Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 13, February 2018 – www.caeaccess.org

An Extensive Survey on Image Security Research Trends

Naveen M.
Research Scholar
Acharya Institute of Technology, Bengaluru, India

G. N. K. Suresh Babu, PhD
Department of Computer Science and Engineering,
Acharya Institute of Technology, Bengaluru, India

ABSTRACT
The digital revolution of the world along with the fast communication system and the technical advancement of the digital images provide the easiest way to communicate data in the form of Images. There are many open threats and risk involves if these image data is compromised. This paper provides a theoretical study of existing methods for the image security. The archival works from IEEE, Elsevier, Springer and some other relevant articles are considered to do literature study of the problem formulation, algorithms and performance metrics. Various aspects of data integrity, privacy, and attacks are also discussed in this paper. The organized outcome is contributory to the researchers, industry, and academician who keep interest in image security domain.

Keywords
Image Security, Image Encryptions, Image Attacks.

1. INTRODUCTION
Recently multimedia data is moving mostly to the destinations over on internet in the different forms of image, text, video, and audio. The digital communication over the internet, everything is accessible and visible to every user. Hence data security is a very critical concern in the today's communication era. The data security is necessary to provide i) Privacy, ii) Integrity and iii) Accessibility. The data privacy is provided to secure the data against the unauthorized access of the user. The integrity represents the correctness of data and accessibility presents that data can be access for official use. To achieve image security, privacy over wireless communication encryption mechanism is a must. The encryption techniques help to encrypt the original image and convert it into an unreadable format where it will be hard to recognize the image without providing the authenticity [1].

The actual reason for encrypting the image is to keep a secret between users, another way, it is important to secure to avoid the terrorism misleading or piracy the contents of the image. The additional advantage of encryption algorithm is to discover the applications in secure storage, broadcasting and dependability of digital images which is very important in the field of military, infrastructure, medical imaging methods and private video conferencing, etc. The basis on the number of security keys utilized to encrypt/decrypt data; cryptographic algorithms are classified as asymmetric algorithms (public key) and symmetric algorithms (secret key). Only one key will be used for encryption and decryption the data into the symmetric key [2].

This key must be distributed before the transmission entities. Thus in symmetric encryption key plays a major role. The efficiency factor of this encryption depends on the key size used, and the weakness of symmetric algorithms is in the distribution of symmetric key between both sender and receiver. The symmetric key cryptography algorithms which include i) Reverse Cipher (RC)-2, ii) DES, iii) 3DES, iv) RC5, AES, and Blowfish, which utilizes certain- or variable-length key. Further, the symmetric key algorithm is categorized as block ciphers (AES, Blowfish) which work on blocks of a precise length and stream ciphers (RC4, Salsa20) that work bitwise over the data. A stream cipher (SC) may be perceived as a block cipher along with block length of 1-bit.Asymmetric cryptography has two key which is a) Public key, b) Private Key. The public key should be shared with everyone which is one key in the pair, and another key in the pair kept a secret is known as a private key. Another way, the usual complete encryption algorithms are utilized to fully encrypt an image and treat entire bits also; it has greater computational difficulty than partial encryption. Also, it takes maximum time for assessment with partial encryption. Thus, the selective encryption mechanism is required for multimedia data. For example: in military and law enforcement. However, some applications need lower security levels like in medical images [3].

This paper discusses the image encryption techniques meant to secure the image. The flaw of the paper is given with following sections: Section 2 discusses the image, image security and encryption techniques. The reviews on existing researches were discussed in Section 3. Section 4 expresses the research gap in providing the image security. Section 5 elaborates the statistical researches performed till now in image security mechanisms. Finally, the conclusion is given in Section 6.

2. BACKGROUND
This section discusses the basic concepts of image, the necessity of the image security over the internet, significances of encryption mechanism and different type image attacks, cryptography techniques and security services evolved.

2.1 About Image
A digital image is nothing more than data- where numbers are pointing differences of a) red, b) green and c) blue at a particular area over a grid of pixels. May occasion, we saw these pixels as small rectangles sandwiched together on a computer screen. With a small creative thinking and several lower level manipulations of pixels with code, but, we may present that information in a countless of ways. Images may be separated into the two categories, which is i) Grayscale image and ii) Color image. An explanation of gray image scale images exhibits only gray shades any color while if the no color information is considered as color images [4]. Figure 1 presents the well-known picture of Lena as a binary image (consists of black and white color only), gray scale image (consists of shades of gray ranging from [0-255] i.e. range

from black-shades of gray-white) and RGB colored image (consists of 3 individual components R, G and B) [4].

Figure 1 a) Binary, b) Gray-scale and c) RGB color image

In current applications as well as in future applications image data will be transferred as it happens today in social network sites such as Face book, Twitter, and Flicker, where one user shares image with many another friends [5, 6, 7, and 8]. Unfortunately, user's privacy may leak if they allowed comment, post, and tag a photo on the social network. The social network may pose a variety of serious security risk and threats to the users. This paper represents an in-depth detail of threats, security risks and various kinds of attacks by using social media [9].

2.2 Image Encryption

The interest towards the image security is increased nowadays due to advancement in image manipulation techniques. Also, many of the research organizations as well as research communities are working on improving the image security against such manipulation techniques [10]. These encryption mechanisms are mainly categorized into symmetric and asymmetric mechanisms [11, 12]. Researchers [13] introduced the Rivest Shamir and Adleman [14] RSA algorithm. This is observed that most of the encryption techniques are not efficient for the image applications, for the traditional encryption some fundamental features of images which are called as bulk data capacity and the information with high redundancy cause some troublesome. These encryption techniques demand some extra operations which apply to the compressed image data and require high computational power and computational complexity. With encryption, the proper latency can be introduced due to their slow encryption and decryption process.

An Innovative encryption method should be developed for valuable data encryption for economic organizations like multi-media applications and E-commerce. For future Internet applications over wireless networks, encryption methods for multimedia applications should be studied as well as developed. The primary objective of the encryption technique is to transform the information/data where only the authorized person can change the content. A discretely valued cryptography technique can be defined as.

- A group of possible cipher texts, C.
- A group of possible cipher keys, K.
- A group of possible encryption and decryption techniques, E and D.

An encryption technique which is also known by a cipher where the message for the encryption is called plaintext and the message which is encrypted is called cipher text. Here the cipher text and the plain text have been denoted by Ct and Pt respectively, and the encryption technique of the cipher can be defined as:-

$$Ct = Eke (Pt)$$

Where Eke is the key of encryption and E is the function which is used for encryption. Hence, the decryption can be defined as below:-

$$Pt = Dkd (Ct)$$

Here, the decryption key can be indicated with “Dkd” and D is the function of decryption. The cipher security needs to rely on Dkd. Figure 2 illustrates the block representation of encryption/decryption process.

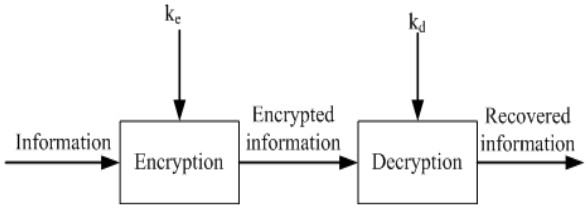

Figure 2 Block of encryption/decryption process

There are some techniques which are used for image security [14]:

In cryptographic encoding, encryption is a conversion of data or information which cannot be read without a key. Encrypted data appears meaningless and is very difficult for unauthorized parties to decrypt without the proper key. There are two ways to do encryption:-

2.2.1 Shared Secret Encryption

The first type of encryption demonstrates secret encryption or symmetric cryptography. It is set to encryption utilizes a secret key to scramble the data into un-readable form [15].

The user from another side requires the same key to read the data. The following Figure.3 represents the symmetric cryptography because the similar key is employed for both encryption and decryption (see figure 3).

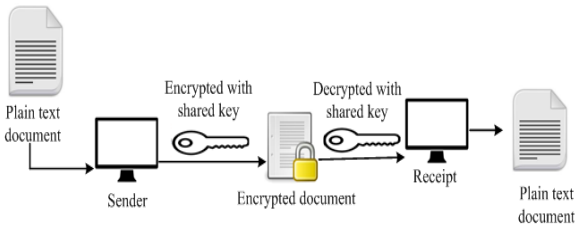

Figure 3 illustrates Symmetric Cryptography

2.2.2 Asymmetric Cryptography

Asymmetric cryptography (AC) is used for one-way purposes. Regarding mathematics, these are functions that are effortless to calculate in one direction however very hard to calculate in reverse. This permits the public key to distribute, which is obtained from the private key. It is extremely hard to work backward and establish the private key. A general one-way function utilized today is factoring huge prime numbers which are multiplication of two numbers. The following Figure.4. Indicates the asymmetric cryptography.

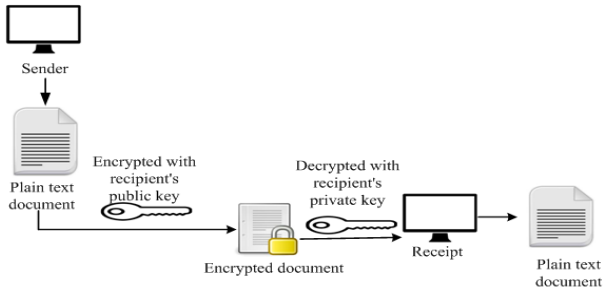

Figure 4 Demonstrates the structure of Asymmetric Cryptography (Public Key)

3. LITERATURE SURVEY

This existing section work illustrates encryption techniques for image security.

This significant work towards image security presented by **Tao et al. (2010)** Where the image encryption depends on multi-order Fractional Fourier Transformation (FRFT). Addition of various orders Inverse Discrete Fractional Fourier Transformation (IDFRFT) of the Interpolated sub-images, creates an Encrypted image and where as it offers to recover original image using a linear system designed by the Fractional Fourier Domain Analysis(FDA)of interpolation of sub-images.**[17]**

Also, the work conducted by **Zhang et al. (2011)** proposed a method in which image encryption is constructed by pseudo-random permutation and also does two works: lossy-compression and Iterative Reconstruction. In which image is first to encrypt then compressed and finally re-constructed which offers the better security and sharpen the original image. **[18]**

In Zhang (2011) provides another method that is Reversible Data Hiding (RDH), which enhance the security level in the encrypted image. In this image is encrypted by Stream cipher, and merges some embedded data after reconstructed the small area of the encrypted image. This algorithm shows the original image contains the embedded data and can only recover by using an encryption key. **[19]**

Similarly the paper demonstrated by Hong et al. (2012) [20] on the modification of Reversible Data Hiding [RDH] Technique in image encryption, with consideration of pixel co-relations in border of side blocks and also reduce the complications and errors of data extraction from Traditional RDH concept which have been proposed by **Zhang [19].** This theory uses Side-match pattern to reduce the error the error rate of extracted bits. Encrypted data is dived into blocks and carries single bit by snapping three lower sized blocks (LSD) of the existing pixel. After Examine the block smoothness, the bit extraction, and image recovery can be achieved. **[19]**

A new concept on image security is proposed by the **Elshamy** et **al. (2013)** which Encrypt optical image by chaotic baker map (CBM) and Double Random Phase Encoding (DRPE). This method is divided into two layers, the first layer called as pre-processing layers and is worked with CBM on the original optical image and the Second layer is implemented with DRPE. The method used in this model increases the security level of DRPE and also avoid the environmental noise [21]. **In Li et al. (2013)** presented a new concept of Advanced Encryption Standard (AES) is used to generate independent round key by the 2D Chaotic map which includes 2D Henon map and 2D Chebyshev map to provide high level security and to overcome the defects of old AES algorithm. The result shown by them is that this algorithm has provided better for image encryption. **[22]**

The paper presented by Hafiz et al. (2014) a new concept on image encryption system which combines Fractal in encrypted source images using single-fractal and multi-fractal. In which the image content is converted into the complex design of Fractal images. The presented scheme of Fractal technique achieves a higher order of potential among various other techniques [**23].**

In Wadi et al. (2014) focuses on improvement of security of multimedia data and data storage, which avoid unauthorized, unofficial and illegal accessing over a network. This theory provides fast and high-security approach. The image is decomposed to Binary coded decimal (BCD), where the bit planes reconstructed and a simple scrambling operation has been used to shuffled bit-planes. Under this scheme of encryption, the algorithm achieves higher security for protecting multimedia data over a network and can avoid common types of attacks and reduces the time complexity of encryption and decryptions operations [24].

By Ye et al. (2016) have resented a significant method to achieve better and strong security on protecting private and un-authorized access of images, which is transmitting over the internet and wireless networks. This procedure consists diffusion procedure depends on auto-blocking Technique and Electro-cardio-graph (ECG) rays. Based on many experiments and theoretical analysis it is observed that this method provides better and efficient security and can resist many attacks [25].

In Li et al. (2016)proposes a method to encrypt the multiple images by using Modified Logistic Map which utilizes Compressive Ghost Imaging(CGI) and co-ordinate Sampling, which achieved higher efficiency of data transmission and also applicable on multiple image encryption and decryption.[26]

Similarly Liu et al. (2015) represents that N-phase logistic sequence is independent and distributed uniformly which having high complexity and good randomness order, uses combined algorithm of logistic map and non-symmetric partition, which suggests that this method is arrived with high-security level for image encryption and also able to resist the attacks[27]. **Bao et al. (2018)** presented a new approach for image security, where the image encryption and sharing matrix is utilized. The presented scheme of secrete image sharing achieves higher order of security against different attacks [28].

Wu et al. (2017) focus on improvement of security levels of Chaotic Tent Maps (CTM) which offers better security. In this, the image encryption mechanism is introduced which utilizes both the CTM concept as well as rectangular transform. The security analysis of the proposed model suggests that the drawbacks of the pure CTM are eliminated [29]

Also, Huang et al. (2016) offer the new approach to encrypt the color image. They have given formula which uses the Logistic mapping and DRPE. In this, the color image pixel is divided into three components (Red, Green, and Blue) by logistic mapping and then it encrypted by DRPE. Here it is shown that this algorithm keeps high potential to defeat the

common types of attacks and provide better security [30]. **Lastly, the paper proposed by Jiang et al. (2018)** introduced data hiding (reversible) approach in encrypted domain. In this embedded data are extracted from encrypted image and image is reconstructed without losing data. This show the original content of image remains protected and provides a good level of security [31].

4. PARAMETERS OF ENCRYPTION TECHNIQUES

The security analysis of an image is performed to understand the weak points of the cryptosystem and it composes retrieval of image or part of it or detecting the secret key without knowing the description key. There are many techniques exist for analyzing the security techniques and are given below:-

- **Statistical Technique:** This technique is builds the relation among the encrypted image and unique key. Thus, the encrypted image look alike the original image. By using the theory of Shannon, different issues of security can be tackled with statistical technique. This technique analyzes the degree of image security.
- **Differential Technique:** This helps to analyze the encryption algorithm sensitivity. In case the recipient generates any change in the image then this manipulation also need to be encrypted.
- **Correlation Technique:** Here, the property of image is observed with correlation value of 0 and 1 and the tough encryption must have value of 0.
- **Key Space Technique:** This is used to analyze the number of tries performed to get the description key.

5. STATISTICS OF RESEARCHES IN IMAGE ENCRYPTION

The researches published in image encryption are discussed in this section. These statistics were collected from IEEE and Springer publications by giving the keyword "image encryption" (cited on 18/01/2018 at 7 PM). The following table 1 illustrates the statistics obtained from IEEE publications.

Table 1 Statistics on image encryption (IEEE)

Type	Count
Conferences	3017
Books	1
Early access articles	24
Journals and Magazines	262
Standards	1

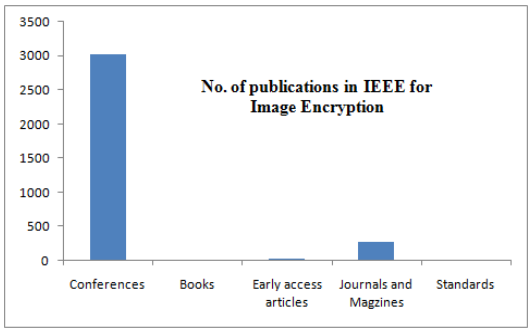

Figure 5 Plot of statistics (IEEE)

The above plot illustrated in Figure 5. Expresses the statistic obtained from IEEE publication.

The following table.2 illustrates the statistics obtained from IEEE publications.

Table 2 Statistics on image encryption (Springer)

Type	Count
Books	90351
Web pages	46
Journals	90
Series	50

The above plot illustrated in Figure. Expresses the statistic obtained from Springer publication.

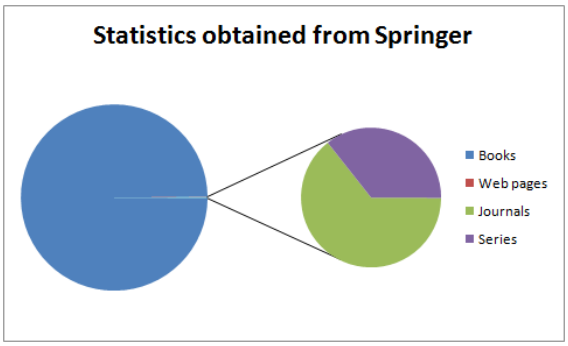

Figure 6 Plot of statistics (Springer)

The above plot illustrated in Figure 6. Expresses the statistic obtained from Springer publication.

6. RESEARCH GAP

The research gap of the domain of image security techniques discussed in this paper can be broadly discussed as below: It is not yet confirmed whether watermarking algorithm should be kept hidden from the attackers. It is dissimilar from cryptography technique and needs special security evaluation metrics. Otherwise, most of the existing watermarking algorithms are bound to be affected by the attackers.

Some algorithms are inclined to certain techniques while they are in a stage where facing trouble with some operations such camera captures, scaling and transformation, etc. Forgery detection techniques are being used now, the accuracy of correct detection is still not fair enough so that it can be applied in the practical applications. One important reason is the obtain ability of large natural mass media variety. The availability of so many sources and contents associated with

the media that have some difficulties to design a model of fixed classifier or decision verge.

A biometric system results cannot be provable as biometrics complex has a property such as variability.

7. CONCLUSION

Ease of access to open network and internet has created a risk for security of digital images which are used in transmission, publishing, and storage. In this paper, it has been surveyed for prevailing research on image encryption using new approach of classifying different type of work using different techniques and more than only encryption. These techniques include compression, chaos mapping, selection, digital signature and public key, which are applied to enhance and increase efficiency of an image encryption algorithm. To evaluate robustness of a cryptosystem general security analyzing techniques foe encrypted image is used. In future concentration is on designing a framework that could address the research gap explored in the study.

8. REFERENCES

[1] E.M. Perse, and J. A. Courtright, "Normative images of communication media mass and interpersonal channels in the new media environment," *Human communication research*, vol. 19(4), pp.485-503, 1993

[2] I. Ozturk and I. Sogukpinar, "Analysis and comparison of image encryption algorithm," *Journal of transactions on engineering, computing and technology*, pp.38, 2004

[3] S. Charbathia and S. Sharma, "A Comparative Study of Rivest Cipher Algorithms," *International Journal of Information & Computation Technology*. ISSN 0974-2239, vol. 4, pp. 1831-1838, Retrieved on 22nd Jan 2018

[4] A.P. Parameshwaran, W-Z.Song, "Encryption Algorithms for Color Images: A Brief Review of Recent Trends," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 10, 2016

[5] K. Xu, Y. Guo, L. Guo, Y. Fang and X. Li, "Control of photo sharing over Online Social Networks," *2014 IEEE Global Communications Conference*, Austin, TX, 2014, pp. 704-709.

[6] K. Liang, J. K. Liu, R. Lu, and D. S. Wong, "Privacy Concerns for Photo Sharing in Online Social Networks," in *IEEE Internet Computing*, vol. 19, no. 2, pp. 58-63, Mar.-Apr. 2015.

[7] K. Xu, Y. Guo, L. Guo, Y. Fang and X. Li, "My Privacy My Decision: Control of Photo Sharing on Online Social Networks," in *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 2, pp. 199-210, March-April 1 2017.

[8] J. Yu, D. Joshi and J. Luo, "Connecting people in photo-sharing sites by photo content and user annotations," *IEEE International Conference on Multimedia and Expo*, New York, NY, pp. 1464-1467, 2009

[9] R. S. Kunwar and P. Sharma, "Social media: A new vector for cyber attack," *International Conference on Advances in Computing, Communication, & Automation (ACCA) (Spring)*, Dehradun, 2016, pp. 1-5.

[10] D.W. Hill and J.T. Lynn, "Adaptive system and method for responding to computer network security attacks," *U.S. Patent No*. 6,088,804. 11 Jul. 2000.

[11] C. Kaufman, R. Perlman, and M. Speciner, "Network security: private communication in a public world," *Prentice Hall Press*, 2002.

[12] D.G. Amalarethinam and J. S. Geetha, "Image encryption and decryption in public key cryptography based on MR," In *Computing and Communications Technologies (ICCCT), 2015 International Conference on*, pp. 133-138. IEEE, 2015.

[13] N. Khanna, J. Nath, J. James, S. Chakraborty, A. Chakrabarti and A. Nath, "New Symmetric Key Cryptographic Algorithm Using Combined Bit Manipulation and MSA Encryption Algorithm: NJJSAA Symmetric Key Algorithm," *2011 International Conference on Communication Systems and Network Technologies*, Katra, Jammu, 2011, pp. 125-130.

[14] K. H. Chang, Y. C. Chen, C. C. Hsieh, C. W. Huang and C. J. Chang, "Embedded a low area 32-bit AES for image encryption/decryption application," *2009 IEEE International Symposium on Circuits and Systems*, Taipei, 2009, pp. 1922-1925.

[15] D. Anggraini and F. Kazhimi, "Encryption on Grayscale Image For Digital Image Confidentiality Using Shamir Secret Sharing Scheme," In *Journal of Physics: Conference Series*, vol. 710, no. 1, p. 012034. IOP Publishing, 2016.

[16] S. Anandakumar, "Image Cryptography Using RSA Algorithm in Network Security," *International Journal of Computer Science & Engineering Technology* 5, no. 9, 2015

[17] R. Tao, X. Y. Meng and Y. Wang, "Image Encryption With the Multi order of Fractional Fourier Transforms," in *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 734-738, Dec. 2010

[18] X. Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image," in *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 53-58, March 2011

[19] X. Zhang, "Reversible Data Hiding in Encrypted Image," in *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255-258, April 2011

[20] W. Hong, T. S. Chen and H. Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," in *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199-202, April 2012.doi: 10.1109/LSP.2012.2187334

[21] A. M. Elshamy *et al*., "Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding," in *Journal of Lightwave Technology*, vol. 31, no. 15, pp. 2533-2539, Aug.1, 2013

[22] J. Li and H. Liu, "Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map," in *IET Information Security*, vol. 7, no. 4, pp. 265-270, December 2013

[23] S. K. Abd-El-Hafiz, A. G. Radwan, S. H. Abdel Haleem and M. L. Barakat, "A fractal-based image encryption system," in *IET Image Processing*, vol. 8, no. 12, pp. 742-752, 12 2014

[24] S. M. Wadi and N. Zainal, "Decomposition by binary

codes-based speedy image encryption algorithm for multiple applications," in *IET Image Processing*, vol. 9, no. 5, pp. 413-423, 5 2015

[25] G. Ye and X. Huang, "An Image Encryption Algorithm Based on Autoblocking and Electrocardiography," in *IEEE MultiMedia*, vol. 23, no. 2, pp. 64-71, Apr.-June 2016.doi: 10.1109/MMUL.2015.72

[26] X. Li *et al*., "Multiple-Image Encryption Based on Compressive Ghost Imaging and Coordinate Sampling," in *IEEE Photonics Journal*, vol. 8, no. 4, pp. 1-11, Aug. 2016

[27] L. Liu, S. Miao, H. Hu and M. Cheng, "N-phase logistic chaotic sequence and its application for image encryption," in *IET Signal Processing*, vol. 10, no. 9, pp. 1096-1104, 12 2016

[28] L. Bao, S. Yi and Y. Zhou, "Combination of Sharing Matrix and Image Encryption for Lossless (k,n) - Secret Image Sharing," in *IEEE Transactions on Image Processing*, vol. 26, no. 12, pp. 5618-5631, Dec. 2017

[29] X. Wu, B. Zhu, Y. Hu and Y. Ran, "A Novel Color Image Encryption Scheme Using Rectangular Transform-Enhanced Chaotic Tent Maps," in *IEEE Access*, vol. 5, pp. 6429-6436, 2017

[30] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," in *IET Image Processing*, vol. 11, no. 4, pp. 211-216, 4 2017.

[31] R. Jiang, H. Zhou, W. Zhang and N. Yu, "Reversible Data Hiding in Encrypted Three-Dimensional Mesh Models," in *IEEE Transactions on Multimedia*, vol. 20, no. 1, pp. 55-67, Jan. 2018