AENSI Journals

Australian Journal of Basic and Applied Sciences

ISSN:1991-8178

Journal home page: www.ajbasweb.com

A Review on Different Image Encryption Techniques for Secure Image Transmission

[1]Prof. S. Suresh Raja and [2]Dr. V. Mohan

[1]*Associate Professor, Master of Computer Applications, KLN College of Engineering, TN, India.*
[2]*Professor and Head, Mathematics, Thiagarajar College of Engineering, TN, India.*

ARTICLE INFO

Article history:
Received 19 August 2014
Received in revised form
19 September 2014
Accepted 29 November 2014
Available online 15 December 2014

Keywords:
Image Encryption, Ciphering Algorithms, Spatial and Frequency domains.

ABSTRACT

This paper focuses mainly on the aspects and approaches of design of an image encryption with both full encryption and partial encryption strategy. A common beginning given for cryptography and images encryption, followed by different techniques in image encryption and related works for each technique and the performance parameters used in each encryption are processed and analyzed. Finally, general security analysis methods for encrypted images are mentioned.

To Cite This Article: Prof. S. Suresh Raja and Dr. V. Mohan., A review on different Image encryption techniques for secure Image transmission. ***Aust. J. Basic & Appl. Sci.,*** *8(18): 528-535, 2014*

INTRODUCTION

In recent years, the advances in communication technology have seen strong interest in digital image transmission. However, growth of computer processor possessing power and storage illegal access has become easier. Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities. New methods for protecting the image in transmission are discovered frequently. This paper holds some of those recent existing encryption techniques and its security issues. The performances of all these encryption techniques are deliberately discussed and its performances are measured.

A. Preliminaries:

A.1 Plain Text:

The original message that the person wishes to communicate with the other is defined as plain text. In cryptography the actual message that has to be send to the other end is given a special name as plain text.

A.2 Cipher Text:

The message that cannot be understood by anyone or meaningless message is what we call as cipher text. In cryptography the original message is transformed into non-readable message before the transmission of actual message.

A.2.1 Ciphers:

A cipher encrypts a single letter or group of letter as a unit, regardless of meaning.

A.2.2 Codes:

A code encodes a word or phrase at a time usually in a fixed way (no keys).

A.3 Encryption:

A process of converting plain text into cipher text is called as encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two

Corresponding Author: Prof. S. Suresh Raja, Associate Professor, Master of Computer Applications, KLN College of Engineering, TN, India.

things—an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

A.4 Decryption:

A reverse process of encryption is called as decryption. It is a process of converting cipher text into plain text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non-readable message (cipher text). The process of decryption requires two things—a decryption algorithm and a key. A decryption algorithm means the technique that has been used in decryption. Generally the encryption and decryption algorithm are same.

A.5 Key:

A Key is a numeric or alpha numeric text or may be a special symbol. The key is used at the time of encryption takes place on the plain text and at the time of decryption take place on the cipher text. The selection of key in cryptography is very important since the security of encryption algorithm depends directly on it.

B. Purpose of Cryptography:

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so on. Due to the great security advantages of cryptography it is widely used today.
Following are the various objectives of cryptography.

Confidentiality:

Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

Authentication:

The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

Integrity:

Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

Non Repudiation:

Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

Access Control:

Only the authorized parties are able to access the given information.

D. Classification and Description of Image Encryption Schemes:

In this section, we classify image encryption schemes in two categories.
a. Spatial Domain Schemes
b. Frequency Domain Schemes.

D.1 Spatial Domain:

In the spatial domain method, the pixel composing of image details are considered and the various procedures are directly applied on these pixels. The image processing functions in the spatial domain may be expressed as

$$g(x,y) = T [f(x,y)],$$

where f(x, y) is the input image, g(x, y) is the processed output image and T represents an operation on f defined over some neighborhood of (x, y).Sometimes T can also be used to operate on a set of input images. The spatial domain is the normal image space, in which a change in position in image I directly projects to a change in position in scene S. Distances in I (in pixels) correspond to real distances (e.g., in m) in S. We can also discuss the frequency with which image values change, that is, over how many pixels does a cycle of periodically repeating intensity variations occur. One would refer to the number of pixels over which a pattern repeats (its periodicity) in the spatial domain.

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 528-535

D.2 Frequency Domain:

The frequency domain is a space in which each image value at image position F represents the amount that the intensity values in image I vary over a specific distance related to F. In the frequency domain, changes in image position correspond to changes in the spatial frequency, (or the rate at which image intensity values) are changing in the spatial domain image.

D.3 Difference between Spatial Domain and Frequency Domain:

In spatial domain, we deal with images as it is. The values of the pixels of image change with respect to scene, whereas in frequency domain, we deal with the rate at which the pixel values are changing in spatial domain.

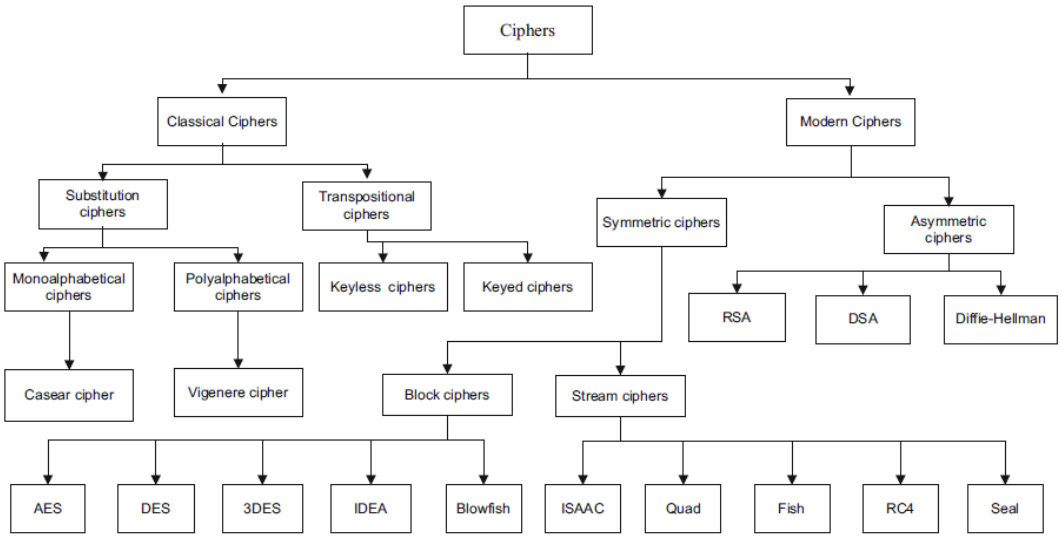

Fig. : Classifications of cryptography algorithm.

E. Literature review of Techniques in Spatial Domain:

Alireza Jolfaei and Abdolrasoul Mirghadri (2010) proposed a technique, in their scheme, they used pixel shuffler and stream cipher to encrypt an image. The pixel rearrangement has two major advantages that are useful for image encryption. It not only rearranges pixel location but also changes the value of each pixel. Confusion is performed by stream cipher itself through nonlinear function operation. Pixel position rearrangement is appropriate before applying encryption, because text has only two neighbors, each pixel in the image is surrounded by eight adjacent pixels. Due to this, each pixel has a lot of correlation with it adjacent pixels. This is very important to disturb the high correlation among image pixels to increase the security level of ciphered images. In order to dissipate the high correlation among pixels, pixel shuffler is used; in which permutation map is applied in two directions: vertical and horizontal, to decrease neighbor pixel correlation. The proposed scheme's key space is large enough to resist all kinds of brute force attack.

In color image encryption Rodriguez-Sahagun, M.T., Mercado-Sanchez, J. B., Lopez- Mancilla, D., Jaimes-Reategui, R., & Garcia-Lopez, J.H. proposed a logistic chaotic map for secure communication in image encryption. They applied Logistic chaotic map in two iterative steps. In 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. As indicated by the execution analysis reported in, it might be presumed that the technique satisfied high security level requirements which worthy encryption speed for variable size of image. The quality of encryption in proposed technique is achieved with moderately small key space. Furthermore it is observed that the original image is independent of the encrypted image with high safety for diverse attacks. The minimum correlation estimation of 0.0013 achieved.

Mastan *et al*. (2011) proposed a nonlinear encryption technique for color image. The method comprise a matrix transformation of pixel diffusion and permutation. It applies diffusion independently on each one channel of color image using both single pixe and block piel. At that point the permutation between three channels R, G, and B is connected interdependently between pixels. This method is designed for sensitive images in medicine and communication. It is faster than AES and could be used continuously in secure image transmission.

In Pareek *et al*. (2011) projected another lossless image encryption algorithm that is based on pixel substitution, which divides the image into blocks of color components. The color part in each one block of the color images is then altered by exclusive-OR operation. The algorithm is simple, fast, yet sensitive to the secret

Australian Journal of Basic and Applied Sciences, 8(18) December 2014, Pages: 528-535

key, because of the key space of that it uses, which makes their technique more suitable for storing/transmitting images of high security prerequisite.

Abugharsa, A. B., & Almangush, H (2011). proposed a method of shifting the rows and columns of an image. Using hash function the original image is partitioned into blocks of 3 9 15 and the shifting table is stored in the shifting table. Further the pixels are shifted through rows and columns before scrambling. The experiment results shows that that there is a close relationship between the original image and the encrypted image, which is affirmed by the correlation coefficient value i.e., −0.0078. It evidenced that the neighborhood pixels in the unique image have nearest value than the neighborhood pixels of the encrypted image, that the consistency in the proposed method is low.

Yadav, R. S and his colleague (2013) proposed a method by combining both shift image blocks and AES. The image is shifted as a block with a help of hash table. The shifted image is again shuffled by AES encryption algorithm. Their technique shows the capability to scramble expansive data sets proficiently and progressively, since the NPCR and UACI values are close standard values, which are 99.6689, and 27.7599 %, respectively. The correlation value of the original image has nearest values between its neighborhoods than the encrypted image neighborhood pixels, which is proof of less consistency by outsider. Confidentiality is a issue in transmitting advanced images over open systems such as internet. The proposed technique is a well suit in image encryption among various plans. Chaos confusion based methodology has recommended quick, efficient and very secure algorithms.

Zhang, G., & Liu, Q. (2011). Offered a method that, as of late an efficient image encryption system based on chaos and permutation–diffusion structural planning is recommended. On the other hand, the plain message affectability, as reported by the creators, is not fulfilling and it is proposed to repeat the algorithm more than twice to get a decent capacity to oppose differential attack. The point of this paper is to push the plain-message affectability of their methodology. Subsequently, the dispersion execution is significantly upgraded and the general security of the image cryptosystem is made strides.

Ding, X., & Chen, G. (2014). Proposed a method of multiplexing the position of the pixels and truncating the operation stage. Its better among color image encryption technique where the inventors crate a procedure of multiplexing the position to encode the image in the spatial channel. Then, the proposed strategy can keep up the nonlinear characteristics for the cryptosystem and evade different sorts of the presently existing attacks, particularly the iterative attack. Activity results displayed to show the security and force execution of the method. It considers a better among the optical color image encryption.

Zhang, Y., & Xiao, D. (2014). Proposed a new image encryption method focused on rotating in matrix bit-level permutation diffusion in blocks. The proposed technique divide the plain image into 8 9 8 pixels blocks with a random matrix, then shuffling each one block into a 8 9 8 9 8 three dimensional parallel matrix, which has six sides as a cube. Permutation is performed by rotating the 3-D matrix that depends on plain image as per various heading. Further the proposed technique diffuse the pixel block to further change that measures the attributes of image after confusion. Experimental results analysis and demonstrate that the method can attain an attractive security execution as well as have a suitable mode in parallel of robustness against noise in corresponding systems.

F. Literature review of Techniques in Frequency Domain:

Lala Krikor, Sami Baba, Thawar Arif, and Zyad Shaaban (2009) proposed a method od decomposing the image into 8 * 8 blocks. The decomposed blocks are transformed to frequency domain from spatial domain by DCT. Then, the DCT coefficients correlated to the higher frequencies of the image block are encrypted using Non-linear Shift Back Register. The concept of ciphering the selective DCT coefficient is based on the fact that the image details are positioned in higher frequencies while the human is most perceived to lower frequencies than to higher frequencies. The proposed method is lossless, hence the information of the images is highly important , and any information loss is not allowed. It is tunable as different level of security can be achieved by selecting different bits for encryption. Variable visual degradation is achieved in the proposed technique. It is compression friendly. To increase the security, the repositioning of blocks is applied after encryption.

Shaimaa A. El-said, Khalid F. A. Hussein and Mohamed M. Fouad (2010) proposed a method as Optimized Multiple Huffman Table for a secure and computational algorithm. The method developed on using a numerical model based compression to generate various tables of the same data type of images or videos. . The tables of the images are used to encrypt and to increase the compression efficiency and security. High visual degradation can be achieved in the proposed technique. No impact is observed on compression efficiency. It is resistant against various types of attack including cipher text only attack and known/chosen plaintext attack. The encryption ratio is 100% in the proposed technique.

Zhou, N., Wang, Y., Gong, L., Chen, X., & Yang, Y. (2012). expressed the technique of image encryption in three ways called color space rotation. The color is initially turned to new through converting the color image from RGB space to RGB Supplement space. The indivual color spot of each pixel is transformed using the proposed preserving transform of Mellin technique on distinctive request of image. On achieving the high

security, the shuffling if pixels is done 3D. The proposed method use a vast key space makes the algorithm a sensitive to security risk. .

Abuturab and his team (2012) proposed a system that secures color images built in light of Arnold transform in gyrator transform domain. For their strategy, the color image is divided into their individual R, G and B parts and then the individual segment will be independently encrypted by applying first random phase mask and then first-order Arnold transform and finally, the gyrator transform. The second random phase mask will be put 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 utilized in the proposed technique and utilized as extra keys within the encryption and unscrambling, which may likely offer vigor against impediment assaults and clamor assaults and high security.

In (He, Y., 2012), a single channel color image encryption system was proposed. The strategy will be built with respect to orthogonal composite grating and twofold random phase encoding. A color image first will be deteriorated into R,GandBparts, which accordingly will be adjusted into an orthogonal composite grating. The twisted composite grating is then encrypted by a regular twofold random phase encryption method. It will be watched that combining the two-fold random phase encoding and orthogonal composite grating decreases the multifaceted nature and cost of encryption.

Sinha *et al*. (2013) proposed another strategy for gray scale image encryption using 3D jigsaw transform. To start with, the image is transformed to bit planes, where every bit plane is separated into more diminutive blocks. The 3D jigsaw transform translocate each block to diverse area in 3D square. They utilized two fractional Fourier transforms (FRFT), the first FRFT is utilized to encode image, and the yield is then reproduced with a random stage code, while the second FRFT is utilized to obtain the encrypted image. By using FRFT and the random stage codes, security is given.

Chen, H., Du, X., Liu, Z., & Yang, C. (2013) proposed a color image encryption algorithm that uses the affine transform in the gyrator transform domains, was proposed. Firstly, the affine transform is connected on the RGB parts of the color image and the real and imaginary parts of their frequency segment are concentrated. Second, the R, G, B image pixel qualities are interchanged by scrambling using a random angle approach. Then, the resulting image is transformed using the gyrator transform and mixed again by a second affine transform. Their test results indicated that high security is attainable by using proposed algorithm.

Sui, Liansheng, & Gao, Bo. (2013), A solitary channel color image encryption is proposed focused around iterative fractional Fourier transform and two-coupled logistic map. Firstly, a gray scale image is constituted with three channels of the color image, and permuted by a succession of chaotic sets which is created by two-coupled logistic map. Firstly, the permutation image is deteriorated into three parts once more. Furthermore, the first two parts are encoded into a solitary one focused around iterative fractional Fourier transform. Essentially, the interim image and third part are encoded into the final gray scale cipher text with stationary white noise distribution, which has camouflage property to some degree. At present encryption and portrayal, chaotic permutation makes the ensuing image nonlinear and disorder both in spatial domain and frequency domain and the proposed iterative fractional Fourier transform algorithm has quicker united rate. Furthermore, the encryption plan amplifies the key space of the cryptosystem. The simulation results and security dissection confirm the achievability and adequacy of this system.

Liu, Z., Li, S., Liu, W., Wang, Y., & Liu, S. (2013). A new proposed chaotic image encryption algorithm proposed to upgrade the security of double random phase encoding. For this a sort of amplitude scrambling operation is outlined and brought into an image encryption process. In the second phase of masking a random information is additionaly utilized for scrambling appropriation so as to spare the space of capacity and transmission of the key data. The scrambling operator is unpredictable for producing the key. Some numerical reproductions have been accommodated trying the legitimacy of the image encryption plan

Li, H., Wang, Y., Yan, H., Li, L., Li, Q., & Zhao, X. (2013), proposed a new method in double image encryption is proposed in chaos based pixel scrambling and further transformed by using gyrator transformation. Two unique images are first viewed in the e amplitude and phase of a complex capacity. Arnold transform is utilized to scramble pixels at a neighborhood complex capacity, where the position of the mixed territory and the Arnold transform recurrence are created by the standard map and logistic map separately. At that point the changed complex capacity is changed over by gyrator transform. The two operations specified in the proposed technique will be executed iteratively. The framework parameters in neighborhood pixel scrambling and gyrator transform serve as the keys of this encryption algorithm. For legitimacy and the security of the proposed technique the numerical reenactment has been performed.

Xingyuan Wang⇑, Dapeng Luan,In their paper, we propose an image encryption algorithm that based on chaos combined with reversible cellular automata which show complex behaviors and have large rule space. The pixels are permuted by the intertwining logistic at the same time change values of pixels. Through reversible cellular automata, the cipher is generated after many rounds on bit-level. Experimental results and security analysis for the proposed algorithms show that our scheme has perfect information protection ability, and satisfied the confusion and diffusion request in cryptosystem.

Sui, L., Xin, M., Tian, A., & Jin, H. (2013). A single-channel color image encryption is proposed focused around a phase recover algorithm and a two-coupled logistic map. Firstly, a gray scale image is constituted with three channels of the color image, and then permuted by an arrangement of chaotic sets created by the two-coupled logistic map. Also, the permutation image is deteriorated into three new parts, where every part is encoded into a phase only capacity in the fractional Fourier space with a phase recover algorithm that is proposed focused around the iterative fractional Fourier transform. At last, a between time image is shaped by the synthesis of these phase-only capacities and scrambled into the final gray scale cipher text with stationary background noise by utilizing chaotic diffusion, which has camouflage property to some degree. At the present time encryption and unscrambling, chaotic permutation and diffusion makes the resultant image nonlinear and issue both in spatial space and recurrence area, and the proposed phase iterative algorithm has speedier joined velocity. Moreover, the encryption plan augments the key space of the cryptosystem. Experimental results and security examination check the practicability and viability of this technique.

G. Parameters Used For Security Analtsis:

Security analysis is the art of find the weakness of a cryptosystem and retrieval whole or a part of a ciphered message (in this area, an image) or finding the secret key without knowing the decryption key or the algorithm. There are many techniques for applying analysis, depending on what access the analyst has to the plaintext, ciphertext, or other aspects of the cryptosystem.
Below are some of the most common types of attacks to encrypted images:

1.Key Space Analysis:

K**ey space** refers to the set of all possible keys that can be used to generate a key, and is one of the most important attributes that determines the strength of a cryptosystem. The number of try to find directly refers to key space of the cryptosystem grow exponentially with increasing key size. It means that doubling the key size for an algorithm does not simply double the required number of operations, but rather squares them. An encryption algorithm with a 128 bit in key size defines a key space of 2128, which takes about 1021 years to check all the possible keys, with high performance computers of nowadays. So a cryptosystem with key size of 128 bit omputationally looks robust against a brute force attack.

2. Statistical Analysis:

Statistical analysis exhibits the relation between the original image and encrypted image. The encrypted image should be completely different from the original image. Due to Shannon theory. It is possible to conclude many kinds of ciphers by statistical analysis. This analysis will determine whether the ciphered image reveals any information about the original one or not.

3. Correlation Analysis:

Two adjacent pixels in a plain image are strongly correlated vertically and horizontally. This is the property of an image, the maximum value of correlation coefficient is 1 and the minimum is 0, a robust encrypted image to statistical attack should have a correlation coefficient value of 0.

4. Differential Analysis:

The aim of this experiment is to determine the sensitivity of encryption algorithm to slight changes. If an opponent can create a small change (e.g. one pixel) in the plain image to observe the results, this manipulation should cause a significant change in the encrypted image and the opponent should not be able to find a meaningful relationship between the original and encrypted image with respect to diffusion and confusion, the differential attack loses its efficiency and become useless.

5. Key Sensitivity Analysis:

In addition of large enough key space to resist a cryptosystem at brute force attack, also a secure algorithm should be completely sensitive to secret key which means that the encrypted image cannot be decrypted by slightly changes in secret key

Conclusion:

In this paper, we have analyzed various existing image encryption approaches and by classification different types of work using other techniques than encryption. These techniques were compression, selection, chaos maps, public key and digital signature which applied to improve and enhance the efficiency of an image encryption algorithm. Finally, the parameters used for security analysis for encrypted images are given which use to evaluate the robustness of a cryptosystem.

REFERENCES

Abugharsa, A.B., H. Almangush, 2011. A new image encryption approach using block-based on shifted algorithm. International Journal of Computer Science and Network Security (IJCSNS), 11(12): 123-130.

Abuturab, M.R., 2012. Securing color information using Arnold transform in gyrator transform domain. Optics and Lasers in Engineering, 50(5): 772-779.

Alexopoulos, C., N. Bourbakis, N. Ioannou, 1995. Image encryption method using a class of fractals. Journal of Electronic Imaging, 43: 251-259.

Alireza Jolfaei and Abdolrasoul Mirghadri, 2010. "An image Encryption approach using Chaos and Stream Cipher", Journal of Theoretical and Applied Information Technology, 19(2): 117-123.

Chen, H., X. Du, Z. Liu, C. Yang, 2013. Color image encryption based on the affine transform and gyrator transform. Optics and Lasers in Engineering, 51(6): 768-775.

Dang, P. and P.M. Chau, 2000. Hardware/software implementation 3-Way algorithm for image encryption, Security and Watermarking of Multimedia Contents II, volume 3971 of Proceedings of SPIE, pp: 274-283.

Dang, P. and P.M. Chau, 2000. Image encryption for secure internet multimedia applications, IEEE Transaction on Consumer Eletronics, 46(3): 395-403.

Dang, P. and P.M. Chau, 2000. Implem1entation IDEA algorithm for image encryption, Mathematics and Applications of Data/Image Coding , Compression and Encryption, volume 4122 of Proceedings of SPIE, pp: 1-9.

Ding, X., G. Chen, 2014. Optical color image encryption using position multiplexing technique based on phase truncation operation. Optics & Laser Technology, 57: 110-118.

Furht, B. and D. Kirovski, 2005. Multimedia Security Handbook, CRC Press, USA.

Furht, B., E. Muharemagic and Daniel Socek, 2005. Multimedia encryption and watermarking, Springer.

He, Y., Y. Cao, X. Lu, 2012. Color image encryption based on orthogonal composite grating and double random phase encoding technique. Optik (International Journal for Light and Electron Optics), 123(17): 1592-1596.

Jolly Shah and Dr. Vikas Saxena, 2011. Performance Study on Image Encryption Schemes IJCSI International Journal of Computer Science Issues, 8(4): 1.

Lala Krikor, Sami Baba, Thawar Arif and Zyad Shaaban, 2009. " Image Encryption using DCT and Stream Cipher," European Journal of Scientific Research, 32(1): 47-57.

Li, H., Y. Wang, H. Yan, L. Li, Q. Li, X. Zhao, 2013. Double-image encryption by using chaos-based local pixel scrambling technique and gyrator transform. Optics and Lasers in Engineering, 51: 1327-1331.

Liu, Z., S. Li, W. Liu, Y. Wang, S. Liu, 2013. Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding. Optics and Lasers in Engineering, 51: 8-14.

Majid Khan, Tariq Shah, 2014. A Literature Review on Image Encryption Techniques Springer online publishing.

Mastan, J.M.K., G.A. Sathishkumar, K.B. Bagan, 2011. A color image encryption technique based on a substitution–permutation network. Advances in Computing and Communications, 4: 524-533.

McCanne, S. and V. Jacobson, 1995. A flexible framework for packet video, Proceedings of 3rd ACM International Conference on Multimedia, pp: 511-522.

Pareek, K.K.S., K. Narendra, V. Patidar, 2011. A symmetric encryption scheme for colour BMP images. International Journal of Computer Applications, Special Issue on Network Security and Cryptography, 42-46.

Rodriguez-Sahagun, M.T., J.B. Mercado-Sanchez, D. Lopez-Mancilla, R. Jaimes-Reategui, J.H. Garcia-Lopez, 2010. Image encryption based on logistic chaotic map for secure communications. IEEE Electronics, Robotics and Automotive Mechanics Conference, pp: 319-324.

Shaimaa A. El-said, Khalid F.A. Hussein and Mohamed M. Fouad, 2010. "Securing Image Transmission using In-compression Encryption Techniques," International Journal of Computer Science and Security", 4(5): 466-481.

Sinha, A., K. Singh, 2013. Image encryption using fractional Fourier transform and 3D Jigsaw transform. Retrieved from http://pdf-world.net/pdf-2013/ Imageencryption-using-fractional-Fourier-transform-and-3DJigsaw-transform-pdf.pdf.

Sui, L., M. Xin, A. Tian, H. Jin, 2013. Singlechannel color image encryption using phase retrieve algorithm in fractional Fourier domain. Optics and Lasers in Engineering, 51: 1297-1309.

Sui, Liansheng, Gao, Bo, 2013. Single-channel color image encryption based on iterative fractional Fourier transform and chaos. Optics & Laser Technology, 48: 117-127.

Xingyuan Wang⇑, Dapeng Luan, 2013. A novel image encryption algorithm using chaos and reversible cellular automata Commun Nonlinear Sci Numer Simulat, 18: 3075-3085.

Yadav, R.S., M.H.D.R. Beg, M.M. Tripathi, 2013. Image encryption techniques: A critical comparison. International Journal of Computer Science Engineering and Information Technology Research, 3(1): 67-74.

Zhang, G., Q. Liu, 2011. A novel image encryption method based on total shuffling scheme. Optics Communication, 284: 2775-2780.

Zhang, Y., D. Xiao, 2014. An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Communications in Nonlinear Science and Numerical Simulation, 19: 74-82.

Zhou, N., Y. Wang, L. Gong, X. Chen, Y. Yang, 2012. Novel color image encryption algorithm based on the reality preserving fractional Mellin transform. Optics & Laser Technology, 44(7): 2270-2281.