, the new classification of ROI is developed via classifying regions into three parts: low, medium and high sensitivity regions. The piecewise and logistic maps are used for encrypting regions in hybrid domain. While, the automatic secret keys are generated based on combination of chaotic map methods. The result, achieved best encrypted area with suitable security performances.

In[45] Parameshachari et al. proposed an idea that joins stage operation and sign encryption as a partial image encryption framework. The encryption approach comprises of multi phases: in the first phase, the process and size of the original image are specified utilizing the Fast Fourier Transform (FFT). After that, the first part of the image is consolidated with the subsequent yield of applying Inverse Fast Fourier Transform (IFFT) keeping in mind the end goal to acquire the balanced variant of the image. For the second stage, the sign encryption technique is used for encrypting the modified image. This sign encryption is gotten by splitting the sign bits of the resulted image in the partially protected image. It could be concluded that the proposed strategy is quick, but might result in low security of the encrypted data.

3.3 Key Management

Key management is highly important in for the fact that an encryption algorithm must be sensitive to the cipher keys, and the key space must be large enough to protect against all attacks, like for instance the brute-force attack[46,47].

Chaotic map is the major source for generating the secret keys. It is based on varying parameters and it is widely used in image encryption. However, most existing chaotic encryption techniques still suffer from major problems such as small key space, slow speed, and weak security[48]. Many researchers are applying chaotic map in selective image encryption, for example, logistic map, Arnold cat map, Lorenzo map and hyper map[49,50]. Likewise, the classical encryption algorithms like Blowfish and AES are still on enhancements in present literatures[51]. The purpose is to enhance security performance of these algorithms by increase in key space size and devising new and fast way for generating secret key.

4. Remaining Issues

Having presented a survey on the various selective encryption methods, here, a discussion on the limitations of the various methods are summarized in such a way that buttresses the inferences drawn in the course of the paper.

In a number of literatures, an approach commonly practiced is the use of partitioning techniques in addressing security requirements for selective encryption. However, it is still with respect to image partitioning, without consideration for the security requirements of selective encryption. Therefore, image partitioning in selective encryption is still a big challenge since the size of the image partitioned can invariably affect security. In this regards, there is still room for further improvement. While selective image encryption offers many advantages over the network transform, it still contends with security since only portions of an image gets adequate security. On decryption, a big gap in selective image encryption is on how to characterize an image into regions so that the encrypted and the non-encrypted information are appropriately identified and displayed. With the use of symmetric block cipher with traditional encryption algorithms, there is a need to enforce security so as to meet the security demands of selective image encryption. Finally, the size of the key space is an important factor in obtaining high security level for any encryption algorithm. Based on the survey of the literatures made so far, a large key space might increase the security level of protection algorithms.

5. Conclusion

In this paper, we reviewed an extensive variety of literary works on selective image encryption with discussions on the difficulties of the various famous strategies, which were talked about three categories: selection region of interest, selective image encryption algorithms, and key managements. From this survey based on these categories, it can be derived the main challenge of the selective image encryption strategies that use less space for encryption but still security is low. There is a more guarantee of security for full encryption than for encryption at certain regions. Therefore, with consideration of the security problem of selective encryption, one can devise means of addressing its limitations. For instance, since colored images are better off for region segmentation, it can be used to determine the best Region of Interest (ROI), which is a viable option for addressing the security challenges of selective encryption.

6. Acknowledgment

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

7. References

1. Kaur R, Singh EK. Image encryption techniques: A selected review. Journal of Computer Engineering. 2013; 9(6):80–83.
2. Ramesh G, Thambiraja E, Umarani DR. A survey on various most common encryption techniques. International Journal of Advanced Research in Computer Science and Software Engineering. 2012; 2(7):226–33.
3. Rajanbabu DT, Raj C. Multi level encryption and decryption tool for secure administrator login over the network. Indian Journal of Science and Technology. 2014; 7(4):8–14.
4. Parameshachari BD, Panduranga HT, Soyjaudah KS. A overview on partial image encryption approaches. International Journal of Engineering Research and Development. 2012; 1(2):49–54.
5. Bhatt V, Chandel GS. Implementation of new advance image encryption algorithm to enhance security of multimedia component. International Journal of Advanced Technology and Engineering Research. 2012 Jul; 2(4):13–20.
6. Parameshachari BD, Soyjaudah KS, Chaitanyakumar MV. A study on different techniques for security of an image. International Journal of Recent Technology and Engineering. 2013; 1(6):14–9.
7. Srinivasan B, Arunkumar S, Rajesh K. A novel approach for color image, steganography using NUBASI and randomized, secret sharing algorithm. Indian Journal of Science and Technology. 2015; 8(S7):228–35.
8. Paar C, Pelz lJ. Introduction to cryptography and data security. Understanding Cryptography. 2010:1–27.
9. Apoorva KY. Comparative study of different symmetric key cryptography algorithms. International Journal of Application or Innovation in Engineering and Management. 2013; 2(7):204–6.
10. Singhal N, Raina JPS. Comparative analysis of AES and RC4 algorithms for better utilization. International Journal of Computer Trends and Technology. 2011; 2(6):177–81.
11. Vijayaraghavan R, Sathya S, Raajan NR. Security for an image using bit-slice rotation method-image encryption. Indian Journal of Science and Technology. 2014; 7(4):1–7.
12. Rehman A, Liao X, Kulsoom A, Abbas SA. Selective encryption for gray images based on chaos and DNA complementary rules. Multimedia Tools and Applications. 2015; 74(13):4655–77.
13. Jawad LM, Sulong G. Chaotic map-embedded Blowfish algorithm for security enhancement of colour image encryption. Nonlinear Dynamics. 2015; 81(4):2079–93.
14. Bhatnagar G, Jonathan Wu QM. Selective image encryption based on pixels of interest and singular value decomposition. Digital signal processing. 2012; 22(4):648–63.
15. Puech W, Bors AG, Rodrigues JM. Protection of color images by selective encryption. In: Fernandez-MaloigneC, editor. Advanced Color Image Processing and Analysis. New York: Springer-Verlag; 2013.
16. Suresh V, Madhavan CV. Image encryption with space-filling curves. Defence Science Journal. 2012; 62(1):46–50.
17. Panduranga HT, Naveenkumar SK. Selective image encryption for medical and satellite images. International Journal of Engineering and Technology. 2013; 5(1):115–21.
18. Jalesh K, Nirmala S. A hybrid approach for enhancing the security of information content of an image. In: Swamy PP, Guru DS, editors. Multimedia Engineering Processing, Communication and Computing Applications. Indian: Springer; 2013.
19. Shekhar S, Srivastava H, Dutta MK. An efficient adaptive encryption algorithm for digital images. International Journal of Computer and Electrical Engineering. 2012; 4(3):380–3.
20. Rad RM, Attar A, Atani RE. A comprehensive layer based encryption method for visual data. International Journal of Signal Processing, Image Processing and Pattern Recognition. 2013; 6(1):37–48.
21. Jain A, Ahmad M, Khare V. A ridgelet based symmetric multiple image encryption in wavelet domain using chaotic key image. 2012 International Conference on Ecofriendly computing and Communication Systems (ICECCS); 2012. p. 135–44.
22. Flayh NA, Parveen R, Ahson SI. Wavelet based partial image encryption. Multimedia, Signal Processing and Communication Technologies. 2009:32–5.
23. Yu Z, Zhe Z, Haibing Y, Wenjie P, Yunpeng Z. A chaos-based image encryption algorithm using wavelet transform. 2010 2nd International conference Advanced ComputerControl (ICACC); 2010. p. 217–22.
24. Vilardy JM, Useche J, Torres CO, Mattos L. Image encryption using the fractional wavelet transform. Journal of Physics: Conference Series. 2010; 274(1):12–47.
25. Pande A,Zambreno J. The secure wavelet transform. Journal of real-time image processing. 2012; 7(2):131–42.
26. Yekkala AK,Udupa N, Bussa N, Madhavan CEV. Lightweight encryption for images. Digest of Technical Papers International Conference on Consumer Electronics, ICCE'07; 2007. p. 1–2.
27. Munir R. Robustness analysis of selective image encryption algorithm based on arnold cat map permutation.

Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics; 2012. p. 1–5.
28. Krishnamoorthi R, Malarchelvi PDSK. Selective combinational encryption of gray scale images using orthogonal polynomials based transformation. International Journal of Computer Science and Network Security. 2008; 8(5):195–204.
29. Rao YVS, Mitra A, Prasanna SRM. A partial image encryption method with pseudo random sequences. In Information Systems Security. 2006; 4332:315–25.
30. Steffi MAA, Sharma D. Comparative study of partial encryption of images and video. International Journal of Modern Engineering Research. 2011; 1(1):179–85.
31. Ou Y, Sur C, Rhee KH. Region-based selective encryption for medical imaging. Frontiers in Algorithms.2007; 4613:62–73.
32. Zhang W, Wong K-W, Yu H, Zhu Z-L. A symmetric color image encryption algorithm using the intrinsic features of bit distributions. Communications in Nonlinear Science and Numerical.2013; 18(3):584–600.
33. Oh JY, Yang DI, Chon KH. A selective encryption algorithm based on AES for medical information. Healthcare informatics research. 2010; 16(1):22–9.
34. Wong A, Bishop W. Backwards compatible, multi-level region-of-interest (ROI) image encryption architecture with biometric authentication. International Conference on Signal Processing and Multimedia Applications; 2007. p. 324–9.
35. Kumar P. RC4 enrichment algorithm approach for selective image encryption. International Journal of Computer Science and Communication Networks. 2012; 13(4):95–9.
36. Brahimi Z, Bessalah H, Tarabet A, Kholladi MK. A new selective encryption technique of JPEG2000 codestream for medical images transmission. 5th International Multi-Conference on Systems, Signals and Devices, IEE SSD'08; 2008. p. 1–4.
37. Kulkarni NS, Raman B, Gupta I. Selective encryption of multimedia images. 32th National Systems Conference; 2008. p. 467–70.
38. Younis HA, Abdalla TY, Abdalla AY. Vector quantization techniques for partial encryption of wavelet-based compressed digital images. Iraq Journal of Electrical and Electronic Engineering. 2009; 5(1):74–89.
39. Richard ELM, Agaian SS. Selective region encryption using a fast shape adaptive transform. Proc. 2010 IEEE International Conference on System Man and Cybernetics; 2010. p. 1763–70.
40. Sasidharan S, Philip DS, A fast partial encryption scheme with wavelet transform and RC4. International Journal of Advances in Engineering and Technology. 2011; 1(4):322–31.
41. Kuppusamy K, Thamodaran K. Optimized partial image encryption scheme using PSO. 2010 International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME); 2012. p. 236–41.
42. Rodrigues JM, Puech W, Bors AG. A Selective encryption for heterogeneous color JPEG images based on VLC and AES stream cipher. Proc. European Conference on Color in Graphics, Imaging and Vision (CGIV'06); 2006. p. 34–9.
43. Taneja N, Rama B,Gupta I. Combinational domain encryption for still visual data. Multimedia tools and applications. 2011; 59(3):775–93.
44. Jawad LM, Sulong G. Classification of novel selected region of interest for color image encryption. Research Journal of Applied Sciences, Engineering and Technology. 2015; 9(11):969–81.
45. Parameshachar PBD, Soyjaudah KM, Devi KAS. Secure transmission of an image using partial encryption based algorithm. International Journal of Computer Applications. 2013; 63(16):33–6.
46. Chattopadhyay D, Mandal MK, Nandi D. Symmetric key chaotic image encryption using circle map. Indian Journal of Science and Technology. 2011; 4(5):593–9.
47. Ramalingam M, Mat Isa N. A steganography approach over video images to improve security. Indian Journal of Science and Technology, 2015; 8(1):79–86.
48. Tamilselvi R, Ravindran G. Image encryption using pseudo random bit generator based on logistic maps with radon transform. Indian Journal of Science and Technology. 2015; 8(11):1–7.
49. Kaur R, Singh EK. Comparative analysis and implementation of image encryption algorithms. International Journal of Computer Science and Mobile Computing. 2013; 2(4):170–6.
50. Huang CW, Yen CL, Chiang CH, Chang KH, Chang CJ. The five modes AES applications in sounds and images. 2010 6th International Conference on Information Assurance and Security; 2010 .p. 28–31.
51. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015; 8(3):216–21.