Security of Medical Images During Transmission: A Systematic Review

K. Prabhavathi
Research Scholar,
Department of ECE, BGS Institute of Technology,
Adichunchanagiri University, B.G.Nagara, Mandya

M.B. Anandaraju
Professor and Head,
Department of ECE, BGS Institute of Technology,
Adichunchanagiri University, B.G Nagara, Mandya

ABSTRACT

Recently the use of applications of telemedicine using medical images has increased rapidly. Author of this Article presents various medical images types and threat that can endanger the transmission of medical images. This overview paper summarizes existing security approaches to medical data with various parameters related with that. A detailed picture of technologies related to security of a system like homomorphism, steganography and cryptography is provided, along with a complete overview of current research. The purpose of this article summarize, evaluate various algorithms with different approaches depending on many parameters like MSE, PSNR, NC, BER and so on.

General Terms

Security, Medical image

Keywords

Cryptography, Watermarking, Medical image, Steganography, Attack

1. INTRODUCTION

Medical images such as Ultrasound, X-rays, C T (Computed Tomography) and M R I (Magnetic Resonance Imaging) plays indispensable role in finding various problems. We can see huge developments through internet to exchange and transfer large set of data. Particularly to develop tele-medicine service’s such as remote surgery, telemedicine, and the urgent need to exchange medical images between the patient's doctor and the scan center. This data (medical) has to be sent on highly secured medium for communication for protection of the patient's private data while transmitting medical images. Suppose an attacker caught the medical image that we transmitted and changed the original details, it will lead to diagnose wrongly. Therefore, integrity and confidentiality have become important issues in the transmission of medical images. Therefore, more care is required for protecting medical images transmitted across public networks. In providing the security to medical images, some standard techniques are used like encryption, steganography and homomorphy.

Nowadays, medical companies recognize additional medical imaging equipment every year, providing revolutionary advanced equipment and the latest technology. Currently, in the world, there are various imaging techniques as shown in Figure 1 to help doctors obtain high-quality images to diagnose diseases more accurately. This medical information may be downloaded without the permission of the prime person. Properties like this create many troubles, like – protection of copyright, ownership proof and security. Sensitive image contain a lot of important information and characteristics that differ from standard images. Medical images contain important information that is far more sensitive compared to various digital images. Every image pixels is required for diagnostic, and every de-formation will lead to false output.

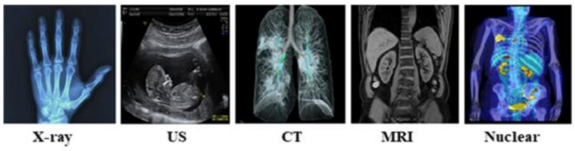


Figure 1: Different types of medical images used for transmission between the medical centres

As shown in Fig. 2, many varieties of assaults can have an effect on scientific pictures all through transmission through eHealth networks. Define secure image attacks unlike conventional transmitted log attacks. The attacks here are not aimed at gathering statistics from cryptography, but at files that contaminate and falsify secure media. They are classified into geometry attacks such as scale, rotate, translate, crop, and stretch. Signal processing solves Adaptive Histogram, C A (Rating Adjustment), H E (Histogram Equalization), G A (Gamma Correction). In terms of alternatives, image filtering, including mean, median, and Sobel filter, can help to reduce the attacks. Apart from this photo compression strategies are different varieties of sign processing assaults as J P E G compression.

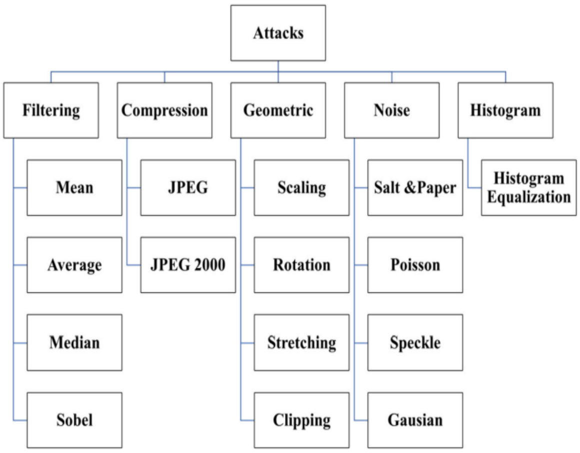


Figure 2: Different types of Attacks

The researchers will introduce various techniques for providing security to the data like encryption of data and masking to ensure data authentication as shown in Figure 3.

Data masking methods are classified into watermarks. andimplicits to load more data in the pixels of the image. Most of these techniques do not allow you to recreate the container image during the reconfiguration phase due to loss during integration or compression. Security of Medical image is very vital in e-Health applications such as storing, retrieving, stealing personal information, and managing the data. Hence many articles and studies published discussing approaches for protection of copyright along with providing security to medical data. Studies focus on one/two approach like encryption, isomorphism, etc. The survey does not cover all approaches.

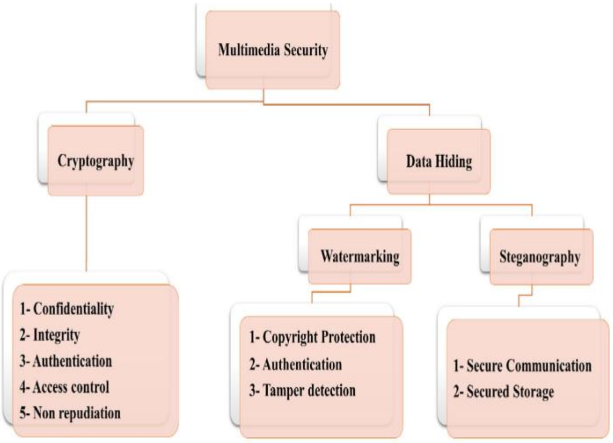


Figure 3: Different approaches used in multimedia security

1.1 Cryptography

The encryption target protects the channel of communication. Because technology of data encryption is provided, those who have same decryption key will get the original image back from encrypted message. It has the advantage of preventing an attacker from changing or updating the communication medium. This is achieved using public key cryptography and hash functions. The techniques like RSA, DES, Blow-fish and AES provides the highest data protection. To get the highest safety, we need to hybridize these methods. Although to encrypt text data, techniques like this are required, they are not effective to secure an image due to the following fundamental characteristics of images: Lots of redundancy and strong correlation between pixels adjacent. Therefore, images need an efficient way to achieve strong security. Encryption typically goes two different stages, called decryption and encryption, like shown in Figure 4 below. Cryptography is used for converting data into a format that is incomprehensible to illegal users who protect it using encryption algorithms. Original image is converted or encoded to a format when no one can read it, during the encryption phase using the private key. Decoding uses the same key to decode the encoded image back to the original image. Encrypted data is sent to the destination over an unsecured channel. Stream ciphers and block ciphers are encryption modes. If the encoded data is restricted, we can use stream cipher. Suppose we have a large data size, it will be divided into blocks and the encryption algorithm will be applied as follows. Various encryption techniques have been presented. Generally various techniques for Image encryption are classified based on position substitution-based algorithms, value transformations, and positional sequence-based algorithms, or by spatial domain and transformation. This study will focus on domain classification as shown below.

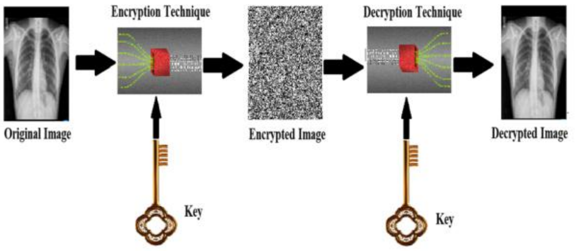


Figure 4: General encryption and decryption model for medical image security

1.2 Spatial domain encryption techniques

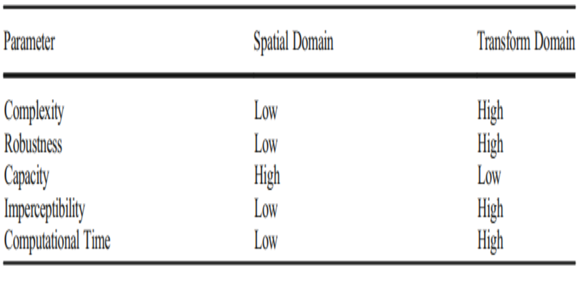
Research works recently closely observed the chaos based encryption and system based on chaotic has almost similar while encoding the image and transmitting. Secure for attacking should be there. It is [1]. Thus, chaotic cryptography is defined as an appropriate combination of chaos theory and cryptography. Real numbers are generally used to define the systems based on chaotic whereas cryptographic systems use integers from finite set. Ciphers like DES and AES are good for text whereas they are bad for encrypting images because the information represented by pixels in the same images is repeated. Chaos-based encryption technology solves this problem by generating a uniformly distributed random key to mask the picture-in-picture information in the encrypted picture [2]. Two scientific terms used here are so highly related that they provides better performance, a higher level of security, and pseudo random number to obtain ciphers stream [3] and ciphers block [4]. A variety of useful and practical applications are well integrated. , Secure communication [5], image encryption [6] and video encryption [7]. The chaos system is considered a set of dynamic equations that change over time. It can be continuous or discrete [8]. Salient features related to chaos system, like determinism, ergodicity, sensitivity to starting conditions, are valuable in cryptosystem design because they are similar to diffusion and confusion properties which are a feature of good crypto system. It will be a choice. Main and the difficult step is choosing a chaos map when designing a chaos-based algorithm [9]. Cryptographic system speed and robustness are important to design a crypto algorithm efficiently. That's why researcher started designing with simpler chaotic cards with smaller keyspaces and less security, such as tent cards and logistic cards. Later, as the design of cryptographic algorithms progressed, higher dimensional chaos maps were applied to improve the speed, security and quality of cryptographic systems.

Many maps related to chaotic concept are analysed to encrypt an image, including henon-map [10], Tinker-bell map [11], 1D Logistic-map [12], 2D Logistic-map [13], and tent-map [14]. Multi-images Block base on cipher encryption of medical image data has been proposed. First and foremost, ROI (Region of Interest) is extracted using operator to detect an edge using Laplacian approach, depending on edges within the block [15]. ACM (Arnold's Cat Mapping) and entropy threshold are combined and encoded using this algorithm only for selected image parts. Entropy threshold separates important and non-important blocks of primary image [16]. The position and value of ROI pixel's in image modified in the Arnold map sequence is manipulated in the brown map [17]. This method encodes an image using the night tour pattern of scan and the henon-map method. In proposed technique, the idea used is - simple image undergoes bit level and pixel level shuffling operations, then we go with a process of diffusion [18].

1.3 Transform domain encryption techniques

Ran-et-al [19] came up with generation of fractional matrix along with a periodic matrix sequence that replaces FRFT from a fractional new matrix sequence in a doubled random phase coding (DRPE) technique. Pei et al. [20] Extends your rare work based on fractional conversions (discrete) to multi-parameter fractional conversions (discrete). The basic idea is to use different fractional powers for different eigenvalues to achieve the multi-parameter properties of eigenvalue decomposition based fractional transformations. Lang-et-al. [21] came up with FRFT type of weight which is a multiplicity source to create a WFRFT (Weighted Fractional Fourier Transform). This allows the WFRFT weighting factor to be generalized to include two vector parameters. It turns out that the maybe Fourier transform generated in this way is a combination of linear FRFT's of various order. Pei and Hue [22] described the generation of fractional degree parameters with a random DFT pendulum matrix.. Tao et al. [23] Proposed to use multiple degree FRFT's. In this case, the image is split into sub-images of equal size in M N, and different sub-images are scrambled to the same size. This increases keyspace, but should be considered a limitation from a transmission and storage perspective. Kangetal [24] came up with two theoretical frameworks called Type I and Type II MPDFRT (Multi Parameter Discrete Fractional Fourier Transforms). This can include existing multi-parameter transformations as a special case. Ran-et-al. [25] explored the possibilities of a variety of common FRFTs in different representations, including generalized FRFT (GFRFT), conventional FRFT (CFRFT), WFRFT. Zhang [26] used the linear sum of matrix of multiple matrices to get matrix of periodic in diagonal. However, the methodology proposed for the multi-parameter framework had certain drawbacks. Ran et al. [27] the parameter vectors are chosen specifically as M-dimensional random vectors of 0 or 1 with equal probability during encryption. The work proposes that if the element of two vectors can be chosen to be an arbitrary integer, the encryption security will be greatly improved. Youseff [28] has shown that the building blocks of cryptographic methods in a multi-parameter frame are linear, and thus breaking these security patterns using a known plaintext attack is similar. MPDFRFT -based cryptosystems have the serious flaw of having multiple choices for decryption keys. This is Zhao et al. equivalent to encryption with a single keyset, as suggested by author. [29]

Frequency domain mechanism reconstructs the host media coefficients after the embedding process. Methodologies include, DCT, DWT, RDWT, DFT and SVD, and more. Spatial domain method is easier to calculate than the frequency domain, but it is less robust to geometric attacks. Evaluate some properties by comparing the spatial domain and transformation domain techniques, as given in Figure 4.



Parameter	Spatial Domain	Transform Domain
Complexity	Low	High
Robustness	Low	High
Capacity	High	Low
Imperceptibility	Low	High
Computational Time	Low	High

Figure 4: Comparison of Spatial and transform domain techniques

1.4 Homomorphic based Image Encryption Techniques

Homomorphic encryption was previously discussed by [30] and [31]. Recently, the author of [32] reviewed cutting-edge technologies for incorporating homomorphic encryption into cloud security. They highlight the homomorphic challenges and limitations of applying HE methods to encrypted data in the cloud. The author of [33] describes the necessary background and related knowledge about the higher education system. The author of [34] outlines how to use HE to calculate big data. They represent relevant challenges, opportunities, and future improvements. The fully homograph encryption properties, applications, and techniques are summarized in [35]. The HE libraries have been reviewed by [36] and also provide an overview of all the languages supported by these libraries. In addition, this study mentioned potential applications of such libraries. The author of [37] presents a systematic review of HE, showing applications for current needs and future prospects, including security and privacy. This study focuses on other potential uses not covered by the above review.

2. PERFORMANCE ANALYSIS OF IMAGE ENCRYPTION ALGORITHM

It is necessary to analyses parameter relationships between source and cipher images to determine the most efficient encryption technique. The following parameters are commonly used to analysis efficiency of general image protection techniques.

2.1 Entropy Analysis

A measure of unpredictability in an encryption system is entropy. Entropy can be calculated using the following formula:

$$H(S) = \sum_{i=0}^{2^M-1} P(si)\log_2 \frac{1}{P(si)} \quad (1)$$

Where P(si) denotes the probability of the ith gray level appearing in the image. For a random image, the ideal value of entropy is 8. Predictability is higher if it's lower.

2.2 M S E (Mean Square Error)

By considering the mean of squared difference between the input and encrypted picture, MSE may be determined. The higher the MSE number, the more nose is introduced, and the lower the signal strength. If I1 is the source picture and E1 is the cypher image, then MSE is given by Eq. 2.

$$MSE = \frac{1}{MXN}\sum_{i=1}^{M}\sum_{j=1}^{N}[X(i,j)-Y(i,j)]^2 \quad (2)$$

Where, row and column are shown as h, w, and image X(i,j) is the source image and image Y(i,j) is the cipher image.

2.3 P S N R (Peak Signal to Noise Ratio)

PSNR is a ciphering quality metric. MSE is greater than PSNR, and vice versa. The PSNR number reflects how strong the signal is. In a mathematical sense, as in.

$$PSNR = 10\log_{10}\frac{255}{MSE} \quad (3)$$

2.4 UACI and NPCR

Number of Pixels Change Rate and Unified Average Changing Intensity are used to find sensitivity of proposed ciphering technique to the source image and key. Eq. 4 is UACI's formula.

$$UACI = \frac{1}{N}\left[\sum_{i,j}\frac{|C1(i,j) - C2(i,j)|}{255}\right] \qquad (4)$$

Here, n and m are column and rows number respectively, with C1(i,j) and C2(i,j) corresponds to the original image and the cypher image, respectively.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} X100\% \quad (5)$$

Here, M represents rows and N represents columns and D(i,j) is given by

$$D(i,j) = \begin{cases} 1, C1(i,j) \neq C2(i,j) \\ 0, \quad otherwise \end{cases} \qquad (6)$$

Where C1(i,j) represents the cipher image and C2(i,j) represents the original.

2.5 S S I M (Structural Similarity Index Matrix)

The amount of similarity between two images is S S I M. It's value will range from 0 to 1. If two images are identical, we have 1 (ideal value otherwise would be 0. It is determined by equation

$$(7).SSIM(x,y) = \left[\frac{(2\mu x\mu y + C1) \quad (2\sigma xy + C2)}{(\mu x^2 + \mu y^2 + C1) \quad (\sigma x^2 + \sigma y^2 + C2)}\right] \qquad (7)$$

2.6 B E R (Bit Error Rate)

The ratio of the number of error bits when comparing two images to the total number of bits in the image is called the B E R. Ideally, 0 would be the BER value. However, the value of B E R is 1 for the encoded image. It is determined by equation (8).

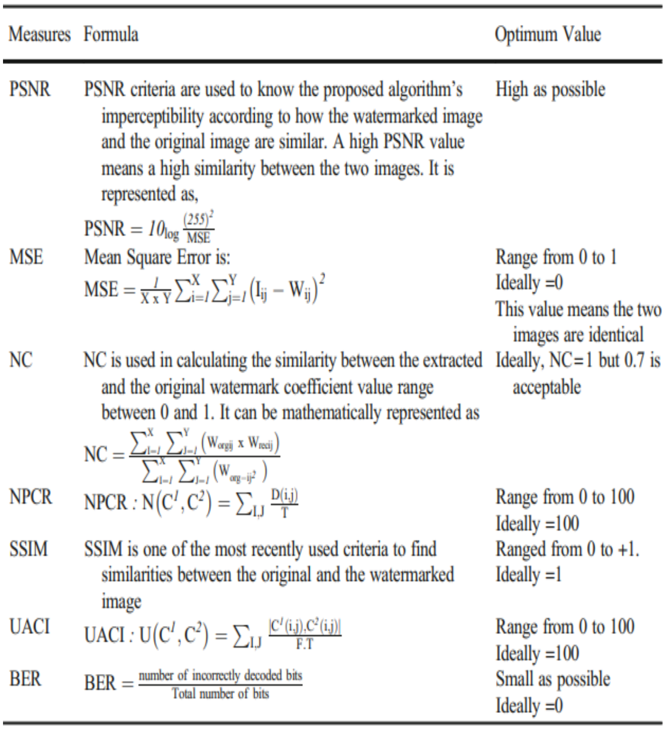
$$BER = \sum_{i,j} \frac{S(i,j)}{T_{pixels}} \qquad (8)$$

Here $T_{pixels}$is the total no. of pixels.

2.7 Normalized Coefficient (N C)

The NC gives the co-relation of two adjacent coefficients. 1 is its ideal value. But, encoded image will be weak. The co-relation of adjacent pixel (closer to 0) makes very tough to infer adjacent pixel.

$$NC = \sum_{i=1}^{X}\sum_{j=1}^{Y}\frac{(org(i,j) * enc(i,j))}{org^2(i,j)} \quad (9)$$



Measures	Formula	Optimum Value
PSNR	PSNR criteria are used to know the proposed algorithm's imperceptibility according to how the watermarked image and the original image are similar. A high PSNR value means a high similarity between the two images. It is represented as, $PSNR = 10_{\log}\frac{(255)^2}{MSE}$	High as possible
MSE	Mean Square Error is: $MSE = \frac{1}{X \times Y}\sum_{i=1}^{X}\sum_{j=1}^{Y}(I_{ij} - W_{ij})^2$	Range from 0 to 1 Ideally =0 This value means the two images are identical
NC	NC is used in calculating the similarity between the extracted and the original watermark coefficient value range between 0 and 1. It can be mathematically represented as $NC = \frac{\sum_{I=1}^{X}\sum_{J=1}^{Y}(W_{orgij} \times W_{recij})}{\sum_{I=1}^{X}\sum_{J=1}^{Y}(W_{org-ij^2})}$	Ideally, NC=1 but 0.7 is acceptable
NPCR	$NPCR : N(C^1, C^2) = \sum_{I,J}\frac{D(i,j)}{T}$	Range from 0 to 100 Ideally =100
SSIM	SSIM is one of the most recently used criteria to find similarities between the original and the watermarked image	Ranged from 0 to +1. Ideally =1
UACI	$UACI : U(C^1, C^2) = \sum_{I,J}\frac{\lvert C^1(i,j), C^2(i,j)\rvert}{F.T}$	Range from 0 to 100 Ideally =100
BER	$BER = \frac{\text{number of incorrectly decoded bits}}{\text{Total number of bits}}$	Small as possible Ideally =0

Figure 5: Performance Metrics

Figure 5 shows the different metric used in any encryption scheme and its ideal values. Parameters for efficient encryption technique should satisfy the ideal values.

3. CONCLUSION

Security of Medical image is very important in many e-Health applications such as management of data, theft identity, retrieval and storage. Here the recent developments to provide security of medical image over the past five years and analyses the challenges of medical image security. List of some well-known image attacks applied to the data to test the proposed algorithm. Several approaches to medical imaging security, such as cryptography are presented in the spatial and frequency domain, and a detailed description of isomorphic encryption is presented. In addition, several performance metrics for evaluating algorithms have been presented. Thanks to our research, researchers can suggest new security methods to protect the transmission of medical data to online medical services.

4. REFERENCES

[1] Noshadian, S., Ebrahimzade, A., Kazemitabar, S.J.: Optimizing chaos based image encryption. Multimedia Tools Appl. 77(19):25,569–25,590 (2018)

[2] Furht, B., Muharemagic, E., Socek, D.: Multimedia encryption and watermarking, vol 28. Springer Science & Business Media (2006)

[3] Liu, Z., Wang, Y., Zhao, Y., Zhang, L.Y.: A stream cipher algorithm based on 2d coupled map lattice and partitioned cellular automata. Nonlinear Dyn. 101(2), 1383–1396 (2020)

[4] Xy, Wang, Xm, Bao: A novel block cryptosystem based on the coupled chaotic map lattice. Nonlinear Dyn. 72(4), 707–715 (2013)

[5] Peng, Z., Yu, W., Wang, J., Zhou, Z., Chen, J., Zhong, G.: Secure communication based on microcontroller unit with a novel fivedimensionalhyperchaotic system. Arab.

J. Sci. Eng., pp. 1–16 (2021)

[6] Som, S., Dutta, S., Singha, R., Kotal, A., Palit, S.: Confusion and diffusion of color images with multiple chaotic maps and chaosbased pseudorandom binary number generator. Nonlinear Dyn. 80(1), 615–627 (2015)

[7] Xu, H., Tong, X., Meng, X.: An efficient chaos pseudo-random number generator applied to video encryption. Optik 127(20), 9305–9319 (2016)

[8] Lan, R., He, J., Wang, S., Gu, T., Luo, X.: Integrated chaotic systems for image encryption. Signal Processing 147, 133–145 (2018)

[9] Sankpal, P.R., Vijaya, P.: Image encryption using chaotic maps: a survey. In: 2014 Fifth international Conference on Signal and image Processing, IEEE, pp. 102–107 (2014)

[10] Wei-Bin, C., Xin, Z.: Image encryption algorithm based on Henon chaotic system. In: 2009 International Conference on Image Analysis and Signal Processing, IEEE, pp. 94–97 (2009)

[11] Krishna, P.R., Teja, C.V.S., Thanikaiselvan, V., et al.: A chaos based image encryption using tinkerbell map functions. In: 2018 Second International Conference on Electronics, pp. 578– 582. Communication and Aerospace Technology (ICECA), IEEE (2018)

[12] Pak, C., Huang, L.: A new color image encryption using combination of the 1d chaotic map. Signal Process. 138, 129–137 (2017)

[13] Hua, Z., Jin, F., Xu, B., Huang, H.: 2d logistic-sine-coupling map for image encryption. Signal Process. 149, 148–161 (2018) 35. Shan, L., Qiang, H., Li, J., Zq, Wang: Chaotic optimization algorithm based on tent map. Control Decision 20(2), 179–182 (2005)

[14] Fang, D., Sun, S.: A new secure image encryption algorithm based on a 5d hyperchaotic map. Plos one 15(11):e0242,110 (2020)

[15] Kiran, P., and B. D. Parameshachari. "Resource Optimized Selective Image Encryption of Medical Images Using Multiple Chaotic Systems." Microprocessors and Microsystems (2022): 104546.

[16] Kiran and B. D. Parameshachari, "Selective Image Encryption of Medical Images Based on Threshold Entropy and Arnold Cat Map". Bioscience Biotechnology Research Communications. 13. 194-202. 10.21786/bbrc/13.13/27.

[17] Kiran, P., H. T. Panduranga, and J. Yashwanth. "Efficient Secure Medical Image Transmission Based on Brownian System." In Cybersecurity, pp. 207-220. Springer, Cham, 2022.

[18] Kiran, Parameshachari, B. D., and H. T. Panduranga. "Secure transfer of images using pixel-level and bit-level permutation based on knight tour path scan pattern and henon map." In Cognitive Informatics and Soft Computing, pp. 271-283. Springer, Singapore, 2021.

[19] Q. Ran, T. Zhao, L. Yuan, J. Wang, L. Xu, Vector power multiple-parameter fractional Fourier transform of image encryption algorithm, Optics Lasers Eng. 62 (2014) 80–86, https://doi.org/10.1016/j.optlaseng.2014.05.008.

[20]] S.C. Pei, W.L. Hsue, The multiple-parameter discrete fractional Fourier transform, IEEE Signal Process Lett. 13 (6) (2006) 329–332. 10.1109/ LSP.2006.871721.

[21] J. Lang, R. Tao, Q. Ran, Y. Wang, The multiple-parameter fractional Fourier transform, Sci. China Series F: Information Sci. 51 (8) (2008) 1010, https://doi. org/10.1007/s11432-008-0073-6.

[22] S.C. Pei, W.L. Hsue, Random discrete fractional Fourier transform, IEEE Signal Process Lett. 16 (12) (2009) 1015–1018, https://doi.org/10.1109/ LSP.2009.2027646.

[23] R. Tao, X.Y. Meng, Y. Wang, Image encryption with multiorders of fractional Fourier transforms, IEEE Trans. Information Forensics Security 5 (4) (2010) 734–738, https://doi.org/10.1109/TIFS.2010.2068289.

[24] X. Kang, R. Tao, F. Zhang, Multiple-parameter discrete fractional transform and its applications, IEEE Trans. Signal Process. 64 (13) (2016) 3402–3417, https:// doi.org/10.1109/TSP.2016.2544740.

[25] Q. Ran, D.S. Yeung, E.C. Tsang, Q. Wang, General multifractional Fourier transform method based on the generalized permutation matrix group, IEEE Trans. Signal Process. 53 (1) (2005) 83–98, https://doi.org/10.1109/ TSP.2004.837397.

[26] F. Zhang, Y. Hu, R. Tao, Y. Wang New fractional matrix with its applications in image encryption, Optics Laser Technol., 64 (2014) 82–93. doi: 10.1016/j. optlastec.2014.03.020.

[27] Q. Ran, H. Zhang, J. Zhang, L. Tan, J. Ma Deficiencies of the cryptography based on multiple-parameter fractional Fourier transform, Optics Lett., 34(11) (2009) 1729–1731. doi: 10.1364/OL.34.001729.

[28] A.M. Youssef, On the security of a cryptosystem based on multiple-parameters discrete fractional Fourier transform, IEEE Signal Process. Lett., 15 (2008) 77– 78. doi: 10.1109/LSP.2007.910299.

[29] T. Zhao, Q. Ran, L. Yuan, Y. Chi, J. Ma Security of image encryption scheme based on multi-parameter fractional Fourier transform. Optics Commun., 376 (2016) 47–51. doi: 10.1016/j.optcom.2016.05.016.

[30] C. Fontaine and F. Galand, "A survey of homomorphic encryption for nonspecialists," EURASIP Journal on Information Security, vol. 2007, pp. 1–10, 2007.

[31] P. V. Parmar, S. B. Padhar, S. N. Patel, N. I. Bhatt, and R. H. Jhaveri, "Survey of various homomorphic encryption algorithms and schemes," International Journal of Computer Applications, vol. 91, no. 8, 2014.

[32] V. Biksham and D. Vasumathi, "Homomorphic encryption techniques for securing data in cloud computing: A survey," International Journal of Computer Applications, vol. 975, p. 8887, 2017.

[33] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," ACM Computing Surveys (CSUR), vol. 51, no. 4, pp. 1–35, 2018.

[34] B. Alaya, L. Laouamer, and N. Msilini, "Homomorphic encryption systems statement: Trends and challenges," Computer Science Review, vol. 36, p. 100235, 2020.

[35] Z. Brakerski, "Fundamentals of fully homomorphic

encryption-a survey." in Electronic Colloquium on Computational Complexity (ECCC), vol. 25, 2018, p. 125.

[36] S. S. Sathya, P. Vepakomma, R. Raskar, R. Ramachandra, and S. Bhattacharya, "A review of homomorphic encryption libraries for secure computation," arXiv preprint arXiv:1812.02428, 2018.

[37] M. Alloghani, M. M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, and A. J. Aljaaf, "A systematic review on the status and progress of homomorphic encryption technologies," Journal of Information Security and Applications, vol. 48, p. 102362, 2019.