A REVIEW OF COLOR IMAGE ENCRYPTION TECHNIQUES

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

**[1] Faculty of Computing, University Teknologi Malaysia (UTM)
Skudai, Johor Bahru, Malaysia**

**[2] Network Engineering Department, Collage of Information Engineering, The University of Al-Nahrain
Baghdad, Iraq**

Abstract

Image encryption plays an important role to ensure confidential transmission and storage of image over internet. However, a real–time image encryption faces a greater challenge due to large amount of data involved. This paper presents a review on image encryption techniques of both full encryption and partial encryption schemes in spatial, frequency and hybrid domains.

Keywords: *Image Encryption, Full Encryption, Partial Encryption, Spatial Domain Image Encryption, Frequency Domain Image Encryption, Hybrid Domain Image Encryption.*

1. Introduction

The current world depends totally on communication and information technology. As a result of the rapid growth in communication technology, there is a great demand for internet for exchanging the information and there is a requirement to provide security for all this information [1]. Images are the highest percentage of multimedia data. Digital color images are being transferred and stored in great amounts through the internet and extensively used in different applications including legal, military and medical [2].

A digital image can be seen as a two dimensional rectangle array. The elements of this array are referred to as pixels. Every pixel carries an intensity value and a location address. Therefore, it is essential to verify integrity, confidentiality and authenticity of the transmitted digital images [3]. One of the significant known solutions that had been offered in modern years to secure data against unauthorized access or hackers is encryption [4]. The procedure of encryption converts plain-data into cipher-data through a finite set of instruction named an algorithm with one or more keys. The algorithms that use similar secret keys for encryption and decryption are classified under private key encryption, whereas asymmetric key encryption uses two dissimilar keys; private key for decryption and public key for encryption [5][6][7].

Image encryption algorithms attempt to convert original images to other images that are difficult to understand in order to keep the image confidentiality between users. In other words, it is important that without a key for decryption, nobody could get to know the content [2]. Majority of traditional algorithms are basically used for encryption of text data; however they do not fit for the multimedia data particularly images due to their huge size. Furthermore, decrypted text result should be similar to the original text, while decrypted image is not required to be similar with original image [6, 7].

Image encryption algorithms can be categorized into full encryption and partial encryption (also called selective encryption) based on the sum of encrypted data. According to the percentage of the encrypted data, unfortunately, the time for processing of encryption and decryption is the main concern in real-time image communication. Time can be categorized into two levels, one for encryption time and another for time for transferring images. The first step is to choose a robust, fast and easy method to implement in order to reduce the time. Encryption and decryption algorithms are not fast enough to deal with the enormous amount of transmitted data. A significant criteria relating to the method is to decrease the image encryption size and maintain quality of the image. Partial Encryption is a suitable method to encrypt only the lowest portion of data to lessen the computational requirements of enormous amounts of multimedia data [8]. It is essential to lessen the images encryption time in distributed network by minimizing the sum of data to encrypt and attaining a reasonable security and minimizing the computation [9]. The implementation of partial encryption just started in 1990's.

On the other hand, the traditional full encryption algorithms are used to completely encrypt an image and treat all bits similarly; it has greater computational complexity than partial encryption. Furthermore, it takes more time in comparison with partial encryption. Therefore, multimedia data needs either a full or selective encryption according to requirements of the application. For instance, applications of military and law enforcement need full encryption. Nevertheless, there is a range of

spectrum applications that require lower security levels, as in medical images that are attained by partial encryption [10].

In the subsequent sections, a detailed discussion on different encryption schemes is presented with particular emphasis on how the encryption schemes ensure that vital information in the image encrypted is retained. Generally, encryption schemes are of two categories, 1) the full encryption scheme, and 2) the partial encryption schemes. These schemes differ, based on the percentage of the encrypted data and are either of the spatial domain, frequency domain or the hybrid domain.

Typically, an image can be said to consist of different regions of varying significance that can be explained by using partial encryption approaches. However, the partial encryption technique requires that similar levels of security are assigned on each feature, which incurs increased computational complexity [40]. In view of this, we limit our discussions on the encryption techniques with respect to consideration for the significances of image features in both categories of encryption.

2. Full Encryption

Information confidentiality is a vital aspect of image encryption. The confidentiality of the encrypted data with a balance in time and cost efficiency of the encryption technique is the challenge still faced in image encryption. This challenge has been identified in a number of literatures ([11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28]) spanning the spatial, frequency and the hybrid domain techniques in full encryption schemes. In subsequent sections, we will emphasize on the techniques in these literatures on the basis of the domains of implementation and the encryption approaches such as block cipher and stream cipher approaches, used in addressing the challenge.

2.1 Spatial Domain

The stream cipher approach has been utilized in a number of literatures, some of which we will be discussing in this subsection. Nien et al. [11] used a hybrid encryption technique for the color image based on the multi-chaotic system. They merged the Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR) methods. First, the PCS, a fast encryption method that can vary the positions of each pixel, is applied to fully eliminate the original image outlines using four third-order chaos's such as Henon, Lorenz, Chua and Rössler chaos maps. Second, the BCR, which uses chaos system to make chaotic codes rearrangement in pixels, are applied. The combination of the PCR and the BCR increases the key space of images to 10180 and completely eradicates the outlines of the encrypted images, blurs the distribution characteristics of RGB-level matrices, and effectively protects against the decryption of exhaustive attack when correlation coefficient is as little as 0.0031.

Rhouma et al. [12] proposed a piecewise linear chaotic map (PWLCM) to build a new digital chaotic cryptosystem. The characteristics of PWLCM are very suitable for the design of encryption schemes. This method transformed the color image into three vectors then mapping the integer values of them into the phase space of the skew tent map. When, the phase space of the skew tent map is divided into 256 equal-width subintervals. The accuracy, efficiency and security of the proposed encryption scheme are thoroughly analyzed and its adequacy for image encryption is proven. The key space is 1093, which is relatively small key space size, but it's resistance against brute force attack is evident because of high values of NPCR and UACI achieved. Furthermore the entropy is 7.9551 that indicates only small amount of data loss.

In Musheer et al. [13] proposed encryption algorithm that exploits three diverse chaotic maps. First, they partitioned the image into blocks of 8x8 pixels, all blocks is shuffled using cat map. Second, the cat map is applied again to distribute all the blocks. Third, a shuffling is made again using the cat map, but this time, it is the final image pixels. Then the final image is encrypted using 1D logistic map. Their experimental result revealed that the technique required great key space, which is about 10112, and are of high sensitivity to minor changes in secret keys. The correlation between the encrypted image and the original image is about 0.0095, which shows that the encrypted image is independent of the original image. The encrypted image entropy reported is of maximum value 7.9992 that indicates only tiny amount of data loss.

In similar manner Wei et al. [14] approached image encryption from the perspective of [13], but differed by the 4D hyper chaos used. They generated four chaotic sequences from 4D hyper chaos. Then encryption is carried out on each R, G, and B color channels of the image based on the first three sequences with inter-cross cipher-block chaining mode. The encrypted image is then shuffled via each three color channels. After numerous rounds of encryption, the cipher image is attained. From [14], it is evident that correlation coefficients of the encrypted image are significantly reduced and is also worth pointing out that a small change in secret key can result in a completely different decrypted image.

Kamali et al. [15] developed an encryption scheme that is a modification of advanced encryption standard (AES), which is a well-known block cipher technique in data encryption. The modification is accomplished by using Shift and Row Transformations: if the values of first row and column are even, the first and forth rows are unchanged, then each byte in the second and third rows is shifted to the right, cyclically. On the other hand, if the first and third rows are unchanged, each byte of the second and fourth rows is shifted to the left. The technique shows strong performance against statistical attacks. However, security can be compromised when entropy reaches its maximum value. The key space used is 2128, while the encryption time is 8.565ms, which shows that the algorithm is fast and sensitive to even small changes.

Z. Aihong et al. [16] proposed a protective transmission of RGB color image based on Logistic map and LSB hiding algorithm. First of all, Logistic map used three chaotic sequences and the R, G and B matrices were permuted by the chaotic sequences. Finally, the LSB hiding algorithm is used to embed encrypted image in the carrier image via transmission. This method has high security, fast operation speed with fewer secret key for any color image. It's suitable for the large color image security transmission over a network.

In [17] a color image encryption method that applies logistic chaotic map in two iterative steps was proposed. For the first step, the logistic map is used to permute pixels of the original image. For the second step, the logistic map is used in the diffusion process. According to the performance analysis reported in [17], it can be concluded that the technique satisfied high security level requirements which acceptable encryption speed for variable size of image. Apparently, it is also observed that encryption quality was attained with relatively small key space. More also it's observed that the original image is independent of the encrypted image with high safety for different attacks due to the minimum correlation value of 0.0013 attained.

Mastan et al. [18] proposed a nonlinear color image encryption technique that comprised matrix transformations such as pixel diffusion and permutation. The technique firstly applies diffusion independently for each channel of color image using both single pixel and block pixel diffusions. Then the permutation between three channels R, G, and B is applied interdependently between pixels. This technique is specifically designed for sensitive fields such as medicine where misinterpretation could result in loss of life. It's faster than AES and can be used in real time secure image transmission. It has very large key space which is about 3.887X1053, and it resists against a brute force attack. However, this algorithm takes longer time for encryption.

In [19] proposed a new lossless image encryption algorithm that is based on pixel substitution, which divides the image into blocks of color components. The color component in each block of the color images is then modified by exclusive-OR operation. The algorithm is simple, fast, but sensitive to the secret key, due to the key space of 2120 that it uses, which makes their technique more appropriate for storing/transmitting images of high security requirement.

An approach to image encryption that is based on sifting rows and columns of image was proposed by Abugharsa et al. [20] . Using a shifting table that is generated by hash function, the original image is divided into block of 3 x 3 pixels. Then the blocks are further shifted through rows and columns before encrypting. We observe from [20] that there is a close relationship between the original image and the encrypted image, which is confirmed by the correlation value (-0.0078) obtained. This implies that the neighborhood pixels in the original image have nearest value than the neighborhood pixels of the encrypted image, which is a good indication that predictability is low. However, due to the high entropy value 7.9926 attained, it can be said that the technique in [20] is anti-differential in terms of security.

The technique used in [21] combined shift image blocks and AES. First, the hash function is used to generate a shift table for shifting the image blocks. Second, the shifted image is fed into the AES encryption algorithm. Their technique shows the ability to encrypt large data sets efficiently and in real-time, since the NPCR and UACI values are near standard values, which are 99.6689%, and 27.7599%, respectively. Furthermore, correlation value (-0.0410) shows that the original image has nearest values between its neighborhoods than the encrypted image neighborhood pixels, which is evidence of less predictability by third party.

2.2 Frequency Domain

Sinha et al. [22] proposed a new method for gray scale image encryption using 3D jigsaw transform. First, the image is transformed to bit planes, where each bit plane is divided into smaller blocks. The 3D jigsaw method then translocates every block to different location in 3D cube. They used two Fractional Fourier transforms (FRFT), the first FRFT is used to encode image, and the output is then multiplied with a random phase code, while the second FRFT is used to obtain the encrypted image. By using FRFTs and the random phase codes, security is provided.

The 0.05 error rate value recorded for the decrypted image shows the image is of high quality.

In [23] the encrypted process includes three phrases, called color space rotation. The color space of original the color image is first rotated via converting the color image from RGB space to RGB complement space. Then the individual color component is transformed using their proposed reality preserving fractional Mellin transform (RPFrMT) on different fractional orders of the image. Finally, on the basis of achieving high security, the scrambling of pixels is done three dimensionally. Our observation is that the large key space due to their technique can make the encryption sensitive to security threat.

Abuturab [24] proposed a method that secures color images based on Arnold transform in gyrator transform domain. For their method, the color image is separated into their respective R, G and B components and then the individual component is independently encrypted by applying first random phase mask and then first-order Arnold transform and lastly, the gyrator transform. The second random phase mask is placed on the gyrator transformed plane, and a further transformation using the second-order Arnold transform and gyrator transform are performed. These enhancing techniques; the Arnold transform and the gyrator transform employed in [24] are used as additional keys in the encryption and decryption, which might likely offer robustness against occlusion attacks and noise attacks, and high security.

In [25] a single channel color image encryption technique was proposed. The technique is based on orthogonal composite grating and double random phase encoding. A color image first is decomposed into R, G and B components, which subsequently are modulated into an orthogonal composite grating. The deformed composite grating is then encrypted by a typical double random phase encryption technique. It is observed that combining the double random phase encoding and orthogonal composite grating reduces the complexity and cost of encryption. However, in the case of security, the technique falls short, evidence to this conclusion is the near 1 correlation value obtained.

In [26] a color image encryption algorithm that uses the affine transform in the gyrator transform domains, was proposed. Firstly, the affine transform is applied on the RGB components of the color image and the real and imaginary parts of their frequency component are extracted. Second, the R, G, B image pixel values are interchanged by scrambling using a random angle approach. Then, the resulting image is transformed using the gyrator transform and scrambled again by a second affine transform. Their experimental results showed that PSNR of 7.72dB was attained. This is an indication that high security is attainable.

2.3 Hybrid Domain

In [27] the proposed encryption method is based on wavelet transformation and chaotic map. The image is transformed using wavelet decomposition in order to map all significant information to the low frequency sub-band. Subsequently, a high-strength chaotic encryption is adopted to encrypt the low frequency wavelet coefficients, while the XOR is operated on the image regions in the high frequency band. A further wavelet reconstruction is adopted for distributing the encrypted information of the low frequency band to the image as a whole. After Arnold scrambling of the resultant wavelet reconstructed image, the image is then diffused to smooth out the regions of encryption. The method's performance is observed to be reasonable based on the reported encryption time of 0.266 seconds and a key space of 2128.

Abd El-Latif A. et al. [28] proposed the combination of the linear feedback shift register (LFSR) and chaotic systems in hybrid domains. First, permutation is performed on the input image pixel positions based on 2D chaotic map in the frequency domain. Second, the resultant image is diffused by applying the cryptographic primitive operations combined with the LFSR and chaotic map. On the basis of the result reported in [28], their method can be said to be immune from brute force attacks. It was also observed that a large key space of 2256 was obtained. They also recorded the encryption time of 0.023s, which shows that their method is very fast and appropriate for real-time application. With the entropy value of 7.999, their method can be said to be robust to exhaustive attack and the possibility of threat is minimal.

3. Partial (Selective) Encryption

The selective encryption technique unlike the full encryption technique, encodes only significant regions in a given image. The main merit of the selective encryption technique is that it can provide equally, privacy and computational requirements without tradeoffs [29]. The advantages of the selective encryption technique are basically in real-time applications, where confidentiality is important and huge amount of data comes into play. In real-time, an important question is usually how to minimize the computational requirements for secure multimedia. Addressing this concern from the partial

encryption perspective is one of the fundamental solutions to computational complexity problem.

The Partial image encryption techniques are derived from the process of separating information into perceptually sensitive and insensitive data based on perception. Here, we present literatures that addressed the fundamental requirement of a partial encryption scheme, which is that the encrypted regions must be independent of the unencrypted regions. Therefore, the proposed schemes in the literature that we will review in the subsequent discussions will be analyzed on the basis of their approach in meeting the partial encryption requirements. Otherwise, their methods will be concluded to be prone to attack on the basis of the correlations between the encrypted and unencrypted pixels [30].

In this section, partial encryption scheme is described with many research efforts in this category encompasses all domains namely, spatial, frequency and hybrid ([31, 32, 33, 8, 34, 35, 36, 37, 29, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50]). In subsequent sections, we will emphasize on the techniques in these studies on the basis of the domains of implementation and the encryption approaches such as block cipher and stream cipher approaches.

3.1 Spatial Domain

Rao et al. [31] the image is initially divided into correlated and uncorrelated data by separating it into first four MSB planes and last four LSB planes. Then a pseudo random sequence on the uncorrelated data is used to encrypt the correlated data. And at the same time, the uncorrelated data still remains unencrypted, afterwards the correlated data is combined with uncorrelated data using cipher to obtain the final image. It is observed that the encrypted image appears noisy, which increases perceptibility of the encrypted region, thereby increasing threat. More so, the computational complexity problem is not addressed.

In [32] proposed a multi-level ROI image encryption universal architecture, for biometric data. In their work, the multi-level ROI encryption and RC4 were used to encrypt an uncompressed raster image. The idea behind their method is that for an authorized viewer, only the specified regions can be viewed. In essence, only an authorized person can view the contents of the encrypted image, though this is basically for the biometric system. At the initial step, multiple ROIs are selected for each image, which are then encrypted at three levels of authority using RC4 and fingerprint matching algorithms. We observed that their method can provide image information security, though the key space size (2128) is large, which shows that the method can be sensitive to small change in secret key.

In [33] the advanced encryption standard AES-Rijndael was implemented based on five criteria, which are plain data compression, block sizes, selectable round, software implementation optimization, and whole routine selection strategy. These criteria form the basis of their so called SEA selective encryption technique, which is an improvement of the AES algorithm. We observed that their technique reduced execution time by 50%, the region on the encrypted data is over 35% and the entropy value is about 7.9892. Hence, based on these values, it can be deduced that the security level of their method is on the average level.

According to Droogenbroeck in [8], a visual degradation of the image can be satisfactory if the encryption is at least between 4 to 5 least significant bit planes. Based on their observation the selective encryption methods was proposed for uncompressed raster images and compressed (JPEG) images using the encryption ratio between 50% to 60%. These percentages have been shown in their work to contribute to fastness and timely encryption. However, it was not proven how their method is robust against cryptanalysis attack.

Similar to the work by Droogenbroeck in [8], is the work of Podesser et al. [34] where a selective encryption algorithm is applied on uncompressed raster images. The resultant image is divided into 8-bit planes, where the most significant bit planes are encrypted using the Schmidt and Uhl's algorithm. This proposed cryptosystem used AES algorithm that is encrypted image without loss of generality. By their cryptosystem, it will be difficult for a third party or an attacker to decode the secret key; this was also shown by the PSNR value of 9dB obtained.

Kumar [35] enhanced the RC4 algorithm for increased security of the RC4 against attacks. The enhanced RC4 was then implemented with the selective image encryption method. The selective image encryption method is of two steps; 1) for selection of significant image region, and 2) for encrypting the selected regions of the image. On the basis of the selection approach, it can be said that less security and less time during encryption is obtainable. This is based on 210ms time recorded for encryption and 8.192% encryption region on the original image. However, with the small region on the original image, where the encryption is performed, security might be compromised.

Rad R. M. et al. [36] proposed a new image encryption method by combining several established algorithms: Blowfish, AES, Serpent and RC6. The method encrypts the sensitive blocks while insensitive block will be rescanning using 4 different pattern types. Each block is classified as

significant or insignificant block via edge detection method. In encryption phase, the combination strategy was adopted for ensuring that various security levels are attained on the basis of the importance of the block. The proposed method provides different levels of protection for the blocks of varying importance in order to reduce computational resources. This method offers a tiny degree of predictability where attacker is difficult to break cipher image.

Panduranga et al. [37] proposed two selective image encryption methods. By first method, the image is divided into sub blocks. The selected blocks are then encrypted by image mapping that is used as input to the selected blocks. The full encryption of selected blocks is also possible, and each block can use the separate map image. Second method, the position of objects in a given image is detected automatically using the morphological techniques, which locate the positions of the objects of the given image. Then encryption of information is made on the detected object, which is then mapped to the original image. These two approaches are very well suited for special applications such as medical image and satellite image. These techniques used here are most useful when the area or region of interest is known.

3.2 Frequency Domain

Rodrigues et al. [29] proposed a method that is based on AES stream ciphering using variable length coding (VLC) of the Huffman's vector. First, the input image is divided into blocks of 8x8 pixels. Second, each block is transformed from the spatial domain to the frequency domain using discrete cosine transform (DCT). Third, the quantization is applied on the resultant image using Zigzag scan method then applying AES encryption method. The merits observed for the method in [29] is that there is the possibility of identifying one or two regions for each block of 8x8 pixels or group of them. This comes from the fact that they have used the AES in CFB (Cipher Feedback Block) mode, and have applied it over each block. It is important to note that the ROI must be defined in unit of block of 8×8 pixels as a default of JPEG format. Their method is observed to have large key space of 2128 that gives the encryption method high sensitivity to a small change in secret key.

Ou Y. et al. [38] proposed the region-based selective encryption method, which is basically for encrypting medical data. Firstly, two MSBs within the region of interest (ROI) are converted to coefficients using the wavelet transform. Then the AES in CFB (Cipher Feedback Block) mode is employed to encrypt only certain regions of the data in code-stream. Based on the fact that the size of the encrypted bit-stream remained unchanged. Their experimental results reveal that the technique provides low security level with the PSNR value of 10.002dB and does not require large area of the image for encryption; only about 1.258% area was utilized. Furthermore, the security will be low because key space is very small about 232.

Yekkalaet al. [39] employed DCT transformation and scalable lightweight encryption technique to encrypt selected blocks that contain edges. The idea behind their selection approach is to encrypt selected blocks with vital information by utilizing the threshold values at a particular range, while the blocks belonging to other ranges are unencrypted. The PSNR value of 14.46dB is obtained, which translates that an intruder or attacker cannot decipher the secret key used for the encryption. However, the computation time is medium due to the large area indicated by 43%, used for encryption.

Brahimi et al. [40] proposed a novel selective encryption of image plane based on JPEG2000, which encrypts only the code-blocks corresponding to some sensitive terrain. The permutation of blocks code elected in the selected precinct is used to improve the security. AES symmetric encryption is used with CFB mode to encrypt the exchanged code blocks. The amount of data processed in the encryption is minimized via permutation and selective encryption together. This algorithm work with any standard ciphers and requires less computational cost. The encrypted area is about 11.64% when this area of original image is small with less time for encryption but security is good when the encrypted image is independent to the original image because PSNR has very small value, about 6.74dB with difficulty to retrieve the original image without knowing the secret key.

In [41], the new technique is introduced using three levels of permutation on selected blocks and coefficients of orthogonal polynomials transform domain. The original image is first divided into blocks of 4 x 4 pixels and scrambled them in three times. Firstly, scrambling selected bits via applying the Orthogonal Polynomials based transform (OPT) then compute the block of OPT coefficients. Then the low level coefficients in OPT of each block are arranged into a one dimensional zigzag sequence. The blocks to be shuffled are selected according to a pseudo-random sequence generated using a secret sub-key as the seed. Finally, the blocks are split into subsets and shuffled. This shuffling changes the high-level spatial configuration of the content, which is much harder for an attacker to analyze. The OPT is configured as an integer transform for less computation time. To reduce the encryption time the scrambling of bits, coefficients and

blocks are also manipulated. The OPT is reported to have large key space of 2256, which is known to increase chances of threat. And with the reported 0.0366 correlation value, OPT presumed to be robust against brute force statistical and differential attacks. The technique is also reported to have utilized standard size of 25% for the region of encryption, which is a good indication that the encrypted image is independent of the original image.

In Kulkarni et al. [42], a selective encryption approach was proposed. The selection utilizes five level wavelet transformations to decompose the input image by applying the wavelet filter banks. To arrange the image in hierarchal structure, the high pass band and low pass band filters are employed so that each structure is of different significance. As per Human Visual System (HVS), the degraded version of original image by the proposed technique gives a sufficient level of transparency. This method selecting the high correlation coefficient of 5 level sub-bands to control the security with transparency. Furthermore, PSNR has very small value, around 3.448dB that is difficult for the intruder to retrieve the original image without knowing the secret key.

Younis [43] proposed a new encryption method; an important part of image level two sub-band is used by employing fuzzy c-means (FCM), an advanced technology for clustering analysis combined with the permutation cipher. Only 6.25-25% of the original data is encrypted with a significant reduction in the time of encryption and decryption. The encryption algorithm include: wavelet packet transform, quantization by FCM, permutation cipher and arithmetic coding to level-two sub-band images. The proposed partial encryption method is fast and secure."“Wavelet based on Vector Quantization and Permutation is more suitable for average level of security because the PSNR of the reconstructed image is large. But, when the number of clusters increases, both PSNR and execution time are increase as well." It can be seen that large key space is supposed to reduce threat and increases the immunity from attacker.

Flayh et al. [44] proposed an efficient partial image encryption technique that employs 3 levels of the discrete wavelet transform (DWT) with the AES cipher and stream cipher. The image is smoothened using a smoothing filter in order to hide details of cipher image so that perceptibility of the encrypted regions in the image is reduced. It is observed that the reconstructed image is almost the same as the original image. Their method reduced encrypted regions by 1.5625%, which subsequently brought down the execution time for the encryption process. It can also be noted that the small portion encrypted increases the correlation of the cipher image, which might make the image to be prone to threat. More also, it is observed that AES, which is known to be of large key space, resulted in the key space of 2128 and when combined with cipher of 216 key space, a large key space is inevitable. Therefore, it should be noted that the size of the key space plays a crucial role in ensuring that the encrypted information is secured.

Richard et al. [45] proposed a new selective regional encryption algorithm. The algorithm is used to partially encrypt the original image by permutation the coefficients in the DCT domain. Edge detection algorithm is used to differentiate image regions. This algorithm uses thresholding to isolate dense image regions from worse image regions. Then the median filter is applied on the resultant image to reduce noise components in the image. A simple encryption method, which uses the properties of energy compaction of a shape adaptive cosine transformation, is then applied in the DCT domain. The encrypted area is about 10% with multi region for image encryption, which might increase security of encrypted data.

Sasidharan et al. [46] proposed a fast partial image encryption scheme using RC4 stream cipher and Discrete Wavelet Transform (DWT). In their proposed technique, the encryption is carried out at the lowest frequency band using the stream cipher. Their basic idea of the stream cipher was to retain all the image information. However, using the stream ciphers consumes more time, since it typically encrypts one byte at a time. The bitwise exclusive-OR (XOR) is used to combine between key stream and original image while the former is generated by random numbers. When edges are encountered, a shuffling algorithm is employed. The encryption time is reduced by encrypting only the lowest frequency band of the image and maintains a high level of security by shuffling the rest of the image using the shuffling algorithm with a large key space value of about 2256. It can be observed in [46] that the entropy result of the encrypted image, which is about 4.7807, provides a freer platform for an intruder to decipher the secret key used to encrypt the image. But it is strong against statistical attack because PSNR has high value, about 20.7056dB.

Kuppusamy et al. [47] proposed a partial image encryption optimization scheme using high energy coefficients of the transformed image, which were selected by employing the particle swarm optimization (PSO) technique within the daubechies4 domain for encryption. Our observation is that with the key space of 2256 and the ability to increase the key space by increasing the number of permutation for each permutation round, reaches to the average level of security. The encrypted area of the image is about 33%,

which is a small rate that indicates medium speed for encryption.

In [48], a technique that applies the Arnold Cat map permutation on low frequency sub-band of the DCT transformed image for encryption was proposed. Their main idea for selecting the low frequency sub-band of the DCT transformed image is attributed to the fact that the human visual system (HVS) is more drawn to information at the lower frequencies than the higher frequency information. Important information such as object, shape, etc. is presented in low frequency sub-bands, while the detailed information is contained in higher frequency sub bands. Our inference is that, since only the DCT coefficient of the low frequency sub-bands is encrypted, the likelihood of predicting the encrypted information is reduced. The technique in [48] is considered to be robust against noise, though to some extent since the decrypted image shows some presence of noise.

3.3 Hybrid Domain

One of the literatures that explored the merits of combining the spatial and frequency domain for effective encryption technique is Taneja N. et al. [49]. In their work the fractional wavelet was used to encrypt only significant sub-bands using Arnold cat map and logistic map. They first of all encrypted the significant part of the image in spatial domain and then the insignificant parts are partially encrypted in the wavelet based frequency domain. Prior to the frequency processing the Prewitt edge detector is used to extract edges in the image, which represent the significant part of the image. From that, a PSNR value of 9.3008dB is observed, which is an indication that their technique ensures better perceptual and cryptography due to the less computational time needed to encrypt the image. It can be concluded that the encrypted image achieved in the hybrid domain using the technique is independent of the original image and is also difficult to alter.

A novel concept that combines phase manipulation and sign encryption in partial image encryption technique was proposed by Parameshachari et al. [50]. The encryption process consists of two stages: in the first stage, the phase and magnitude of the input image are derived using the Fast Fourier Transform (FFT).”Then the phase component of the image is scrambled prior of the inverse Fast Fourier transformation (IFFT) in order to obtain the modified version of the image. For the second stage, the modified image is partially encrypted by using sign encryption. The sign encryption is obtained by extracting the sign bits of the modified image in the partially encrypted image. It can be deduced that the proposed method is fast and of low security for the encrypted data. It is also evident that the encrypted image is independent of the original image and will be difficult for an intruder to know the secret key given the medium value of the entropy (7.5742) and more threat prone achieved.

4. Conclusions

In this paper, we reviewed a wide-range of image encryption algorithms and classified them on the basis of full and partial image encryption schemes under spatial domain, frequency domain and hybrid domain categories. In the course of this review, some observations were made, which are that full encryption scheme ensures high level of security of encrypted data due to the fact that they encrypt the entire image, though much time is spent in such a process. In the case of partial encryption, only a region or some part of the image is encrypted. In other words, the time spent in encrypting the region of interest is less in comparison to the full encryption schemes. For this reason, the partial encryption scheme is more appropriate for real-time applications.

Conclusively, while partial encryption techniques seem promising in terms of encryption time, achieving an encryption technique that balances security with processing time for real-time applications is still a challenge. However, some key elements such as the type of data to be encrypted, the percentage of the data that must be protected, and the measures put in place to protect the data from cryptanalytic attack, when considered in the design of a real-time image encryption technique can be a viable solution to real-time image encryption problems.

References

[1] H. T. Panduranga, and S. K. N. Kumar, “Multiple Image Encryption Using Phase Manipulation and SCAN Methods”, in proceedings of 4th International Conference on Signal and Image Processing (ICSIP 2012), vol. 222, no. Icsip 2012, pp. 257–264.

[2] R. Kaur, and E. K. Singh, “Image Encryption Techniques : A Selected Review”, Journal of Computer Engineering (IOSR-JCE), vol. 9, no. 6, 2013, pp. 80–83.

[3] N. A. V. Ephin M, and Judy Ann Joy, “Survey of Chaos based Image Encryption and Decryption Techniques”, IJCA Proceedings on Amrita International Conference of Women in Computing (AICWIC’13) Proceedings published by International Journal of Computer Applications (IJCA) , January 2013, no.2 pp. 1–5.

[4] E. Thambiraja, G. Ramesh, and Dr.R.Umarani, “A Survey on Various Most Common Encryption Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, July 2012, pp. 226–233.

[5] M. A. El-wahed, S. Mesbah, and A. Shoukry, “Efficiency and Security of Some Image Encryption Algorithms”, in

proceedings of the World Congress on Engineering, July 2008, vol. I, pp. 4–7.

[6] V. Bhatt, and G. S. Chandel, "Implementation of New Advance Image Encryption Algorithm to enhance security of multimedia component", International Journal of Advanced Technology & Engineering Research (IJATER), vol. 2, no. 4, 2012, pp. 13–20.

[7] A. B. Abugharsa, A. S. B. H. Basari, and H. Almangush, "A New Image Encryption Approach using The Integration of A Shifting Technique and The AES Algorithm", International Journal of Computer Applications, vol. 42, no. 9, 2012, pp. 38–45.

[8] M. A. A. Steffi, and D. Sharma, "Comparative Study of Partial Encryption of Images and Video", International Journal of Modern Engineering Research (IJMER), vol. 1, no. 1, 2011, pp. 179–185.

[9] B. D. Parameshachari, and K. M. S. Soyjaudah, "A New Approach to Partial Image Encryption", in 1st International Conference on Advances in Computing (ICAdC), 2013, Vol. 174, pp. 1005–1010.

[10] W. Puech, A. G. Bors, and J. M. Rodrigues, "Protection of Colour Images by Selective Encryption", in Advanced Color Image Processing and Analysis, New York: Springer, 2013, pp. 397–412.

[11] H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu, C. K. Huang, and Y. H. Hsu, "Hybrid image encryption using multi-chaos-system", in 7th International Conference on Information, Communications and Signal Processing (ICICS), Dec. 2009, pp. 1–5.

[12] R. Rhouma, D. Arroyo, and S. Belghith, "A new color image cryptosystem based on a piecewise linear chaotic map", in 6th International Multi-Conference on Systems, Signals and Devices, Mar. 2009, pp. 1–6.

[13] Musheer Ahmad, and M. Alam, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, vol. 2, no. 1, 2009, pp. 46–50.

[14] W. Wei, L. Fen-lin, G. Xinl, and Y. Yebin, "Color image encryption algorithm based on hyper chaos", in 2nd IEEE International Conference on Information Management and Engineering, 2010, pp. 271–274.

[15] M. R. Kamali, Seyed Hossein, Reza Shakerian, and Maysam Hedayati, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", International Conference on Electronics and Information Engineering (ICEIE), 2010, vol. 1, no. Iceie, pp. 141–145.

[16] A. Z, L. L, and S. Z, "Research on Method of Color Image Protective Transmission Based on Logistic Map", in International Conference on Computer Application and System Modeling (ICCASM), Oct. 2010, Vol. 9, no. Iccasm, pp. 266–269.

[17] M. T. Rodriguez-Sahagun, J. B. Mercado-Sanchez, D. Lopez-Mancilla, R. Jaimes-Reategui, and J. H. Garcia-Lopez, "Image Encryption Based on Logistic Chaotic Map for Secure Communications", IEEE Electronics, Robotics and Automotive Mechanics Conference, Sep. 2010, pp. 319–324.

[18] J. M. K. Mastan, G. A. Sathishkumar, and K. B. Bagan, "A Color Image Encryption Technique Based on a Substitution-Permutation Network", Advances in Computing and Communications, vol. 4, 2011, pp. 524–533.

[19] K. K. S. Pareek, Narendra K, and Vinod Patidar, "A Symmetric Encryption Scheme for Colour BMP Images", International Journal of Computer Applications in Special Issue on Network Security and Cryptography", 2011, pp. 42–46.

[20] Ahmed Bashir Abugharsa, and H. Almangush, "A New Image Encryption Approach using Block-Based on Shifted Algorithm", International Journal of Computer Science and Network Security (IJCSNS), vol. 11, no. 12, 2011, pp. 123–130.

[21] R. S. Yadav, M. H. D. R. Beg, and M. M. Tripathi, "Image Encryption Techniques: A Critical Comparison", International Journal of Computer Science Engineering and Information Technology Research, vol. 3, no. 1, 2013, pp. 67–74.

[22] A. Sinha and K. Singh, "Image encryption using fractional Fourier transform and 3D Jigsaw transform", http://pdf-world.net/pdf-2013/Image-encryption-using-fractional-Fourier-transform-and-3D-Jigsaw-transform-pdf.pdf.

[23] N. Zhou, Y. Wang, L. Gong, X. Chen, and Y. Yang, "Novel color image encryption algorithm based on the reality preserving fractional Mellin transform", Optics and Laser Technology, vol. 44, no. 7, Oct. 2012, pp. 2270–2281.

[24] M. R. Abuturab, "Securing color information using Arnold transform in gyrator transform domain," Optics and Lasers in Engineering, vol. 50, no. 5, May 2012, pp. 772–779.

[25] Y. He, Y. Cao, and X. Lu, "Color image encryption based on orthogonal composite grating and double random phase encoding technique", Optik - International Journal for Light and Electron Optics, vol. 123, no. 17, Sep. 2012, pp. 1592–1596.

[26] H. Chen, X. Du, Z. Liu, and C. Yang, "Color image encryption based on the affine transform and gyrator transform", Optics and Lasers in Engineering, vol. 51, no. 6, Jun. 2013, pp. 768–775.

[27] Z. Yu, Z. Zhe, Y. Haibing, P. Wenjie, and Z. Yunpeng, "A chaos-based image encryption algorithm using wavelet transform", in 2nd International Conference on Advanced Computer Control, March 2010, Vol. 2, no. 4, pp. 217–222.

[28] A. a. Abd El-Latif, X. Niu, and M. Amin, "A new image cipher in time and frequency domains", Optics Communications, vol. 285, no. 21–22, Oct. 2012, pp. 4241–4251.

[29] J. M. Rodrigues, W. Puech, and A. G. Bors, "A Selective Encryption for Heterogeneous Color JPEG Images Based on VLC and AES Stream Cipher", 3rd European Conference on Colour in Graphics, Imaging and Vision (CGIV'06), June 2006, vol. 1, pp. 34–39.

[30] V. Suresh and C. E. V. Madhavan, "Image Encryption with Space-filling Curves", in defence Science Journal, vol. 62, no. 1, 2012, pp. 46–50.

[31] Y. V. S. Rao, A. Mitra, and S. R. M. Prasanna, "A Partial Image Encryption Method with Pseudo Random Sequences", Lecture Notes in Computer Science, International Commission on Intervention and State Sovereignty (ICISS), vol. 4332, 2006, pp. 315–325.

[32] A. Wong and W. Bishop, "Backwards Compatible, Multi-Level Region-of-Interest (ROI) Image Encryption

Architecture with Biometric Authentication", International Conference on Signal Processing and Multimedia Applications, July 2007, pp. 324 – 329.
[33] Ju-Young Oh, Dong-Il Yang, and Chon KH, "A Selective Encryption Algorithm Based on AES for Medical Information", Healthcare informatics research, vol. 16, no. 1, Mar. 2010, pp. 22–9.
[34] B. D. Parameshachari, and K. M. S. Soyjaudah, "Analysis and Comparison of Fully Layered Image Encryption Techniques and Partial Image Encryption Techniques", Communications in Computer and Information Science, vol. 292, 2012, pp. 599–604.
[35] P. Kumar, "RC4 Enrichment Algorithm Approach for Selective Image Encryption", International Journal of Computer Science & Communication Networks, vol. 2, no. 2, 2012, pp. 181–189.
[36] R. M. Rad, A. Attar, and R. E. Atani, "A Comprehensive Layer Based Encryption Method for Visual Data", International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 6, no. 1, 2013, pp. 37–48.
[37] H. T. Panduranga, and S. K. Naveenkumar, "Selective image encryption for Medical and Satellite Images", International Journal of Engineering and Technology (IJET), vol. 5, no. 1, 2013, pp. 115–121.
[38] Y. Ou, C. Sur, and K. H. Rhee, "Region-Based Selective Encryption for Medical Imaging", 1st Annual International Workshop, 2007,vol.4427, no. 4613, pp. 62–73.
[39] A. K. Yekkala, N. Udupa, N. Bussa, and C. E. V. Madhavan, "Lightweight Encryption for Images", IEEE. International Conference on Consumer Electronics, Jan. 2007, vol. 3, pp. 1–2.
[40] Z. Brahimi, H. Bessalah, a. Tarabet, and M. K. Kholladi, "A new selective encryption technique of JPEG2000 code stream for medical images transmission", 5th International Multi-Conference on Systems, Signals and Devices, Jul. 2008, pp. 1–4.
[41] R. Krishnamoorthi and P. D. S. K. Malarchelvi, "Selective Combinational Encryption of Gray Scale Images using Orthogonal Polynomials based Transformation", International Journal of Computer Science and Network Security, vol. 8, no. 5, 2008, pp. 195–204.
[42] N. S. Kulkarni, B. Raman, and I. Gupta, "Selective encryption of multimedia images," 32th National Systems Conference, Dec. 2008, pp. 467–470.
[43] H. A. Younis, T. Y. Abdalla, and A. Y. Abdalla, "Vector Quantization Techniques For Partial Encryption of Wavelet-based Compressed Digital Images", Iraqi Journal of Electrical and Electronic Engineering, vol. 5, no. 1, 2009, pp. 74–89.
[44] N. a. Flayh, R. Parveen, and S. I. Ahson, "Wavelet based partial image encryption", International Multimedia, Signal Processing and Communication Technologies(IMSPCT), Mar. 2009, pp. 32–35.
[45] R. E. L. M. and S. S. Agaian, "Selective Region Encryption Using a Fast Shape Adaptive Transform", IEEE International Conference on Systems, Man, and Cybernetic (ICSMC) , 2010, pp. 1763–1770.
[46] S. Sasidharan, and D. S. Philip, "A Fast Partial Encryption Scheme with Wavelet Transform and RC4", International Journal of Advances in Engineering & Technology(IJAET), vol. 1, no. 4, 2011, pp. 322–331.
[47] K. Kuppusamy, and K. Thamodaran, "Optimized partial image encryption scheme using PSO", in International Conference on Pattern Recognition, informatics and medical engineering, May 2012, pp. 236–241.
[48] R. Munir, "Robustness Analysis of Selective Image Encryption Algorithm Based on Arnold Cat Map Permutation", in Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics, Nov. 2012, pp. 1–5.
[49] N. Taneja, B. Raman, and I. Gupta, "Combinational domain encryption for still visual data", Multimedia Tools and Applications, vol. 59, no. 3, Mar. 2011, pp. 775–793.
[50] P. Parameshachari B D, K M Sunjiv Soyjaudah, and Sumitrha Devi K A, "Secure Transmission of an Image using Partial Encryption based Algorithm", International Journal of Computer Applications, vol. 63, no. 16, 2013, pp. 33–36.

Lahieb Mohammed Jawad received the B.Cs. degree in computer science from University of Al-Nahrain, Iraq, in 1999 and the M.Sc. degree in Computer Science from University of Al-Nahrain, Iraq, in 2002. Currently, she is pursuing her Ph.D. degree in Unversiti Technologic Malaysia. Her research interest includes image processing and understanding, multimedia encryption, watermarking, steganography, Intelligent Vision, artificial Intelligent. She published two papers.

Ghazali Bin Sulong received his BSc degree in statistic from National University of Malaysia, in 1979, and MSc and PhD in Computing from University of Wales, Cardiff United Kingdom, in 1982 and 1989, respectively. He is currently a professor at the Faculty of Computing, Universiti Teknologi Malaysia. His research interest includes Biometric – fingerprint identification, face recognition, iris verification, ear recognition, handwriting recognition, and writer identification; object recognition; medical image segmentation, enhancement and restoration; human activities recognition; data hiding – digital watermarking and steganography; image encryption; image compression; image fusion; image mining, digital image forensics; object detection, segmentation and tracking.