An Overview of Crypto-Compressive Based on Selective Coding

Enas Kh. Alamiry[1], Faisal G. Mohammed[2]

[1] Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

[2] Department of Remote Sensing and Geographic Information's, College of Science, Baghdad University, Baghdad, Iraq

Abstract: ***Image encoding (visual cryptography) is special encryption technique to hide the information contained within an image. In such a way it can't be decrypted or recognized by neither human visual system (HVS) nor cryptanalysis algorithms. Partial image encryption have become very popular due to rapid evolution in information technology and visual communications over open networks, it is considered crucial to real time applications that need to be very fast and entirely secured, where the digital data must kept intact from eavesdroppers and unauthorized access. Most of today's techniques encrypt all of the image data which consumes tremendous amount of time and computational payload. This paper introduces the image Encryption strategy along with its main categories (full and partial encryption), partial Encryption sub-categories, and the leading schemes proposed for Partial Image Encryption (PIE)that only apply the encryption algorithm to merely a portion of the image data which produces huge reduction in processing time and computational Complexity.***

Keywords: Partial Encryption, Selective Encryption, Cryptography, Image Scrambling

1. Introduction

Nowadays, internet is considered a major source for information gathering and transmission. Electronic-financing, military and medical applications involve extensive use of digital media[1][2][3]. In such scenarios security plays an important role [4][5][6][7]. One way to achieve security goals is encrypting the digital media. Visual cryptography is the conversion of image data from its original form to another from that is basically hides the content of images and preserves privacy from unauthorized access[8][9][10][7][4][11].

Unlike text data image data have different features such as bulk capacity, high correlation against pixels, high redundancy and not to forget their huge size that makes them slow to process and difficult to apply[9][12][13][14][15].

There are many information hiding techniques such as steganography, watermarking, and cryptography [4][7][3][16]. Traditional encryption techniques provide good security level but they are not suitable to multimedia data[1][9]. Another approach has been considered to preserve security and privacy of images known as "*Partial Encryption of Images"* that is obtained by applying cipher to part of the image to produce an obvious reduction in processing time and computational payload [7][9][17][18][11][14][19]. Data are much easier to manipulate and dominate using compression algorithms that partition the data according different aspects and reduces its volume then the result is encrypted to provide security[20][10][1][5][21][22][15].

This paper is organized as follows: in section one we are presenting general guide line for different techniques for partial encryption, section two is the partial encryption strategy, section three is a literature review listing the leading researches in the field, section four lists the Experimental results for some schemes, and finally section five are the conclusions conducted from the schemes studied.

2. Image Encryption

Image encryption is the technique through which we can reserve the image data from eavesdroppers during transmission and storage. Encryption can beaccomplished by encrypting the image data so that they can't be understood. The main goal is to make the image data not comprehensible to any unauthorized access that might intercept them. Perceptual security in image encryption is not the only concern but also concentrate on accomplishing it with achieving a high cryptographic security(comparative study). Image encryption was not studied as normal encryption or visual encryption. It was used to encode digital media (images) to provide confidentiality and intellectual property fortification against unauthorized access**.** Information confidentiality is an essential aspect of image encryption. The confidentiality of the encrypted data with a parity in time and cost effectiveness of the encryption technique is the obstacle still faced in image encryption [23]**.**

1) Full Image Encryption

Full image encryption is the procedure of encrypting the sequence forming the image data. This type of image encryption is robust and entirely secures the contents of the image and preserves the perceptual security by keeping the image quality as fair as possible[24] hence the processing time is fatal in applications requires real time processing and also the extensive computations required to encrypt each and every last bits in the processed image.

2) Partial (Selective) Image Encryption (PIE)

The partial encryption technique unlike the full encryption , that encodes only the significant regions(Region of Interest RoI) in a given image. The main advantage of the partial encryption technique over full encryption is that it can offer equally, privacy and computation complexity requirements reduction without tradeoffs. The main impact of the partial encryption technique are basically shown in real-time applications, where confidentiality is significant and huge amount of data comes into play. In real-time, the main question is usually how to diminish the computational complexity requirements for secure image transmission and storage. Addressing this matter from the partial encryption perspective is one of the ultimate solutions to computational complexity problem.

The Partial image encryption techniques are resultant from the process of separating information into perceptually sensitive and insensitive data based on perception, which is that the encrypted areas must be independent of the unencrypted ones.[25]

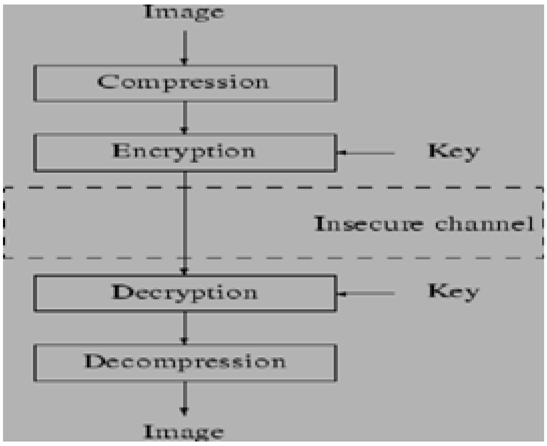

Figure 1: Partial encryption strategy

3. Classification and Description of Image Compression and Encryption

The former researches can be categorized according to the application of the two processes image compression and image encryption as:

a) Compression followed by Encryption (CE)

In this category an intruder have fewer clues about how to access the image data but encryption may again increase the size. Aninnovative approach proposed called *"partial encryption"*to reduce encryption and decryption time in image and video communication and processing. In this approach, onlyportion of the compressed data is encrypted. This approach is suitable for the JPEG and MPEG compression algorithms. As well as, partial encryption schemes such as quad-tree and wavelet image compression, and an extension for video compression. Partial encryption permits the encryption and decryption time to be significantly minimized without affecting the compression operation of the underlying compression algorithm. It will likely be shown that though a large portion of the compressed data is left unencrypted, it is hard to recover the original data without descrambling the scrambled part. Applications using low bit rate compression algorithms would outcome in smaller portions to be scrambled, making the partial encryption approach even more reasonable andappealing. The results on video compression are similar. Thus, a substantial reduction in encryption and decryption time is achieved.[26]

b) Encryption followed by Compression (EC)

In this category size is not again maximized but an intruder may have more clues about how to access the image data. One of the main advantages of using CE is that the amount of data to be scrambled is considerably reduced, and as a consequence, the processing time is also decreased. Obviously, with the cascaded Image estimates scheme for example, the more loops you use, the less data need to be encrypted, but the compression ratio amplifies. Besides security and processing time, one of the major requirements of joint encryption and compression is to preserve the same compression performance when encryption is taken into consideration. In the mentioned approach, as the Image transform is tremendously tunable, determining the number of loops of the cascaded image that offers the best trade-off between processing time and compression ratio. Its main strength is the processing time, as it only computes consecutive Image transforms, which are not computationally expensive, and only the finishingbasis projection is scrambled, which certainly can be very small. The proposed approach present a processing time reduction against the full encryption.[27]

c) Joint Compression and Encryption (JCE)

This approach is occupied these days, which may be rapid when compared to previous two categories but it is complicated. Here, we explain entirely pipelined single chip architecture for executing a new simultaneous image compression and encryption technique appropriate for real-time applications. The proposed technique utilizes the image transform assets to accomplish the compression and the encryption simultaneously. First, to comprehend the compression, image transform applied to a number of images. Second, opposing to conventional compression algorithms, only some distinctive points of image transform outputs are multiplexed. For the encryption procedure, a random number is generated and added to some particular image transform coefficients. Similarly, to improve the substantial implementation of the proposed approach, a special consideration is given to the image transform algorithm. In fact, a new way to comprehend the compression based on image transform algorithm and to reduce, simultaneously, the substantial requirements of the compression process is offered.[28]

4. Literature Survey

Some related works to the current overview are summarized in the following points:

1) Som et al. [7]Proposed a non-adaptive scheme based on chaos. They first decomposed the gray scale images to their equivalent 8-bitplanes, then encrypt the bit planes using couple tent map binary number generator (PRBNG) the four significant bit planes are determined by the level of significance for each pixel value and encrypted using a key obtained by applying the recurrence relation of tent map based on couple tent map binary number generator (PRBNG) the significant bit planes are then combined to produce the cipher image.
2) Parameshachari et al. [9]presented a novel algorithm for partial image encryption using combined phase modulation and sign encryption. First Fourier Transform

(FT) is applied to the input image to get the phase and magnitude, then the image phase is scrambled using sign encryption that extracts sign bits to obtain partially encrypted image.

3) Kekre et al. [8] introduced a scheme for partial image encryption that the input image is partitioned in to four components (LL, HL, LH,HH) using sinusoidal wavelet transform, LL,LH and HH are then scrambled using Walsh sequency and the result is partially encrypted image, while the HL sub-band is neglected.
4) Selective encryption technique has been proposed by Paraveenkumar et al. [4]where the confusion and diffusion are applied to the input image producing new values using pseudo-random number generator then the result is xored with the original pixel values, the modified image is then transformed using Discrete Cosine Transform (DCT) and quantized, finally, the compressed image is encrypted using Arnold Shuffling to produce a scrambled image.
5) Choudhary et al. [17] presented a partial encryption scheme where the input image is partitioned into blocks using block wise shuffling and permuted by utilizing Arnold map the permuted blocks then combined to form the final presentation of the scrambled image.
6) Bahrami et al. [13] presented a scheme for partial encryption of images using orthogonal transform known as Discrete Cosine Transform (DCT) that provides good compaction for multimedia data, the DCT coefficients are then quantized and the entropy coding is calculated to produce compressed image. The compressed image is then encrypted using stream cipher with an encryption key generated similarly to AES key generation process, then each coefficient is encoded using different stream cipher algorithm.
7) Belazi et al. [1] introduced a partial encryption scheme utilizing lifting wavelet transform to compress the image and extract the requisite information to be encrypted. The substitution boxes (S-boxes) generated by chaotic system and linear fractional transform are used to encrypt the image components, the confusion and diffusion characteristics are achieved by three phases: block permutation, substitution, and diffusion using dynamic keys in encryption process to produce scrambled image.
8) Panduranga et al. [18] Proposed a scheme for selective image encryption that only the region of interest is detected either manually or automatically to be encrypted using morphological operation. The block encryption process have two inputs first is the selected block and the second is the map image to encrypt the block partially, complete encryption for selected blocks can be achieved by using separate map image for each block.
9) Lian et al. [22]introduced two aspects for partial image encryption (sub-band and bit-plane) sub-band layers are dependent on each other which provide a vulnerable security that the encrypted layers can be recovered from the unencrypted ones, while, bit- planes are independent. The most significant 8-bits of the low frequency blocks are encrypted with AES cipher, while the middle and high frequency blocks are all encrypted with AES cipher to form the scrambled image.
10) Hazarika et al. [10] Proposed a partial encryption scheme where the input image is transformed using Discrete Wavelets Transform (DWT) to four components while only the (LL approximation) is quantized and the bit positions are permuted using two dimensional chaotic logistic map then the result is XORed with third chaotic logistic map, finally the whole image is retransformed using Inverse Discrete Wavelet Transform (IDWT) to produce the encrypted image.
11) Panduranga et al. [19]introduced a scheme for image partial encryption that the input image is divided for several blocks; each time the image is divided into different block sizes. Bits in each block are permuted using chaotic map to generate new sequences to generate the cipher image.
12) Wen et al. [2] introduced selective image encryption infrared target-based scheme by utilizing block cross encryption and logistic-sine system. First the infrared beam targets specific regions of the image that can be effectively detected using geometric active counter model based on partial differential equation (PDE); the detected regions of interest are encrypted using block cross encryption mode based on logistic-sine system to produce scrambled images.
13) Zhou et al. [3] designed novel scheme for partial encryption combining compressive sensing with discrete fractional random transform. A measurement matrix and two random circular matrices utilized in compressive sensing are generated by using two dimensional logistic modulation map; the modified image is then encrypted using Arnold Transform and discrete fractional random transform.
14) Zang et al. [29] proposed an embedded partial encryption for compressed color images based on chaos. The color images is decomposed to (RGB) components that are going to be transformed to YCbCr each channel is then transformed using Discrete Wavelet Transform (DWT); the coefficients matrix is then encoded by CSPIHT that maintains three sets of data: list of insignificant pixels (LIP), list of insignificant sets (LIS), and list of significant pixels (LSP). The generation of key stream is done by the Pricewise Linear Chaotic Map (PWLCM) that is going to be XORed with (LIP) bit stream to produce partially encrypted image.
15) Rehman et al. [30]proposed selective image encryption scheme based on DNA complementary rules and block cipher; where the input image is divided into blocks, the most significant bit (MSB) in each block is added under DNA algebraic addition operation to least significant bit (LSB) that is already encrypted by selecting chaotically different DNA rules for each pixel. The image blocks are permuted using piecewise linear chaotic map (PWLCM) while the selection of encoding and decoding rules is done by logistic sequence for each pixel.

5. Comparison of Some Experimental Results Studied

Among the verity of schemes studied there are many aspects to measure the output of the experimented images some use point correlation between pixels in cipher and original images, similarity index measure (SSIM), Peak average fractional change in pixel value (PAFCPV), Mean Squared Error(MSE), and processing time as scale for system performance. Here in **Table1** is a list of some of the tested images encryption/ decryption time along with the image size.

Table1: Image encryption and decryption processing time for some of the tested subjects

item	Image name	Ref.	Image Size	Encryption time(sec)	Decryption time(sec)
1	Boat	[7]	---------	0.923	0.634
2	Boat	[22]	256*256	9.2	---------
3	Elaine	[7]	---------	0.398	0.296
4	Map	[7]	---------	0.915	0.814
5	Baboon	[7]	---------	0.398	0.296
6	Baboon	[21]	512*512	1.113	---------
7	Baboon	[22]	512*512	9.9	---------
8	Airplane	[21]	512*512	1.099	---------
9	Lena	[21]	256*256	0.272	---------
10	Lena	[3]	256*256	0.606061	---------
11	Lena	[3]	512*512	2.6354	---------
12	Lena	[22]	256*256	7.9	---------
13	Lena	[12]	256*256	0.0538	---------
14	Lena	[12]	512*512	0.2338	---------
15	Lena	[1]	256*256	0.155	---------
16	Lena	[13]	256*256	1.75	---------
17	Barbra	[21]	512*512	1.113	---------
18	Couple	[21]	256*256	0.273	---------
19	Couple	[13]	256*256	1.74	---------
20	Jelly beans	[21]	256*256	0.273	---------
21	Peppers	[21]	512*512	1.092	---------
22	Peppers	[22]	256*256	9.5	---------
23	Tiffany	[21]	512*512	1.100	---------
24	Group	[21]	400*300	0.503	---------
25	Child	[21]	256*197	0.211	---------
26	Friends	[21]	259*194	0.210	---------
27	Model in black dress	[21]	512*768	1.1676	---------
28	Camera man	[22]	256*256	8.0	---------
29	Village	[22]	512*512	10.3	---------
30	Jet	[22]	256*256	8.8	---------
31	Light house	[10]	512*512	2.0748	1.2636
32	Clock	[13]	256*256	1.73	---------
33	Chemical plant	[13]	256*256	1.67	---------
34	Aerial	[13]	256*256	1.65	---------
35	Stream and bridge	[13]	256*256	1.66	---------
36	Man	[13]	256*256	1.69	---------
37	Airport	[13]	256*256	1.68	---------

* The symbol "**---------**" indicates that subject wasn't tested in that particular scheme.

6. Conclusions

In today's open networks nothing is secured, and the images with critical and sensitive information should be kept intact, the partial image encryption schemes are used to preserve security and reduce both processing time and computational complexity. Here we had studied partial image encryption schemes and techniques in the span of four years (2013-2017) and concluded the following:

1) Partial image encryption is solution for reducing the cost of data over mobile and wireless networks.
2) Provide better security than traditional encryption techniques and higher performance.
3) The tradeoff of high speed is the degradation in the descrambled image quality.

The Partial encryption approach is suitable for transmission applications and real time encryption.

References

[1] A. A. E.-L. A.-V. D. R. R. S. B. Akram Belazi, "chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transform," optics and laser in engineering, Elsevier , pp. 37-50, 2017.

[2] y. z. z. f. j.-x. c. wening wen, "infrared target based selective encryption by chaotic map," optics communications, Elsevier , pp. 131-139, 2015.

[3] J. Y. C. T. S. P. Z. Z. Nanrun Zhoua, "double image encryption scheme combining DWT-based compressive sensing with discrete fractional random transform," optics communications, Elsevier , 2015.

[4] C. S. K. T. J. R. a. R. A. Padmapriya Praveenkumar, "Chaotic & Partial Encrypted Image on XOR Bus - Unidentified Carrier Approach," in 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), ©2016 IEEE, Coimbatore, INDIA, 2016.

[5] P. Sonali.A.Chaudhari, "Review on Secret Data Hiding in Encrypted Compressed Video Bit Streams," International Journal of Computer Science Trends and Technology (IJCST) , vol. 3, no. 2, pp. 94-96, 2015.

[6] P. A. V. Priya R Sankpal, "Image Encryption Using Chaotic Maps: A Survey," in Fifth International Conference on Signals and Image Processing, © 2013 IEEE , BANGALORE, INDIA, 2014.

[7] S. S. Sukalyan Som, "A Non-adaptive PartialEncryption of Grayscale Images Based on Chaos," in First International Conference on Computational Intelligence: Modelling, Techniques and Applications (CIMTA-2013), Elsevier , 2013.

[8] T. S. a. P. N. H. H.B. Kekre, "Partial Image Scrambling Using Walsh Sequency in Sinusoidal Wavelet Transform Domain," Intelligent Systems Technologies and Applications, Advances in Intelligent Systems and Computing , Springer International Publishing Switzerland 2016 , pp. 471-484, 2016.

[9] K. M. S. S. S. D. K. A. Parameshachari B D, "Secure Transmission of an Image using Partial Encryption based Algorithm," International Journal of Computer Applications, vol. 63, no. 16, pp. 33-36, 2013.

[10] S. B. S. Nitumoni Hazarika, "A Wavelet Based Partial Image Encryption using Chaotic Logistic Map," in 2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT) , 2014.

[11] D. D. W. D. T. a. S. V. Nitin Kumar, "Review on Different Chaotic Based Image Encryption Techniques," International Journal of Information and Computation Technology, vol. 4 , no. 2 , pp. 197-205, 2014.

[12] y. z. c.-m. p. C. p. c. zhongyun hua, "2D sine logistic modulation map for image encryption," Information Sciences, Elsevier, pp. 80-94, 2015.

[13] m. n. saeed bahrami, "encryption of multimedia content in partial encryption scheme of DCT transform coeffiecent using a light weight stream algorithm," optik, Elsevier, pp. 3693-3700, 2013.

[14] M. K. •. T. Shah, "A Literature Review on Image Encryption Techniques," 3DR REVIEW, Springer, pp. 5-29, 2014.

[15] v. p. k. k. s. narend k. pareek, "diffusion-substitution based gray image encryption scheme," digital signal processing, Elsevier, 2013.

[16] N. Z. Salim M. Wadi, "Rapid Encryption Method Based on AES Algorithm for Grey Scale HD Image Encryption," in The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013) , Elsevier , 2013.

[17] R. K. G. Nilesh Y. Choudhary, "Partial Image Encryption based on Block wise Shuffling using Arnold Map," International Journal of Computer Applications, vol. 97, no. 10, 2014.

[18] N. S. K. Panduranga H T, "Selective image encryption for Medical and Satellite Images," International Journal of Engineering and Technology (IJET), vol. 5, no. 1, 2013.

[19] D. S. K. ,. K. Panduranga H T, "Partial Image Encryption using block wise shuffling and chaotic map," in Proceedings of International Conference on Optical Imaging Sensor and Security, Coimbatore, Tamil Nadu, India, July 2-3, 2013 , Coimbatore, Tamil Nadu, India, 2013.

[20] c. dong, "color image encryption using one time keyand coupled chaotic system," signal processing: image communication, Elsevier, pp. 628-640, 2014.

[21] A. M. Z. E. A. S. Osama A. KHASHAN, "Performance study of selective encryption in comparison to full encryption for still visual images," Journal of Zhejiang University-SCIENCE , springer, pp. 435-444, 2014.

[22] X. ShiguoLian, "On the design of partial encryption scheme for multimedia content," MathematicalandComputerModelling, Elsevier, pp. 2613-2624, 2013.

[23] M. A. Shahed, "Wavelet Based Fast Technique For Images Encryption," Basrah Journal of Science , p. 127, 2007.

[24] R. R. M. A. M. R. Rasha Elhadary, "Wavelet Based image encryption: a comparative Study," International Journal of Advanced Research in Computer Science, 2014.

[25] G. B. S. Lahieb Mohammed Jawad, "A REVIEW OF COLOR IMAGE ENCRYPTION TECHNIQUES," IJCSI International Journal of Computer Science Issues, vol. 10, no. 6, No 1, November 2013, 2013.

[26] H. C. a. X. Li, "Partial Encryption of Compressed Images and Videos," IEEE TRANSACTIONS ON SIGNAL PROCESSING, vol. 48, no. 8, AUGUST 2000, 2000.

[27] S. C. P. C. F. A. A. Kingston, "LOSSLESS IMAGE COMPRESSION AND SELECTIVE ENCRYPTION USING A DISCRETE," IEEE, 2007.

[28] A. A. Maher Jridi, "A VLSI Implementation of a New Simultaneous Images Compression and Encryption Method," ieee, 2010.

[29] x. w. xinjun zhang, "Chaos-based partial encryption of SPIHT coded color images," signal processing, Elsevier, pp. 2422-431, 2013.

[30] A. u. R. &. X. L. &. A. K. &. S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," Multimed Tools Appl, # Springer Science+Business Media New York , 2014.