Dynamic smart random preference for higher medical image confidentiality

DOI : 10.36909/jer.17853

Adnan Gutub*

Computer Engineering Department, Umm Al-Qura University, Makkah, Saudi Arabia

* Corresponding Author: aagutub@uqu.edu.sa

ABSTRACT

It is essential to secure the information to store or transfer medical digital files without destruction. Currently, all used e-health files requests to be utilized in well-controlled, protected, and dependable style avoiding breaches and hacking. This research focuses on medical confidentiality encrypting grayscale health images for comfortable safe utilization. The work depends on resilience randomization and XOR operations for its medical-image cryptography. It tests performance of some random generators conveying the best every time running that is dynamically changing depending on e-health image variations. The research tests several randomizations structures processed as two sequenced encryption methods adopting substitution and transposition. The work tested random variations to encrypt different medical grayscale images revealing attractive remarks. The paper investigation intends to recognize appropriate preference via secrecy testing typical notations. The work indicates this flexibility of best applicable PRNG and its change features interesting privacy intellectual medical gray-image security for open e-health research direction to benefit from.

Keywords: Security of medical gray-image; PRNG Randomization; Digital image encryption; XOR e-health ciphering; Substitution coding; Transposition encryption.

INTRODUCTION

Digitalization of our common e-life made any multimedia communication and storage in risk due to illegitimate confidentiality breaches. Digital medical gray-images, as focus of our research, is the most sensitive e-health media type used needing proper security (Gutub et al., 2019). Therefore, e-health image encryption is compulsory for protecting patient's privacy as well as preventing undesired untrusted manipulation, which is provided via image symmetric cryptography via confirmed agreed-upon key passwords (Alharthi & Gutub, 2017). In general, medical gray-image encryption can be performed via transposition or substitution as well as combination of both (Gutub, 2011). The transposition procedure repositions pixels spots based on placing rules, as deeply explained within (Al-Otaibi & Gutub, 2014). The substitution progression exchange pixel values as coding to be regained distinctively via password secret key each and every time desired (Gutub & Tenca, 2004). Both approaches realize the confidentiality goals of confusion and diffusion adhering to cryptography secrecy attitude (Al-Juaid & Gutub, 2019). Image crypto approaches can be commonly understood via three models, namely permuting, substituting, and combination of both (Saha et al., 2018). The permuting pixels relocate the pixels spots via reordering, as illustrated in Figure 1. The substituting performs replacing reformation via key generator hiding originality. The combination of permutation and substitution can be interesting benefitting from advantages of both (Banthia & Tiwari, 2013).

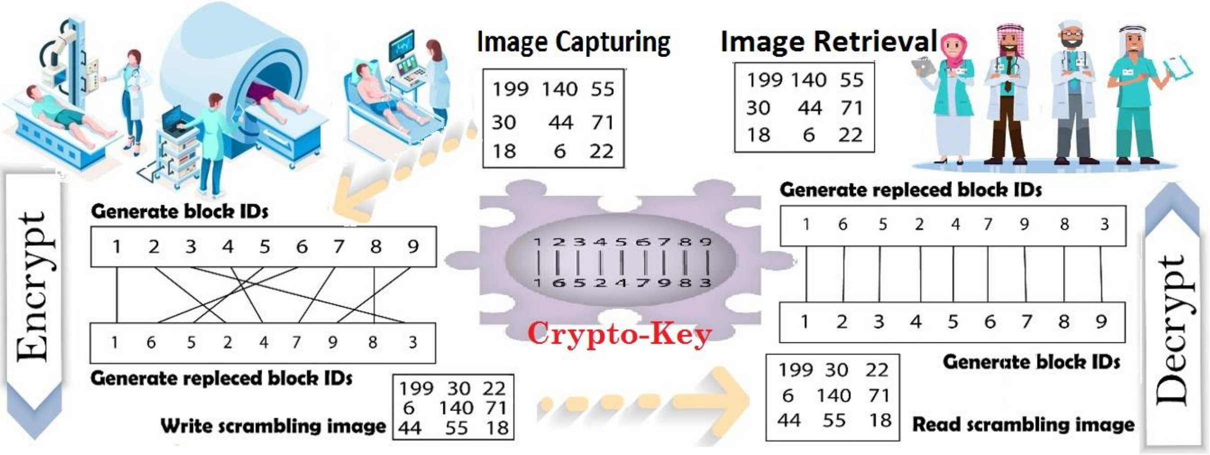


Figure 1. Crypto simplification process

This paper deals with symmetric encryption, as same key to ignite the pseudo-random number generator (PRNG) produce secret sequence stream, to be involved mathematically with the image pixels for the intended encryption (Banthia & Tiwari, 2013). This PRNG random sequence needs to enjoy unpredictability and randomness (Sivakumar & Devi, 2017), which is different than most IoT machine learning and deep learning strategies (Roy et al., 2022). Although this PRNG is 'pseudo', i.e. not fully random, its cryptography application is random enough as needed. The PRNG entails the initial value password, called ‘seed’, to be offered using true random number generator (TRNG) scheme, or any independent default value, which can be selected from the user, as principally covered integrating PVD data hiding strategies of Jeyaprakash et al. (2021) and grayscale services steganography of Sahu and Gutub (2022). Then, the PRNG provides stream of random numbers aiming good selection for cryptographic intents, i.e. recommended to pass the tests of United States NIST (Al-Qurashi & Gutub, 2018). The intention is to stress on PRNG to create random numbers sequences of great ambiguity long performance, reflecting good selection features, such as, large period, uniformity, reproducibility, consistency, portability, independence, efficiency, permutations, and disjoint subsequences (Ramasamy et al., 2019). Therefore, selecting this PRNG process will be our objective study for medical image encryption. We will test for effective generators aiming efficient gray-image confidentiality assuming that weak randomness confirms insecure privacy (Sivakumar & Devi, 2017). Our research exposes the performance of four famous PRNGs, pretending utilizing them for image encryption running experimentations on medical gray-images (public from Google) at the block of pixels level to obtain cipher images. The work investigates involving both permutation and substitution sequential techniques applied on same PRNGs for fair comparisons. The research implements the crypto approaches by creating the key streams using all four PRNGs aiming for selecting the appropriate best one depending on the image data and results. The common four PRNGs algorithms involved are Mersenne Twister (MT), SIMD-oriented Fast Mersenne Twister (dSFMT), Combined Multiple Recursive (MRG), and Multiplicative Lagged Fibonacci (MLFG). This procedure tests pixel transformation independently via all PRNGs involved. Then, all assorted trials are linked via same performance metrics to fairly choose suggested PRNG pretending highest effectiveness to secure specific medical grayscale images.

The research flow is organized by coming Section 2 describing the background in brief. Section 3 presents the proposed enhanced grayscale image secrecy mechanism based on testing all PRNGs procedure via different crypto schemes. Section 4 covers the summary of noted experimentations outcomes comparisons. Section 5 concludes the work.

RELATED BACKGROUND IN BRIEF

Electronic authenticity studies have presented many image encryption procedures to insure CIA assurances (Gutub, 2022a). This section provides relative summarization of linked crypto encryption practices, where PRNG processes are utilized to convert the cover e-images to cipher-images. For example, Saha et al. (2018) discussed using PRNG for image crypto investigation aiming efficient secure analogy. It worked integrating two pixels procedures of permutation and substitution, i.e. shuffling pixels via LFSR and PRNG XOR replacement, imitating rows with columns to yield crypto images. Relatively, Ramasamy et al. (2019) presented symmetric password generation for image crypto confidentiality adopting block mixing and zigzag alteration directing to adjusted logistic-tent map verification. Consequently, the password-key is produced on color images via XORing with PRNG and gray copy, as affected by the zigzag conversion in a smart complex way. This ciphering scheme can be very related to combination of authentication strategy of e-Videos (Gutub, 2022b) and e-Audios (Gutub, 2022c) as advancing lightweight image watermarking (Gutub, 2022d).

Contrarily, Saputra (2017) presented image scrambling via linear congruent key generator one-time pad approach expressing remarkable hard cryptanalysis image secrecy system. Likewise, Sahu (2020) revised many digital image steganography and steganalysis running over three decades; as benefitting from previous studies of optimal information hiding approach based on pixel value differencing and modulus function (Sahu and Swain, 2019) in coordination to information hiding using group of bits substitution (Sahu and Swain, 2017). All different schemes relied on dissimilar image data confidentiality where some run its method by chaos model strategy operating XOR function image ciphering authentication. Comparatively, Rohith et al. (2014) style revealed additional trusting mixture to chaos classifications as to distribute key password to an alternative of producing key by single chaos, similar to Pak and Huang (2017) whom agreed upon chaotic image ciphering structure. Their (Pak and Huang, 2017) secrecy method performed pioneering results compared to many previous chaotic-map related cryptography. The process reflected its chaotic steam for scrambling image pixels spots gaining real image indistinctness condition.

Sivakumar and Devi (2017) projected an interesting asymmetrical phase crypto, running XOR digitization, affecting key shaped via Lagged Fibonacci Generator (LFG) serving image secrecy applications. This LFG exploitation via graph square progression with consideration of above image crypto strategies motivated our encryption crypto feasibility of exploring several PRNGs aiming attractive applicability.

PROPOSED SCHEME

This work discusses adoption of various PRNGs password key streaming mechanisms found applicable for medical gray image confidentiality. The study tests four different PRNGs applied on three types of crypto functions to find the effective image encryption collection process. In other words, based on every e-health image coding full testing, we test all four PRNGs and crypto routines to first-rate one generator and one crypto-scheme to be suggested. In other words, the study dynamic selection is running between four PRNGs types via three standard crypto procedures as being unbiased, i.e. fully dependent on specific medical image data tested. This examination run parallelly on all four PRNGs, within this investigation, to select the preferred confidentiality scenario for each medical image according to every crypto scheme, as outlined in Figure 3. In other words, the modelling of image cryptography is involving identical strategy for encryption and decryption, testing all four types of PRNGs separately aiming to be showing high or low efficiency marks quantities.

The research examines all its experimentations on six commonly studied Google medical images, namely Brain-Top, Brain-Side, Chest, Fingers, Legs and Uterus, as shown in Figure 4.

Our e-health images testing comments three outputs crypto configurations based on transposition, XOR substitution and combination of both. The results considered same arithmetical merits for testing the three images security to reach applicable evaluation among each other. To be clear (Figure 3), the three image encryption modelling phenomena are described as follows:

- Model 1 (Transposition): Permute image pixels via transposition benefitting from works described in (Sivakumar & Devi, 2017) and (Sarma & Lavanya, 2017). This permutation allows initial value reauthorization affecting pixel locations mixing arrangement. Recall that this transposition is going to be applied for all four PRNGs independently.
- Model 2 (Substitution): Replace pixel values via XOR one-time pad procedure, such as (Saputra, 2017) and (Sivakumar & Devi, 2017). The research lists changes contrasted among preceding model 1, also remarking the four PRNGs results.
- Model 3 (Combination): Merge model 1 and model 2 crypto processes as consecutive integrated image cryptography, as to be examined with the other models for all PRNGs in fair-minded evaluation exploration.

This search endorses cryptography of all medical images testbench appropriately smartly remarking the results to help selecting agreement of the preferred confidentiality approach, i.e. depending on the precise medical image pixel repression, as detailed later. We tested the encryption procedures to be used on medical grayscale images on the different PRNGs, partially analogous to crypto research of Saha et al. (2018).

<u>Crypto via transposition permutation</u>

- Insert original medical grayscale image.
- Select secret password PIN, utilized as PRNG seed.
- Distribute medical image as blocks of pixels.
- Run four PRNGs parallelly using same PIN to generate different randomization e-streams. Four PRNGs adopted are: MT (Mersenne Twister), dSMFT (SIMD-oriented Fast Mersenne Twister), MRG (Combined Multiple Recursive Generator), and MLFG

(Multiplicative Lagged Fibonacci).

- Change pixels locations based on PRNGs streams generating four scrambled images, as output of permutation encryption model.

Crypto via substitution XORing

- Recall the PRNGs e-streams as same random digits utilized for transposition.
- Apply one-time-pad XOR substitution on different random streams to image pixels.
- Study the four image variations after substitution.
- Return the best PRNG resulting efficient cipher image.

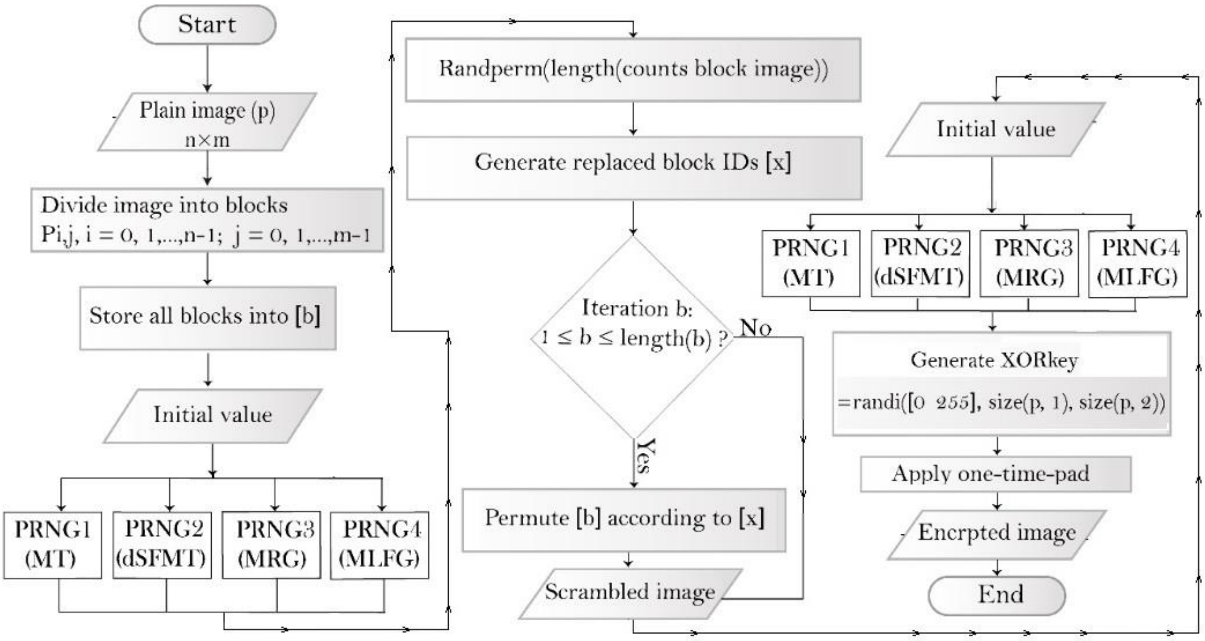
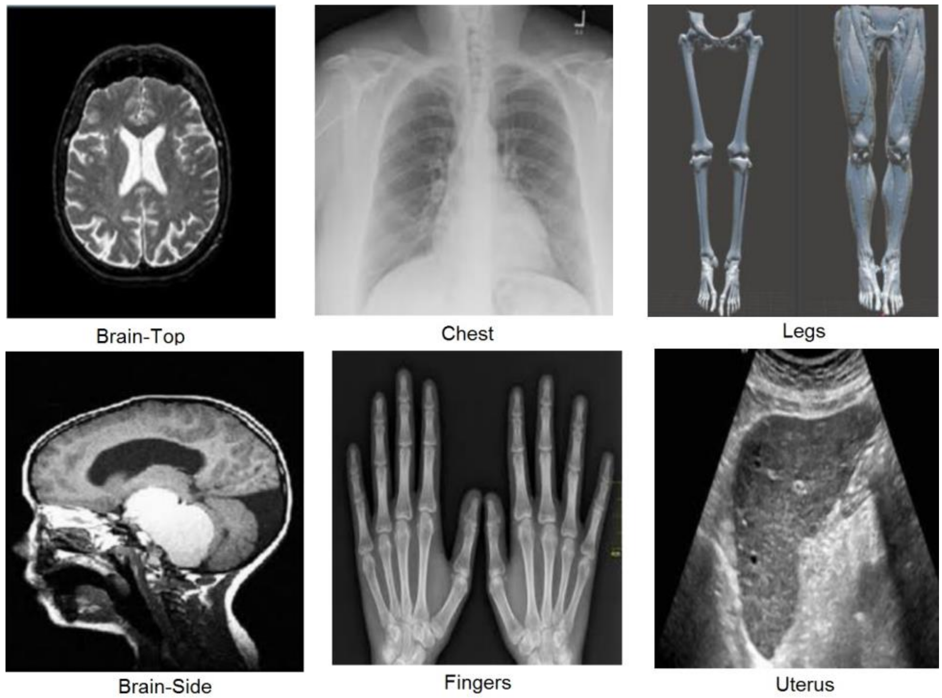


Figure 3. Proposed dynamic medical-image confidentiality procedure

The decryption progression needs to reverse the exact encryption scheme noting the PRNG selection utilized for effective image retrieval. The method operates easier than encryption since the PRNG and encryption are already known, i.e. at the storage reading time or receiver processing of transmission. Notes that the two steps of transposition and substitution needs to be swapped to gain same bits secrecy manipulation. It should be mentioned that all this decryption procedure can be feasible to get back the plain original image if and only if the same exact PIN password is adopted.



Brain-Top

Chest

Legs

Brain-Side

Fingers

Uterus

Figure 4. medical grayscale images testbench

This study enhances medical image crypto process to find the efficient PRNGs selection and encryption process according to the specific e-health image data. Therefore, our study notes main secrecy image quality performance combining parameters from Peak Signal to Noise Ratio (PSNR) and Structural Similarity index (SSIM) in a preference figure-of-merit estimation. Recall that this security effectiveness preference is covering the three encryption attempts testing all four PRNGs in an attractive comprehensive exploration. Interestingly, the experimentations showed differences in results to be compared aiming best suitability for confidentiality-effectiveness discussed within the coming Section 4 remarks.

INVESTIGATION COMPARISONS AND REMARKS

The exploration examines the model's simulation assuming all coding attempts have been run on same medical grayscale images testbench shown in Figure 4, i.e. to assure confidentiality fairness analysis. The search involved PSNR and SSIM analysis differentiating image quality estimations, being completely applied as dissimilar to entropy investigation of (Wu et al., 2011) and unlike statistical spreading variations of correlation-based measures of works (Norouzi et al., 2015) and (Rajkumar & Malathi, 2016) as well as (Wang & Bovik, 2002), (Gutub & Al-

Roithy, 2021) and (AlKhodaidi & Gutub, 2020). This research is relating the original image to encrypted images in similarity numerical manner. In general, we run the tests figuring values of PSNR and SSIM, such that as PSNR increase and SSIM reduce, the study analysis indicates better image encryption confidentiality.

Recall that this exploration determined possibilities for enhancing encryption of grayscale medical images via dynamically changing PRNG which are based fully on the unexpected e-health data content. As a remark, this study tried exploring each crypto metric (PSNR and SSIM) separately, then, we presented combination scenarios for each encryption model of possible merit-mixing features, as applying prioritization effectiveness, hoping to allow the reader to be convinced ranking the preferences accordingly.

To be optimistic, the operative procedure for medical gray-image security can be determined by selecting suitable encryption and PRNG. Thus, the testing PSNR and SSIM measures of crypto quality are shown in Table 1, as focused on dynamically enhancing secrecy trying to combine these different features in a prioritization effectiveness figure-of-merit analysis, principally following research of (AlKhodaidi & Gutub, 2020) computing cost analysis, to help predicting the image-stego suitability remarks. We signified this prioritization combining weights as *Preference = PSNR/SSIM*, noting high and low secrecy, respectively. Note that PSNR decibel mark, represents human perception, with low value informing most sameness making our desire to see it as high as possible, as shown in Figure 5. Relatively, SSIM value ranges between 0 and 1, as shown in Figure 6, with 1 indicating most identicality estimation close to 0 being our confidentiality preference.

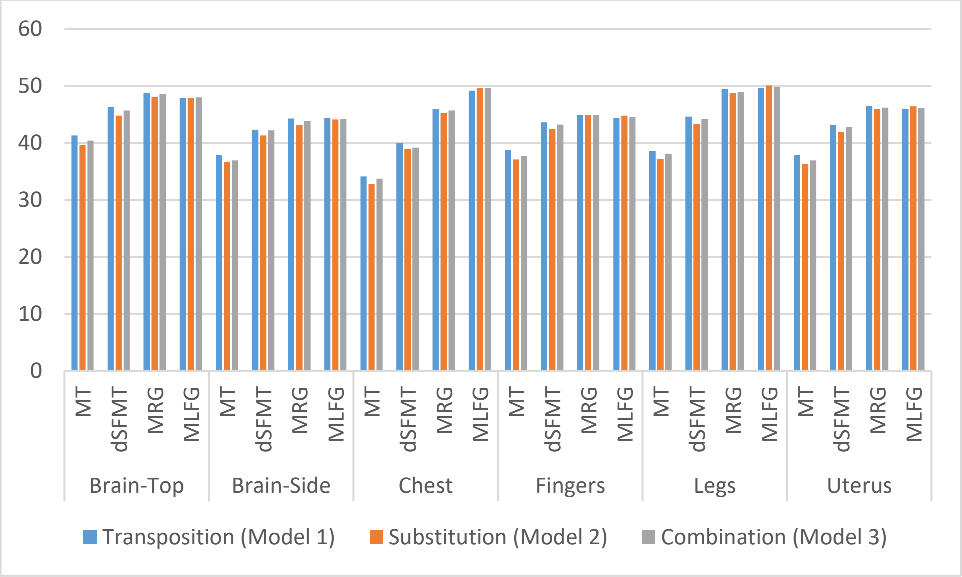


Figure 5 PSNR Results

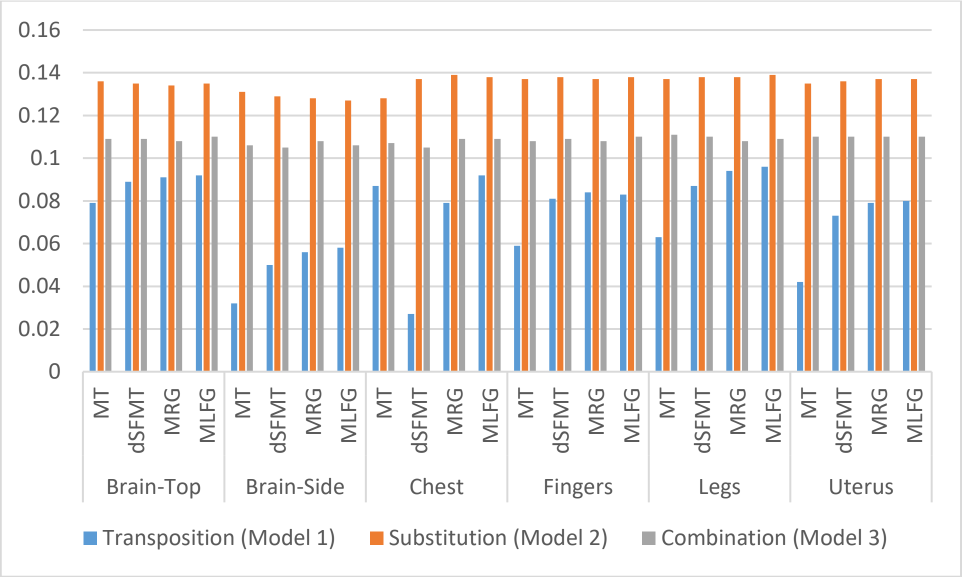


Figure 6 SSIM Results

The prioritization preferences are listed as shown in Table 1, to sense the best PRNG for utilizing every medical image (Figure 4) crypto analysis finding Model 1 Transposition preference of MT for Brain-Side, Fingers, Legs and Uterus as well as MRG for Brain-Top and dSFMT for Chest. This analysis of Model 1 priority preferred MT by above 66% not picking MLFG at all. Interestingly, Model 2 XOR Substitution designated MRG for Brain-Top and Fingers, MLFG for Brain-Side, Legs, Uterus and Chest, fully ignoring MT and dSFMT. This Model 2 mostly elected MLFG for around 66% followed by MRG for just above 33%.

Likewise, Model 3 crypto-combination nominated MRG for Brain-Top, Uterus and Fingers, MLFG for Brain-Side, Legs and Chest, making Model 3 choice split 50% between MRG and MLFG leaving MT and dSFMT without being designated.

Table 1. Transposition, substitution, and combo-cryptography prioritization.

Image	**PRNG**	**Transposition (Model 1)**			**Substitution (Model 2)**			**Combination (Model 3)**		
		PSNR	**SSIM**	**Preference**	**PSNR**	**SSIM**	**Preference**	**PSNR**	**SSIM**	**Preference**
Brain-Top	MT	41.3	0.079	522.8	39.6	0.136	291.2	40.4	0.109	370.7
	dSFMT	46.3	0.089	520.3	44.8	0.135	331.9	45.7	0.109	419.3
	MRG	48.8	0.091	**536.3**	48.1	0.134	**359**	48.6	0.108	**450**
	MLFG	47.9	0.092	520.7	47.9	0.135	354.9	48	0.11	436.4
Brain-Side	**MT**	37.9	0.032	**1184.4**	36.7	0.131	280.2	36.9	0.106	348.2
	dSFMT	42.3	0.05	846.1	41.3	0.129	320.2	42.2	0.105	402
	MRG	44.3	0.056	791.1	43.1	0.128	336.8	43.9	0.108	406.5
	MLFG	44.4	0.058	765.6	44.1	0.127	**347.3**	44.2	0.106	**417**
Chest	MT	34.1	0.087	392	32.8	0.128	256.3	33.7	0.107	315
	dSFMT	40	0.027	**1481.5**	38.9	0.137	284	39.2	0.105	373.4
	MRG	45.9	0.079	581.1	45.3	0.139	325.9	45.7	0.109	419.3
	MLFG	49.2	0.092	534.8	49.7	0.138	**360.2**	49.6	0.109	**455.1**
Fingers	**MT**	38.7	0.059	**656**	37.1	0.137	270.9	37.7	0.108	349.1
	dSFMT	43.6	0.081	538.3	42.5	0.138	308	43.2	0.109	396.4
	MRG	44.9	0.084	534.6	44.9	0.137	**327.8**	44.9	0.108	**415.8**
	MLFG	44.4	0.083	535	44.8	0.138	324.7	44.5	0.11	404.6
Legs	**MT**	38.6	0.063	**612.7**	37.2	0.137	271.6	38.1	0.111	343.3
	dSFMT	44.6	0.087	512.7	43.3	0.138	313.8	44.2	0.11	401.9
	MRG	49.5	0.094	526.6	48.7	0.138	352.9	48.9	0.108	452.8
	MLFG	49.6	0.096	516.7	50.1	0.139	**360.5**	49.8	0.109	**456.9**
Uterus	**MT**	37.9	0.042	**902.4**	36.3	0.135	268.9	36.9	0.11	335.5
	dSFMT	43.1	0.073	590.5	41.9	0.136	308.1	42.8	0.11	389.1
	MRG	46.5	0.079	588.7	46	0.137	335.8	46.2	0.11	**420**
	MLFG	45.9	0.08	573.8	46.4	0.137	**338.7**	46.1	0.11	419.1

This study overall PRNG relationship selection can be shown as Table 2 summarizing the preferred dynamic randomization scheme among all simulations. Every medical image cryptography had completely different preference values depending on the model used, making the best PRNG fair selection possible only after testing all four PRNGs, in an unexpected surprising manner. For example, Table 2 show that Brain-Top image frequently preferred MRG within all models. The medical images Brain-Side, Legs and Chest selected MLFG for above

66% keeping MT with 33% and dSFMT with around 16% nomination. The e-health image Fingers preferred MRG double its preference of MT while the image Uterus gave same preference percentage to MRG, MLFG and MT.

To summarize these observations statistically, considering all selections together, the best PRNGs can be MLFG wining around 39% of all choices, followed by MRG of 33%, MT by almost 22% keeping dSFMT with lowest probability of less than 6%. An interesting observation can be reported that most PRNG preferences have been common for Model 2 (Substitution) and Model 3 Combo-Cryptography, making it an interesting feature to study more within linked elaborated research. Also, this (Table 2) preferences can give guessing idea of appropriate PRNG selection of MLFG and MRG as mostly having better preference more than the other two PRNGs, which can be the common case for medical images, especially if hardware-built ASIC implementation is requested.

Table 2. All models PRNG preference in relation to medical images

Images	Model	Preference	PRNG	Images	Model	Preference	PRNG
Brain-Top	1	536.3	MRG	Fingers	1	656	MT
	2	359	MRG		2	327.8	MRG
	3	450	MRG		3	415.8	MRG
Brain-Side	1	1184.4	MT	Legs	1	612.7	MT
	2	347.3	MLFG		2	360.5	MLFG
	3	417	MLFG		3	456.9	MLFG
Chest	1	1481.5	dSFMT	Uterus	1	902.4	MT
	2	360.2	MLFG		2	338.7	MLFG
	3	455.1	MLFG		3	420	MRG

CONCLUSION

This investigation presents a research of four different PRNGs driving medical image crypto alteration progressions. The PRNGs adopted have been Mersenne Twister (MT), SIMD-oriented Fast Mersenne Twister (dSFMT), Combined Multiple Recursive (MRG), and Multiplicative Lagged Fibonacci (MLFG). Every PRNG have been tested trailing transposition shuffling, XOR substitution replacement, and a combination of both, as mixed ciphering process. All encryption routines experienced the identical PRNGs on same medical gray images testbench making dissimilar ciphering results collected all together for ranking preference.

Therefore, the research three models run the images testing on all PRNGs clearly to offer evaluation numerical PSNR and SSIM readings, which have been united professionally for confidentiality efficiency via priority figure-of-merit analysis. Remarkably, this preparation competence formulation quantified secrecy dynamic flexibility mixture based on medical image e-details as well as ciphering structure variances, selecting the favored PRNG high-quality embracing based on security approximation. To be optimistic, the most probable PRNGs preference can be very different based on the specific image based on overall running remarks. Therefore, Brain-Top image preferred MRG PRNG for all its crypto models. The images Brain-Side and Legs selected MT for Transposition (Model 1) and MLFG for the other two models; whereas image Chest chose dSFMT for Transposition (Model 1) and also MLFG for the other two, making it similar in these circumstances. From this point of view, It has been found that MT PRNG is mostly preferred for crypto model 1 (Transposition) making it the favored selection. For model 2 and model 3, it is mostly choosing MRG or MLFG PRNGs in an interesting selective image-dependent manner.

In general, the results of the crypto encryption operations showed variation of stimulating results. The study based its image quality measurements on estimation rates that can change if other prioritization parameters have been selected, as looking for other attractive future manners. This guides to future work plan, for achieving better security, to select the higher effective generator from the output of this paper and apply AI advancements with the moderately effective generator, hoping to find new gorgeous annotations (Singh et al., 2022). Future research is expected to find ways to increase the security as key factors to be showing remarkable research out-of-the-box directions.

REFERENCES

Alharthi, N., Gutub, A. 2017. Data visualization to explore improving decision-making within Hajj services. Scientific Modelling and Research. 2: 9-18.

Al-Juaid, N., Gutub, A. 2019. Combining RSA and audio steganography on personal computers for enhancing security. SN Applied Sciences. 1: 830.

AlKhodaidi, T., Gutub, A. 2020. Trustworthy Target Key Alteration Helping Counting-Based Secret

Sharing Applicability. Arabian Journal for Science and Engineering. 45: 3403–3423.

Al-Otaibi, N., Gutub, A. 2014. 2-leyer security system for hiding sensitive text data on personal computers. Lecture Notes on Information Theory. 2: 151-157.

Al-Qurashi, A., Gutub, A. 2018. Reliable secret key generation for counting-based secret sharing. Journal of Computer Science & Computational Mathematics. 8: 87-101.

Al-Roithy, B., Gutub, A. 2021. Remodeling Randomness Prioritization to Boost-up Security of RGB Image Encryption. Multimedia Tools and Applications. 80(18): 28521–28581.

Banthia, A., Tiwari, N. 2013. Image Encryption using Pseudo Random Number Generators. International Journal of Computer Applications. 975: 8887.

Gutub, A. 2022a. Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing. CAAI Transactions on Intelligence Technology, IET (IEE) - Wiley, in press http://doi.org/10.1049/cit2.12093

Gutub, A. 2022b. Adopting counting-based secret-sharing for e-Video Watermarking allowing Fractional Invalidation. Multimedia Tools and Applications (MTAP). 81(7): 9527–9547.

Gutub, A. 2022c. Regulating Watermarking Semi-Authentication of Multimedia Audio via Counting-Based Secret Sharing. Pamukkale University Journal of Engineering Sciences. 28(2): 324-332.

Gutub, A. 2022d. Watermarking Images via Counting-Based Secret Sharing for Lightweight Semi-Complete Authentication. International Journal of Information Security and Privacy. 16(1):1-18.

Gutub, A., Al-Roithy, B. 2021. Varying PRNG to improve image cryptography implementation. Journal of Engineering Research. 9(3A): 153-183.

Gutub, A., Al-Juaid, N., Khan, E. 2019. Counting-based secret sharing technique for multimedia applications. Multimedia Tools and Applications. 78: 5591-5619.

Gutub, A., Tenca, A. 2004. Efficient scalable VLSI architecture for Montgomery inversion in GF(p). Integration, The VLSI Journal. 37: 103-120.

Gutub, A. 2011. Subthreshold SRAM designs for cryptography security computations. International Conference on Software Engineering and Computer Systems, Universiti Malaysia Pahang, Malaysia.

Jeyaprakash, H., Kartheeban, K., Sahu, A.K., Chokkalingam, B. 2021. Data Hiding Using PVD and Improving Security Using RSA. Journal of Applied Security Research. DOI: 10.1080/19361610.2021.1900692

Norouzi, B., Seyedzadeh, S., Mirzakuchaki, S., Mosavi, M. 2015. A novel image encryption based on row-column, masking and main diffusion processes with hyper chaos. Multimedia Tools and Applications. 74: 781-811.

Pak, C., Huang, L. 2017. A new color image encryption using combination of the 1D chaotic map. Signal Processing. 138: 129-137.

Ramasamy, P., Ranganathan, V., Kadry, S., Damaševičius, R., Blažauskas, T. 2019. An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic - Tent map. Entropy. 21: 656.

Rajkumar, S., Malathi, G. 2016. A comparative analysis on image quality assessment for real time satellite images. Indian Journal of Scince and Technology. 9(34): 1-11.

Rohith, S., Bhat, K., Sharma, A. 2014. Image encryption and decryption using chaotic key sequence generated by sequence of logistic map and sequence of states of Linear Feedback Shift Register. International Conference on Advances in Electronics Computers and Communications, Bangalore, India.

Roy, P., Saumya, S., Singh, J., Banerjee, S., Gutub, A. 2022. Analysis of community question-answering issues via machine learning and deep learning: State-of-the-art review. CAAI Transactions on Intelligence Technology, IET (IEE) - Wiley, in press. http://doi.org/10.1049/cit2.12081

Saha, S., Karsh, R., Amrohi, M. 2018. Encryption and Decryption of Images Using Secure Linear Feedback Shift Registers. International Conference on Communications & Signal Processing (ICCSP), Chennai, India.

Sahu, A.K., Gutub, A. 2022. Improving grayscale steganography to protect personal information disclosure within hotel services. Multimedia Tools and Applications (MTAP). in press. DOI: 10.1007/s11042-022-13015-7

Sahu, A.K., Sahu, M. 2020. Digital image steganography and steganalysis: A journey of the past three decades. Open Computer Science. 10: 296–342.

Sahu, A.K., Swain, G. 2019. An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function. Wireless Personal Communications. 1-16. DOI:10.1007/S11277-019-06393-Z

Sahu, A.K., Swain, G. 2017. Information Hiding Using Group of Bits Substitution. International Journal on Communications Antenna and Propagation. 7(2): 162-167.

Saputra, I. 2017. Image Scrambling Using One Time Pad with Linear Congruent Key Generator. International Journal of Informatics and Computer Science (IJICS). 1(1): 8-14.

Sarma, K., Lavanya, B. 2017. Digital image scrambling based on sequence generation. International Conference on Circuit, Power and Computing Technologies (ICCPCT), India.

Singh, A., Satapathy, S., Roy, A., Gutub, A. 2022. AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope. Arabian Journal for Science and Engineering (AJSE), in press. http://doi.org/10.1007/s13369-021-06348-2

Sivakumar, T., Devi, K. 2017. Image Encryption using Block Permutation and XOR Operation". International Journal of Computer Applications. 975: 8887.

Wu, Y., Noonan, J., Agaian, S. 2011. Shannon entropy based randomness measurement and test for image encryption. arXiv preprint arXiv:1103.5520.

Wang, Z., Bovik, A. 2002. A universal image quality index. IEEE Signal Processing Letters. 9: 81-84.