Journal of Theoretical and Applied Information Technology

31st December 2023. Vol.101. No 24
© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SURVEY ON COMPONENTS THAT GOVERN THE EXECUTION OF CRYPTOSYSTEMS

YAHAYA GARBA SHAWAI[1,2], MOHAMAD AFENDEE MOHAMED[2], USMAN HARUNA[3], MOHAMMED AMIN ALMAIAH[4, 5] ,ABDALWALI LUFTI[6,7], SULAIMAN IBRAHIM MUHAMMAD[8,9]

[1]National Open University of Nigeria
[2] Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin, Malaysia
[3]Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu
[4]Faculty of Information Technology, Aqaba University of Technology, Aqaba, 11947, Jordan
[5] Applied Science Research Centre, Applied Science Private University, Amman, 11931 Jordan
[6]College of Business, King Faisal University, Al-Ahsa, Saudi Arabia
[7]MEU Research Unit, Middle East University Amman, Jordan
[8]Institute of Strategic Industrial Decision Modelling, Scchool of Quantitative Sciences, Universiti Utara Malaysia
[9]Faculty of Education and Arts, Sohar University, Sohar 311, Oman.
yshawai@noun.edu.ng, shawaiyahayagarba76@gmail.com

ABSTRACT

The aim of the review was to carry out a survey on the components that govern the experimental simulation of a cryptosystems, which includes input images, hardware and software facilities, algorithm formulations. The components were analysed with regards to the performance of the encryption algorithms, based on specific finding of individual execution time. The review paper discovered the existing literature within the fields of image encryption based chaotic system, with aid of adapting new proposed systematic review framework known on as YAFSU. The search strategy process based on search and selection were considered as to be the pre-requisite of the framework, with regards to the extracted data and synthesis implementation. It is believed that the review may put impact on the researcher's with interest on chaotic cryptosystems based on images, to discover the input images, hardware and software facilities that should be considered for the experimental simulations. In addition, performances of existing encryption algorithms were analysed, to highlights ways to be followed in developing robust image encryption algorithm that may outperform the existing ones. The limitations of the reviewed literature were discovered, that some image encryption algorithm simulations suffered from fewer input images utilizations, which in many cases resolved to poor performance or in-efficiency of the encryption algorithm. Moreover, it was observed that no research exist to prove the claim "The effectiveness of the execution time depends on the Hardware capacity of the computer systems". Considering reviewed literatures, it was discovered that both Saleh et al and Mohamed et al. Used high capacity computers than that of Nadeem et al. But, various execution time obtained by the researcher's disproving the earlier claim.. It was recommended that more finding should be discovered based on utilization of many input images during the experimental simulation, which will assist in monitoring both the security and performance of the proposed encryption schemes. Both the gray/coloured images need a discovery that may clear the claim which said "The effectiveness of the execution time does not depend on the Hardware capacity of the computer systems".. in addition, it was observe that recent articles used older version of software tool being utilized during the experimental simulation. .

***Keywords*:** *Encryption Scheme, Experimental simulations, Images, Inputs, Hardware and Software, Cryptography*

1. INTRODUCTION

Cryptography explained the design and analysis of mathematical techniques that enable communication security of the sent data or Information [13]. The Data or information transferred could be either text, images, audio and video [16]. Sending information via shared networks may attract hacker's attention, since the information may be open and public. Confidentiality of the secured transmission of such information became a problem [16]. The information can be secured using cryptographical

schemes (algorithms) which will be solution to the stated problem, since cryptography is basically described as tool for communication security. Due to technological advancement, digital images are transmitted via network. Images such as military, intelligence and medical should be secured enough against intruders [6]. The present research get rids of writing a survey article that will concentrates on image encryptions schemes based on chaotic systems. Most proposed image encryption algorithms concentrate in pixel and frequency domain. It was discovered that encryption schemes impacted on the compression were not considered. To address the drawback, a researcher combines the advantages of DCT in compression and character of chaotic sequence to overcome such difficulty[49]. Therefore, since transmitted images need to be secured, it is also bellied that movable images such as video need to be secured likewise. Video are movable images which are presented with sounds popularly known as audio. Similarly, if the video needs to be secure during the transmission process, it will be good idea to get rid of securing the audio part as well, in order to prevent intruders in changing the Information. To transmit a video via network, high bit rate is required which is considered as a challenge, the research work by Hassan et al., removed the redundancies within video data using video compression [21]. The cryptographical requirements in the field of digital image encryption image was meet by chaos. Chaos and cryptography are closely related which make chaotic encryption algorithm natural for secure communication [36].

Chaos can be described as important character of non-linear dynamical systems which are applicable to various aspects of Science and Engineering [37]. Due to the character of chaos stated by Muhammad et al., it will be good idea if chaotic system can be applied to the field of communication due to its exhibition of chaotic behaviours. In 2018, ShanJun and Junli discovered that chaos was applied to the field of confidential communication due to dynamical system behaviour, its highly sensitive to noise that does not predict initial value and system parameters [49]. The Advent of chaos to the field of confidential communication, it is believed that the aspect of cryptography arises. As such, it will be concluded that chaotic cryptography is in to existence now days. In 2016, Mozhgan et al., [36] said that chaotic cryptographic algorithms have proposed efficient ways for data encryption scheme development. Furthermore, Ahmed et al., [3] describes that chaos encryption is among the best technique that enhance communication security. Similarly, Fatma et al., [16] describes chaotic-based ciphering as data protection that may be sent over public and shared communication networks. Although chaotic cryptography present high security properties, but it does not guarantee that all encryptions schemes must be successful, some may be unsecured. In 2019, Shuqin et al., [51] confirmed that some chaotic encryption schemes for image encryption have some insecurity problems due to short orbit of the digital chaotic system. However, it was discovered that image encryptions based on chaotic systems was considered efficient and exceptional encryption method due to properties and convergence of the chaotic maps [56]. In addition, Nadeem et al., [40] presented that large key space, unpredictability, ergo city and high sensitivity, contributed in making image chaotic encryption schemes productive and secured. However, it was discovered that most of the existing chaos-based image encryption algorithms adopted hyper-chaotic systems [57].

Table 1: Comparison of Chaotic and Cryptographic Properties [55]

Chaotic characteristic	Cryptographic property	Description
Ergodicity Topological mixing property	Confusion	The output of the system is similar for any Input.
Sensitivity to initial conditions and control parameters	Diffusion	A small difference for the input produces very different output
Deterministic	Deterministic pseudo randomness	A deterministic procedure produces pseudo-randomness
Complexity	Algorithmic complexity	A simple algorithm produces very complex output

The steps by step way of securing the sent messages were known be Algorithm, which are considered to be important aspect of cryptosystem. Since, the present survey considers the aspect of image encryption based

chaotic system. Therefore, the encryption algorithm will focus on chaotic Maps based on dimensions with regards to the mathematical expressions. However, for the algorithm to be valid and accepted by the academic world, one need to test for the validation. Testing the validity of any algorithm can be done through taking experimental simulations, which may required some component such as inputs, the hardware and software. Once the simulations has being carried out, the performance of the algorithm can be monitored based on the time complexity. As such, the researcher can be recommendation on the acceptability or not, for the proposed algorithms. At this junction it will good idea if, the survey can discuss the various input images being utilized during simulation for various encryption algorithms. Input images are the pre-requisite for the experimental simulations during the test of any algorithms. In most cases, these images were fetched from some database, either from intuitions, university and hospitals. It was discovered that, the images are seen to appear in different sizes and capacity. But, due to the investigations, most of the researcher often mentioned that the capacity of the images affect the simulations. That means, the higher the capacity, the higher the time execution it takes. Similarly, the sizes also affect the time of the simulation as well, smaller sizes executes faster than the higher ones. However, the sizes and capacity of the input images should consider the both the hardware and software capacity of the computer device being utilized for the experimental simulation.

1.1. Relationship Between Cryptography And Chaos

Their exist relation between the properties of cryptography and that chaotic systems following a discovery by the existing literatures. The survey presented the relationship at Table 1, together with some discussions that highlight the connections of both the properties. The confusion property is directly connected with mixing property for the topology of the ergodicity, the diffusion is connected to the control parameter and sensitivity to initial condition was connected to. Both chaotic systems and cryptography are discovered to be deterministic that happens to be pseudo random in nature. Investigations reveal that chaotic systems are said to be deterministic for the known parameters. Hence, when the initial conditions are known, then chaotic system are said to be deterministic [31]. However, it was discovered that random output which are unique in nature can obtain when strong cryptosystems. Secured encryption can be obtain, researcher's are to employ confusion and diffusion properties. Majid et al., has proved the earlier claim, that chaotic cryptosystem should consider both confusion and diffusion stages, assumed to operate on square measuring [24]. At the encryption process, permutation method was applied to the plain images without affecting the pixels value. In contrary, diffusion operates as the reverse of the confusion, the key during the confusion stage were obtain from the parameters of chaotic map considering value of the initial conditions [16].

1.2. Comparative Analysis With Existing *Review Articles*

In addition, it was observed that, the review paper have analysed the existing review articles that relate to the applicability of chaotic system. The section of the article has being provided to take a comparative analysis with the existing survey/review articles. Table 3 highlighted some of the discovered limitations, which are assumed to be addressed by the present review article.. It was discovered that, some of the review articles that were in to existence failed to discussed the aspect of chaos and cryptography [12, 16, 32, 43 and 50]. Moreover, it was investigated that some review articles failed to present discussion on components of the cryptosystems, which includes input images, hardware and software utilization, the algorithm formulation. However, investigations reveal that some research articles were discovered to have weak references [10, and 12]. Moreover, some researcher's failed to mention the research limitations, so as to have suggestions for future research [48]. On the other hand, Berg et al. [8] took a survey based on the science of physics with regards to chaotic system. Moreover, Shafali [48] have focused a review article on the basis of chaotic systems, but the researcher failed to consider general form of chaotic maps with respect to the image encryption algorithms. The researcher, consider only, Arnold, Baker, Henon, and logistic Maps for most of the developed algorithms. In contrast, the present review has addressed the earlier mentioned limitations that exist within the consulted review articles. Table 2 have summarized the discussion on the, how such

difficulties have been addressed. The present review considers the existing relationship between chaos and cryptography as summarized within table 2. The relationship was discussed based on the two properties such as, confusion and diffusion.

2. METHODOLOGY

Information is said to be vital to every human being that are required for survival. Now days, technological advancement have assisted many people in fetching information, with aid technological devices. These information are considered to be useful, which can be shared through networks assisted by some devices such as computers devices (desktop and laptop devices), mobile device to mention a few. It was discovered that due to hackers or intruder that may try to access the sent information, the information need to be secured for authentication from both the sender and receiver of the information. The security of the shared information is considered to be vital, in order to be able to receive correct and reliable information. As such, the idea of hiding the shared was initiated, popularly known as cryptography. However, it was observed that chaos can be applied to the aspect to cryptography, in order to secure the shared information sent via networks. The shared information may be either plain text, images and vedio clips. Considering the literatures, it was observed that many researchers' were conducted to explore chaotic system based on cryptography with regards dimensional maps [2, 4, 15, 17, 18, 25, 27, 35, 36, 48, and 58]. For a research to be reliable, it have to consider the systematic review of the current researcher's that do exist. The present research took review analysis on the components of cryptosystem with regards to relationship chaotic systems and cryptography. The paper tried to analyse the input images that were utilized for the experimental simulation with regards to uts performance. In addition, the hardware and software were also analysed based on the execution speed. Similarly, the encryption algorithms were also analysed to discover the performance of each individual research work. The researcher fetched out the existing research that were based on image encryption with regards to chaotic systems. The study exposed the basic chaotic systems, how it was utilized for the encryption and decryption techniques, based on the components of cryptosystems. Some of the limitation of the previous research's were discovered, and recommendation for feature work were describe at the conclusion section of the papers. The researcher followed some steps to facilitate the systematic review process such as: The search strategies definition; Primary studies selection; Data extraction and synthesis strategies implementation.

2.1. Search Strategy/ Search Process

Related articles were searched considering the field of study, the articles were considered between the years 2015-2022. The selections of the articles were based on the searched topic, the researcher considered most relevant literatures, that were closely related to the searched topics. The researcher adopted two processes such as search process and study selection, during the selection and search process. Hence, the search strategy was describes by the scope, involvement and criteria of the outcome. In addition, the search strategy was described as scope, involvement and outcome criteria. It was observed that the search strategy can be assisted using the searching and selection processes. However, Chaos systems, cryptography, security behaviour based on cryptosystems were considered to be the searched terms. Therefore the researcher defines the search strings by evaluations of the probable searched terms options

A. SEARCH PROCESS

The research describes search process based on two phases such

Primary Search: During the primary search, the researcher considered atleast 30 online database that contain either journal or conferences research articles. The online database comprises of goggle scholar, Springer, Elsevier, MDPI, IEEE, ACM, Research gate, Spie Digital to mention a few.

Secondary Search: at the point of the secondary search, the researcher performed through review for the cited references based on the primary search. The researcher determined previously selected literatures within the relevant citation.

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

B. STUDY SELECTION

At the selection process, the researcher is more concern with the followed criteria at the selection process, at this moment, the inclusive and exclusive technique was employed at the selection process, which assisted the researcher for most appropriate research at the process of the systematic review.

Selection of primary studies: The primary studies selection, 200 journals/conferences articles were selected. The selection was undergone through the use of some keywords such as "Chaos System", "Cryptography", "Applicability of Chaos". Out of 200 articles, 59 research articles were selected.

2.2. Extraction Of Data

A well designed data extraction form was created, which enable the researcher to keep records of the obtained information from the search engine. The form can be utilized as a database, showing the information of the fetched articles. The database is comprised of a table that contain 11 rows and 4 columns. The stored information is paper title, authors-name, and database engine that papers were obtained. A total of 200 articles were obtained, based on inclusion and exclusion criteria. The researcher accepted 55 articles for the review process. Secondary search was applied to four (4) articles, which are added to the former 55 accepted articles, which produces 59 articles. Details of the article based on the primary searched were displayed in table 2 below.

Moreover, the present review have presented overall framework of the methodology known as YAFSU, shown in figure 1 below. The framework gave the pictorial presentation of the method applied during the review process. It will not be necessary, for a researcher to read the detail discussions on the methodology, since the framework is added.

Table 2: Fetched Articles based on Primary Search

Database	Found Articles	Selected Article	Duplicate Articles
Springer	41	10	10
Elsevier	8	3	2
Research-Gate	31	11	8
MDPI	8	3	2
IEEE Explore	49	15	12
ACM	3	1	1
Spie Digital Library	3	1	0
Korea Science	3	1	1
Google Scholar	54	14	14
Total	200	59	50

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

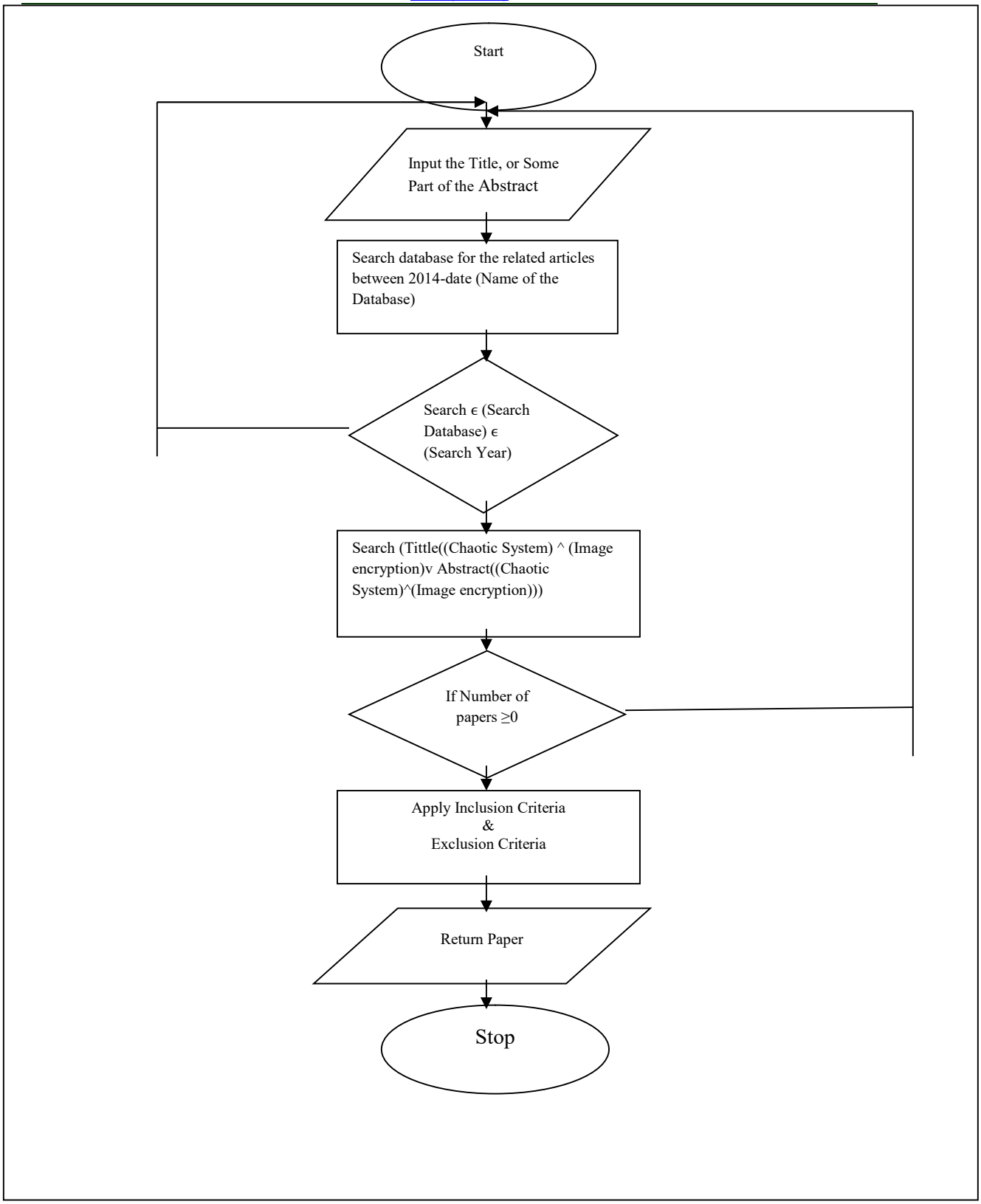

Table 3: Comparison of the Review papers on Chaos

	Authors	Limitation of the existing Survey	Present Review
1	[48]	The Chaotic Maps based on the dimensional systems were not discussed. The relationship between Chaos and Cryptography Need further Discussions. The Components of cryptography was not discussed	The Survey Classified the Chaotic Maps based on Dimension. The Survey Paper Discussed the Relationship Between Cryptography and Chaotic Systems. The Components of cryptosystem were discussed
2	[2]	. The Components of cryptography was not discussed	The Components of cryptosystem were discussed
3	[56].	The Chaotic map was not discuss based on the dimensional system Most of the research articles used during the review process are out of date. The Components of cryptosystem was not discussed	The Survey Classified the Chaotic Maps based on Dimension. The present survey used recent articles. The Components of cryptosystem were discussed
4	[54]	Lack discussions on Chaotic dimensional Systems. The Components of cryptography was not discussed	The Survey Discussed Chaotic Systems based on Dimensions The Components of cryptosystem were discussed
5	[12]	The chaotic Maps were not classified based the dimensional system. References for survey paper are weak The Components of cryptosystem was not discussed	.Chaotic maps are classified based on dimensions. Recent references were utilized The Components of cryptosystem were discussed
6	[30].	The Components of cryptosystem was not discussed	The Components of cryptosystem were discussed
7	[13]	The reference within the research paper were not up to date The Components of cryptosystem was not discussed	Up to date reference are utilized. The Components of cryptosystem were discussed
8	[57].	The researcher only focused on Arnold Affine, Baker, Henon, and Logistic Maps only. No Recommendation for future work. The Components of cryptosystem was not discussed	. The survey focused on most frequently chaotic Maps in general. Recommendations for future work was stated The Components of cryptosystem were discussed
9	[73]	The Components of cryptosystem was not discussed	The Components of cryptosystem were discussed
10	[25]	Logistic map was Only Discussed. . The Components of cryptosystem was not discussed	Discussed chaotic map based on their Dimensional systems. . The Components of cryptosystem were discussed
11	[10].	The Components of cryptosystem was not discussed	The Components of cryptosystem were discussed
12	[37].	.Lack Discussion on relationship between Cryptography and chaotic Systems. The Components of cryptosystem was not discussed	The Relationship between Cryptography and Chaotic Maps were discussed. The Components of cryptosystem were discussed
13	[14]	The Components of cryptosystem was not discussed	The Components of cryptosystem were discussed
14	[15]	The Review did not classify the chaotic systems-based dimensions. The Reviewer Consider Lorenz; Logistic; Henon Chaotic Maps. Most the references were out of date The Components of cryptosystem was not discussed	The present Survey Discuss the Mathematics behind Chaotic system based on Dimensions. The Reviewer considered popularly known chaotic maps. The Reviewer used Most recent references The Components of cryptosystem were discussed
15	[66].	Even though the researcher discussed chaotic systems, but failed to present respective chaotic system based on dimension.	Chaotic system were discussed based on dimensional maps. The Components of cryptosystem were discussed

		The Components of cryptosystem was not discussed	
16	[12]	The Survey Discussed the Physics aspect of Chaos. The Components of cryptosystem was not discussed	The Survey was carried out based on the crypto graphical aspect of Chaos. The Components of cryptosystem were discussed
17	[36].	Did not give detail discussion on the chaotic system classification based on dimensions. The Components of cryptosystem was not discussed	Chaotic system was discussed based dimensional maps. The Components of cryptosystem were discussed
18	[10]	Lack Discussion on Cryptography and chaotic Systems relationship. The Components of cryptosystem was not discussed	Discussed the relationship between cryptography and chaotic maps. The Components of cryptosystem were discussed

3. COMPONENTS OF CRYPTOSYSTEM

3.1. Input

A. GRAY IMAGES

It was discovered that, image encryption algorithms can be validated with the aid of an experimental simulations, which may require the usage of different input images, that may appears at different sizes and capacity. At this junction, the present survey will be classifying the input images based on either gray or coloured. In addition, the survey took tentative analysis on the input images, based on the existing image encryption literatures. Considering the literatures, it was investigated that some literatures couldn't present discussions on the input images being utilised during experimental simulations [58, 44]. In addition, the various sizes of the input images were not highlighted at some various literatures [19, 25, 37, 30, 38 and 47]. To address the earlier limitations, it was discovered that some literatures describes the input images with respect to their sizes. In 2016, Standard Lena images were utilized for the experimental simulation during the image encryption process, the images took the sizes of 512 x 512 respectively [36, 56]. To determine the performance of the encryption algorithms based on execution time, was considered to be difficult, as both the researcher's failed to describe the time complexity. Similarly, [53] failed to describe the execution time during results discussion. Even though, the researcher used 2 images (Cover images & Logo Images) in contrary to the earlier research. To address the earlier limitations, Chengqi et al., [11] proposed encryption scheme that executed within a speed of 133ms. The algorithm operates on 2-gray that appears to maintain a size of 256 x 256. In addition, Xiao et al., [57] used standard Lena images for its experimental simulation based on the images sizes of 512 x 512. The authors reveal that the proposed encryption scheme executed within a time of 147 ms. Therefore, it was discovered that the higher sizes images take a lot of time for its executions. To prove the claim, Xiao et al., presented higher executing time than that of Chengqi et al.

Recently, Saleh et al., [46] discovered that the use of more than two input images create better execution time during the experimental simulations. These claimed was proved, as the researcher utilized three input images for its experimental simulations such as CT scan (750 x 870); MRI (512 x 512) and X-Ray (1338 x 1094). The author, obtained 91.4MB/s as execution time, possessing better performance than those with two images. Moreover, it was investigated that the higher the input, the faster the execution it becomes. To prove the claim, it was discovered that Nadeem et al., [39] used four gray images by maintaining the same size of 256 x 256 respectively. The input images comprises of Clock, Baboon, Moon and Chemical Plant. The experimental simulations produces execution time of 0.185s. Similarly, the same researcher used four input images such as Ct Para nasal; Pair of Carnival; Ct Abdomen; Knee. The researcher obtained 0.0053MBps as the corresponding execution time. Furthermore, it was investigated that some experimental simulations were undergone with eight images of 256 x 256 by size. The inputs include Lena CameraMan, Pepper, baboon; Lena, Deblur, Mandrill, Pepper [13 and 29]. The author's records execution time of 0.2029MBps and

0.15827(without SI Units). However, Hossam and Aly [22] failed to describe the execution time, despite the utilisation of 10 input images for the experimental simulations. One may challenge that the literature was published at year 2017. Therefore, more work need to be done for researchers with the research interest within the relevant field, that may enhanced findings on experimental simulations beyond that of Hossam and Aly. Table 4 present the summary of the review articles based on gray images with respect to execution time.

Table 4: Gray Input Images

	Author's	Input Image	Time
1.	[7]	2 Gray Images (256x256)	133ms
2.	[13]	Lena; CameraMan; Pepper; Baboon; Deblur; Mandrill; Pepper (256x256).	0.2029MBps
3.	[15]. "	Cell; Penguin; Girls ; Nike; TestPat; Pirate; Mandi; Moon; Cameraman and Couple (256x256).	NIL
4.	[20].	Lena; CameraMan; Pepper; Baboon; Deblur; Mandrill; Pepper (256x256).	0.15827, but no unit
5.	[26]..	Standard Lena (256x256)	NIL
6.	[30].	Clock; Baboon; Moon; Chemical (246x256)	0.185s
7.	[31].	Ct Paranasal; Carnical; Ct Abdomen; Knee (256x256).	0.0053MBps
8.	[35]. "	Ct Scan(750x870); MRI(512x512); XRay(1330x1094)	91.4MB/s
9.	[40]	Cover(512x512); Logo(256 x256)	NIL
10.	[41]	Standard Lena (512x512)	147 ms
11	[43]	Standard Lena (256x256)	NIL

C. COLOURED IMAGE

To balance the discussion on input images, the present survey has key in to consideration on some relevant discussions with regards to colour images. But, investigations reveal that some literatures failed to describe the input images utilized for the experimental simulations. Ja' afar et al., [24] has proving the claim by discussing the results of its experiment, without describing the input images being utilized. In contrary, the existence of literatures that presented the input images for the simulation was considered to be solution to the earlier problem [3, 7, 15, 28, and 31] utilizing standard Lena images as Input for the experimental simulations. As mentioned earlier, the performance of the execution lies on the capacity of the input images. As such, the survey discovered literatures that used more than one input image for simulations. Tripirneni et al., [53] took an experimental simulation using two coloured images such as Logo with a size of 256 x256 and cover with size of 512 x 512. Even though, it was expected to have better execution time than the earlier research. But, the authors, failed to discuss the time complexity during the result interpretations. To address the difficulty, Nestor et al., [41] obtained an approximate execution time of 0.5916s, when the researcher used three input images maintaining the sizes such as 256 x 256. Moreover, Fatma et al., [16] carried its experimental simulations with aid of four coloured images such as Lena, Baboon, Plane and Men respectively. It was discovered that the researcher obtained execution time of 0.5642s faster than that of Nestor et al. Similarly, Manjit et al., [32] presented execution time of 0.0307s faster than all the earlier simulations, when the researcher used Wild (256 x 256), dance (512 x 512), Manipal-Unversity-Jaupur (1024 x 1024) and Bird (2048 x 2048) as input images respectively. Therefore, the claimed which said that the use of larger amount of input images lead to the presentation of better execution time has being proved. In addition, Nadeem et al., [40] outperformed the earlier mentioned literature, presenting 0.0053MBps as the execution time, when six images were utilized as input for the experimental simulations. The authors used Lena, Baboon, Girl, Tree, House and Beans, both the images maintain the same sizes of 256 x 256 respectively. Table 5 present the summary of the reviewed articles based coloured images with respect to their execution time.

Table 5: Coloured Input Images

	Authors	Input Images	Time
1.	[10].	Lena, Baboon,	0.5642s

		Plane and Men	
2.	[23]	used Wild(256 x 256), Dance (512 x 512), Manipal-Unversity-Jaupur (1024 x 1024) and Bird (2048 x 2048)	0.0307s
3.	[31]	Lena, Baboon, Girl, Tree, House and Beans, (256 x 256)	0.0053MBps
4.	[33]	three input images (256 x 256)	0.5916s
5.	[40]	Logo(256 x256); Cover (512 x 512)	NIL

3.2. Hardware Components

A. GRAY IMAGES

Computer Hardware is among the pre-requisite for any experimental simulation. The survey highlights some key areas of the computer capacity to be utilized during the simulation process, such as Hard disk, RAM, the Processor. These utilities need to be access before a researcher concludes for the acceptance of any computer utilization, which may be used during the experimental simulations. It is added that, hardware components are considered to be crucial components of a computer system, which need be considered during any experimental simulations. It was discovered that, most of the experiment simulation yield positive result, when higher capacitated computers are taken in to consideration. The present survey critically analysed the existence of some literatures that utilizes hardware components during the experimental simulations. Considering the consulted literatures, it was discovered that some literatures failed to describe the hardware utilizations during the experimental simulations. Considering the reviewed literatures, some encryption schemes that are based on gray images, failed to describe the hardware components that was utilized during the experimental simulation [19, 25, 36, 49, 56 and 58]. However, the existence of some literatures that discussed the hardware components for experimental simulations have cleared the difficulty of the aforementioned drawbacks. Sathishkumar al., [47] used a computer system with a specification of CPU@2.2GHz Pentium IV, 4GB RAM, showing good performance when compaired to some related literatures, executing the simulation within 45s.

In 2017, Xiao et al., [21] used an equipped computer device with specification of Intel Duo-core CPU@2.27GHz Pentium II and 2GB RAM memory. The simulation was executed within 147ms, it was clearly seen that the simulation executes faster than that of Sathishkumar et al. Even though, Sathishkumar et al., used a computer device that possess better hardware components than that of Xiao et al. But, ideally it was believed that the higher the capacity of the hardware, the faster the execution it becomes. Therefore, the present survey focuses on investigation of the reviewed article, in order to prove the earlier claim. Chengqi et al., [11] consider using a computer with hardware specification such as Intel Duo-core CPU@2.27GHz Pentium II, with 2GB RAM memory and 200GB hard disk. It was discovered that the experimental simulation took 133ms to execute. It was observed that the researcher used a computer with higher capacity than that of Xiao et al., which also show better performance. In contrary, [53] took it experimental simulation with an equipped computer, based on hardware component of Intel Core i3 CPU@3.0GHz, 4GB RAM, 500GB. Even though the researcher utilized a high capacity computer, but the execution time was not described within the literature. As such comparison cannot be done with existing work. Moreover, K.shankar et al., [27] also to failed the discussed the execution time, the comparison with other related article was not possible, even though the researcher used high capacity computer based on some computer hardware components such as Intel Core i5 CPU@3.0GHz, 4GB RAM. It was discovered that another literature discussed it experimental results without the performance analysis, even though it present a capacitated computer with hardware components such as Intel Core i3 CPU@3.0GHz, 3GB RAM, 500GB hard disk [30].

In 2020, Nadeem et al., [39] was equipped with a computer device that executed on certain hardware specification such as Core™ i5-4210U CPU@2.40GHz, 8GB RAM. The authors reveal execution time of 0.185s, considered to perform better than the aforementioned simulations. In contrary, Saleh et al., [46] has cleared the argument, saying that the performance an

encryption algorithm did not depend on the computer system capacity. It was discovered, that the authors utilized computer with higher capacity hardware components such as Intel Core i7 CPU@3.6GHz and 32G RAM. The experimental simulation records execution time of 91.4MB/s, which reveal better performance than the Nadeem et al. Therefore, it is shown clearly that higher capacity computer has higher tendency of producing better execution time than the lower ones. In addition, it was discovered that faster execution time was obtained showing faster performance than that of Sale's simulation [34]. The author utilized a computer with hardware specification of Intel Core i7-7700 HQ processor and 16GB RAM, that produces average execution time for three images as 40.9ms, assumed to be faster than that of Xiao et al. and Chengqi et al. In 2021, Haotian et al., have carried out a recent research showing the executions time appears to be lower than Saleh et al. and Mohamed et al. simulations. Even though the researcher used higher capacity computer with following specification Intel(R) Core(Tm) i7-8650 CPU@2.11GHz with 8GHz RAM. But, it failed to outperform the mentioned simulations. Therefore, it was observed that recent literature used higher capacity computers for the simulations. But, it was discovered that the execution time was not encouraging. As such, it can be recommended that coloured images need to be reviewed, so as to analyse the impact of the hardware capacity. Table 6 present the summary of the discussion.

Table 6: Hardware Components For Gray Images

	Author's	Input Images	Hardware	Time
1.	[7]	2 Gray Images (256x256)	Intel Duo-core CPU@2.27GHz Pentium II, with 2GB RAM memory and 200GB hard disk.	133ms
2.	[13].	Lena; CameraMan; Pepper; Baboon; Deblur; Mandrill; Pepper (256x256).	Intel(R) Core(Tm) i7-8650 CPU@2.11GHz with 8GHz RAM	0.2029MBps
3.	[14].	Standard Lena (512x512)	Intel Duo-core CPU@2.27GHz Pentium II, with 2GB RAM memory	NIL
4.	[18].	NIL	Intel Core i5 CPU@3.0GHz, 4GB RAM.	NIL
5.	[21].	NIL	Intel Core i3 CPU@3.0GHz, 3GB RAM, 500GB hard disk	NIL
6.	[24].	Barbara; Boat; Clown; Lena (256x256)	Intel Core i7-7700 HQ processor and 16GB RAM	40ms
7.	[30]	Clock; Baboon; Moon; Chemical; Plant (256x256).	Core™ i5-4210U CPU@2.40GHz, 8GB RAM	NIL
8.	[35].	Ct Scan(750x850); MRI (512x512); XRay(1338x1090)	Intel Core i7 CPU@3.6GHz and 32G RAM	91.4MB/s
9.	[36].	NIL	CPU@2.2GHz Pentium IV, 4GB RAM,	45s
10.	[40].	Cover(512x512); Logo(256x256)	Intel Core i3 CPU@3.0GHz, 4GB RAM, 500GB.	NIL
11	[41]	Standard Lena (256x256)	Intel Duo-core CPU@2.27GHz Pentium II and 2GB RAM memory	147

B. COLOURED IMAGES

Now, it's high time to look into the various hardware components for the coloured based simulation. Considering the reviewed literatures, it was discovered that some literatures failed to present discussions on the utilized hardware components during experimental simulations [3, 15, 24, 28 and 31]. To address the limitation, it was observed that there exist some literatures that describe the computer specification for the simulations [16, 23, 25, 28, 31, 33, 40 and 63]. In 2015, Fatma et al., [16] took an experimental simulation with a computer

that possesses hardware components such as Pentium IV CPU@3GHz, 160GB Hard Disk, 512MB RAM. The simulation took 0.5642s of execution time, even though the researcher used lower capacity computer, but it obtained better execution time than that of Muhammad. Muhammad et al., [37] that recorded an execution time of 1.95425s when the experiment was simulated with a computer that utilizes hardware specification of Intel(R) Core(TM) i7-3740QM CPU@2.70GHz , 8GB RAM and 500GB Hard-disk. Arguments occurred that, it is mandatory for the high capacity computers to perform better, during the experimental simulations. As such, the present survey will take a little analysis, in order to prove the claim. But, it was discovered that, some literature failed to describe time taken during the execution process [35, 53]. Mollaeefar et al., [35] failed to describe the execution time irrespective of the experimental simulations. The authors utilized a computer device with hardware specifications such as Intel Core i5-6200 CPU@2.30GHz with 4GB RAM. Similarly, Tripirneni et al., [53] failed to deliver the time taken to executes the experiments, when a computer devices with hardware specification of Intel Core i3 CPU@3.0GHz , 500GB Hard Disk, 4GB RAM, was utilized. Therefore, it can be clearly stated that the performance of the hardware cannot be determined when the execution time of any simulation is not presented.

To address the earlier limitations, Nadeem et al., [40] has conducted analyse on a proposed encryption algorithm based on computer utilization. The execution time clears the argument, which says lower capacity computers can be predicted to produce better execution time. The authors records 0.0053MBp execution time, when a computer with a specification of Intel(R) Core(Tm) i5-4210CPU@1.70GHz, 8GB RAM was utilized for the simulation [40]. In contrary, investigations reveal that some researchers obtained higher execution time, when higher capacity computers were utilized during experimental execution [63]. The author, have recorded 1.1967 execution time, when a computer with hardware specification such as Intel(R) Core(Tm) i5-6200CPU@2.3GHz with 4GB RAM was utilized. Nestor et al., [41] records execution time of 0.5916, seen to have better performance than that of Roayat. The execution time was obtained, when the researcher used a computer device with a hardware specification of Intel Corei5 CPU@2450M with 6GB RAM. However, Manjit et al., [32] records 0.0307s execution time, when a computer with hardware components is utilized such as Intel(R) CPU ES-2630V4 CPU@2.40GHz with 16GB RAM. . The execution time was considered to perform better than that of Nestor et al. As such, need arises for a research that may outperform the execution time of Manjit et al. However, since the survey has discussed much on hardware component of the utilized computers, it has come to a junction that software components need to be discussed. Both of them operated collectively with each other. Table 7 below presented the summary of reviewed articles that discussed hardware component for coloured images

Table 7: Hardware Components For Coloured Images

	Authors	Inputs Images	Hardware	Time
1.	[16].	Lena; Baboon; Plane; Men (256x256)	Pentium IV CPU@3GHz, 160GB Hard Disk, 512MB RAM	0.5642s
2.	[23].	Wild(256x256); Dance(512x512); Manipal University Janpur (1024x1024); Bird(2048x2048).	Intel(R) CPU ES-2630V4 CPU@2.40GHz with 16GB RAM,	0.0307s
3.	[25].	Standard Lena (256x256)	Intel Core i5-6200 CPU@2.30GHz with 4GB RAM	18.6ms
4.	[28].	Lena; Baboon; Vegetable; Crane; Elephant; Butterfly; Bird; Wheelbarrow; Radio; Telescope; Brain (256 x 256).	Intel(R) Core(TM) i7-3740QM CPU@2.70GHz , with 8GB RAM and 500GB Hard-disk.	1.95425s
5.	[31]..	Lena; Baboon; Girl; Tree; House; Beans (256x256)	Intel(R) Core(Tm) i5-4210CPU@1.70GHz, 8GB RAM [31].	0.0053MBps
6.	[33].	IMG1; IMG2; IMG3 (256x256)	Intel Corei5 CPU@2450M with 6GB RAM	0.5916s
7.	[63].	Baboon; pepper ;	Intel(R) Core(Tm) i5-	1.1967

		Lena; House (256x256).	6200CPU@2.3 GHz with 4GB RAM	
8	[40]	Cover(512x512); Logo(256 x256)	of Intel Core i3 CPU@3.0GHz , 500GB Hard Disk, 4GB RAM,	NIL

3.3. Software Components

A. GRAY IMAGES

Software components works together with hardware for a successful execution of any experimental simulation. The survey discussed software utilizations during the execution process for the reviewed literatures. Observations reveal that some of the existing literatures failed to describe their software utilization during the result interpretation of the experimental simulations [19, 25, 29, 36, and 49]. In addition, it was discovered that some literature presented the software utilization without the versions. The earlier mentioned difficulties were addressed, due to existence of research article that critically discussed the software utilization in detail. During the experimental simulations, it was noticed that, various software's were supported by different operating systems considering the reviewed literatures, it was investigated that some authors failed to describe the supported operating system utilization, during the experimental simulations [11, 20, 39, 46, 57, 52, and 56]. In 2015, Sathishkumar et al., [57] simulate its experiment with aid of MATLAB based on version 7.6. The authors records 45s execution time, which assumed to perform better than Zia et al., [56] since the execution time was not stated. After long period of time, a new version 2017a was discovered and utilized by [53] which was considered to be the latest version at that time. However, it was analysed that latest research on image encryption used MATLAB based on version R2016b [52]. The research was conducted at the year 2020, but version of the software used during simulation was considered to be out dated. As such, the effectiveness of the output may be affected

In Contrary, Muhammad et al., [34] have challenged the earlier mentioned drawback, by introducing MATLAB software 2018b for the experimental simulation. The authors use the latest MATLAB software than the earlier mentioned literatures. Findings reveal that the software version used, may affect the execution time of the encryption algorithm. However, some researcher's consider other simulation software's rather than MATLAB [46 and 57]. In 2017, Xiao et al., [57] took its experimental simulation with Visual C^{++}. It was observed that the researcher obtained execution time of 147 ms, considered to be effective and perform better than earlier researcher's, which utilized MATLAB software, for their experimental simulations. Considering the reviewed literatures, it was investigated that Xiao et al., [57] was the only literature that used C^{++} for execution of its experiment simulations. . However, Saleh el al., [46] used Java SE 1.8 virtual machine during its experimental simulation. It was discovered that, Java appears to execute faster than MATLAB and C^{++}. The author's records execution time of 91.4MB/s higher than the earlier researcher's. At this junction, the survey discusses literatures that were able to present operating systems utilization for executing their experiments simulations. In 2018, an encryption algorithm was simulated with a MATLAB version2013a under window operating system platform [30]. Recently, Nadeem et al., [39] Runs its executions under the operating system of window 10. The author used MATLAB version R2016 during its simulation, which records execution time of 0.185s. Even though, the authors records good performance for its execution. But, it was discovered that the research was carried out at the year 2020, instead of utilizing latest version that exist, the researcher move to utilize version 2016. In contrary, Haotian et al., [20] simulated its experiment with MATLAB without presenting its version and supported operating system. But, the researcher recorded a better performance of 0.2029MBps than the earlier works. In other words, Karim et al., [29] addressed the difficulty by introducing the utilized operating system. But, failed to present the software that was utilized for the experimental utilization. However, the survey tried discover the coloured images, analyse the drawback, give discussions on the relevant software utilization with respect to the performance. Finally, recommendations were giving for further research. Table 8 present the summary on the discussions for software components based on gray scale images.

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 8: Software Components For Gray Images

	Author's	Input Images	Soft-ware	Time
1.	[13].	Lena; CameraMan ;Pepper; Baboon; Deblur; Mandrill; Pepper (256x256).	MAT-LAB	0.2029MBps
2.	[20]	Lena; CameraMan; Pepper; Baboon; Deblur; Mandrill; Pepper (256x256).		0.1527 no unit
3.	[21]	NIL	MAT-LAB, 2013a	NIL
4.	[24]	Barbara; Boat; Clown Lena (256x256)	MAT-LAB, 2018b	40ms
5.	[30].	Clock; Baboon; Moon; Chemical (246x256)	MAT-LAB, R206	0.185s
6.	[35]	Ct Scan (750x870); MRI(512x512); XRay(1330x1094)	MAT-LAB	91.4 MB/s
7.	[36].	NIL	MAT-LAB, 7.6	45s
8.	[39]	CT Paranasal; Cervical X-Ray; CT Abdomem; Knee X-Ray (256x256).	MAT-LAB, R2016b	332in s
9.	[40]	Cover (512x512); Logo(256 x256)	MAT-LAB, 2017a	NIL
10.	[41]	Standard Lena (512x512)	C++	147 ms
11.	[43]	Standard Lena(256x256)	MAT-LAB, 2015	NIL

A. COLOURED IMAGES

It was observed that some of the coloured encryption algorithm failed to describes the software tool used during the experimental simulation [4, 15, 16 and 31]. Considering the literature, the earlier problem was solved, due to the existence of some research articles that deeply discussed the software utilizations for the experimental simulations [3, 24]. Both the authors used a MATLAB for simulating the proposed encryption algorithm, without stating the software versions. As such, if the version of the software is not known, the performance may not be assessed. Therefore, it will be good idea for researcher's to state the detail discussion on the software utilization, in line with the version. Mollaeefar et al., [35] used version R2013b MATLAB that operates on Window 7 of a notebook device. The author records an estimate execution time of 18.6ms during its experimental simulation. Recently, Nadeem et al., [40] used a MATLAB version 2016 that operates on 64 bit operating system, which consider to be up to date than the earlier research. It was discovered that the researcher records execution time of 0.0053MBps, which appears to be better the earlier mentioned research work. But, it was observed that the researcher used old version of the MATLAB, since version 2018 was in existence. Manjit et al., [32] deal with the above problem, by employing the version 2018a for its simulation. But, it was observed both Nadeem et al., and Manjit et al. articles suffered from lack of the discussions on the supporting operating system. Roayat [44] have cleared the arguments, by simulating the experiment with aid of the software supported by the operating system. It was clearly, stated that the researcher used a MATLAB Version 11 based on computer devices that operates on window 10. The researcher records execution time of 1.1967 without the S I Units. Even though, the researcher used latest version software for the simulation. But, the execution time was not that effective than the earlier research. As such, it can be concluded that the not all time latest version software perform better than the older versions. Therefore, some research work needs to be undergone to show that latest version software are more efficient than the older ones. Table 9 present the summary on the discussions for software components based on coloured images

Table 9: Software Components For Coloured Images

S/N	Author's	Input Images	Software	Execution Time
1.	[13].	Lena; CameraMan; Pepper; Baboon; Deblur; Mandrill; Pepper (256x256).	MAT-LAB	0.2029MBps
2.	[16].	Lena; Baboon; Plane; Man (512 x 512)	MAT-LAB	
3.	[23].	Wild (256x256); Dance (512x512); Manipal University Janpur (1024x1024); Bird (2048x2048).	MAT-LAB, 2018a	0.0307s
4.	[25].	Standard Lena	MAT-LAB,	18.6ms

		(256x256)	R2013b	
5.	[31].	Lena; Baboon; Girl; Tree; House; Beans (256x256)	MATLAB, 2016	0.0053MBps
6.	[63].	Baboon; pepper; Lena; House (256x256).	MAT-LAB, V11	1.1967

3.4. ALGORITHMS

A. GRAY IMAGES

In 2018, K Shankar et al., [27] introduced an efficient encryption scheme that operates based on optimal key. The algorithm was chaotic based on C-functions with XOR that enable it security. The security of the algorithm made the cipher image to be un-predicted. The limitation of the research was the use of 1-Dimensional maps for the algorithm formulations. The performance of the algorithm cannot be assess, since the researcher failed to describe the execution time within the article. Similarly, Mohamed et al., [34] developed the proposed encryption algorithm with the 1- Dimensional chaotic map known as cosine fractional map, which operates based on Lena images. The Simulation took different direction, as the researcher utilized Lena images for the executions. 40ms was recorded as execution speed, which addressed the earlier limitation, and assumed to perform better. Even though the input image differs, but cannot address its limitations. It was observed, that more work need to be put in place that may use several input images. However, considering the reviewed literature, the survey, came across a research article that used two (2) dimensional chaotic map during the development of its encryption algorithm, such as logistic and Lorenz maps. In addition, [49] utilized logistic and discrete cosine function based on chaotic map. The maps were used to develop an encryption algorithm in compressed formats. The compressed performance of the image was combined with chaotic sequence for the algorithm to operate smoothly. The operations of the algorithm is based 5 steps such as DCT processing; Compression; Displacement Encryption; Symbol Encryption; Repeat step 3-4 until encryption sequence is obtained.

Similarly, Hai et al., [19] adopted a 2-dimensional logistic map to create a hyper chaotic encryption algorithm. The encrypted image can be produced as follows: the plain images are converted to pixels points; Pseudorandom sequence was generated to obtain M_2; Now M_2 converted to pixel point; Then, column and row permutation was performed to produce the encrypted image. But, the performance of the algorithm cannot be assess, since the researcher failed to describe the execution time. Saleh et al., [46] have addressed the limitation by obtaining execution time of 91.4MB/s, when the researcher introduced a framework for the medical image encryption that gave the privacy to patients. The framework was developed based on chaotic maps, which depend on the key and construction of the S-box. The algorithm was giving in 7 steps such as: construct the Dynamic S-Box based on the generation of two none using PRNG; initialize chaotic sequence C; C was iterated N_T Times; chaotic sequence was initiated bad C; C_k was calculated based on conditions such as C_o=0 where

Table 10: Algorithm for Gray based Images

	Authors	Chaotic maps	Algorithms	Execution Time
1.	[7]	2-Dimensional maps	At the **initialization** stage is as follows: iterates $\frac{L+4}{4}$ for the CPLM taking initial values as (x, y, z, v_0) to produce sequence that appear to be pseudo-random in nature; positive and integer sequence such as b_i and x_i are obtained. The **Permutation,** real sequence is obtained; circular operation were executed with matrix $B_{(i,j)}$ =0;. The **diffusion** stage, it is required to obtain $t_3=(t_1-\lfloor t_1 \rfloor *10^8 \bmod 256)$ and $t_4=(t_2-\lfloor t_2 \rfloor *10^8 \bmod 256)$; then acquire; k_i= (bitxor(k_{i-1},t_3)+ bitxor(k_{i-1},t_4)mod256); if sequence is not acquired, then repeat step 1-3; compute the value t_5 and t_6 based on $t_i = x_{i+1}$ + ki/2*256; similarly, compute $t_7 = (t_5-\lfloor t_5 \rfloor)*10^8$ mod256) and $t_8 = (t_6-\lfloor t_6 \rfloor)*10^8$ mod256); Obtained C_i == (bitxor(k_{i-1},t_7)+ bitxor (k_{i-1},t_8)mod256); Repeat 5-7 until sequence is acquired	133ms
2.	[12]	2-Dimensional logistic map	Convert plain images to pixels points; Pseudorandom sequence was generated to obtain M_2; Now M_2 converted to pixel point; Then, column and row permutation was performed to produce the encrypted image	NIL
3.	[18]	1-Dimensional Logistic Map Tent Map	Set the optimal keys with medical image and fixed points; Iterate 5 towards 100>; Obtain M Plain Image R*C Times; If Fraction>100 proceed to next steps, otherwise skip the step; if fraction>100, then iterate 3 times, divide value to 15 digit integer; sort confusion; structural parameter are provided to evaluate diffusion; process the tent map to get random code; encrypt the plain image XOR	NIL
4.	[20].	3-Dimensional	Histogram equalization; Row Rotation; Colum Rotation;, XOR logical operation.	0.15827, no SI Unit
5.	[24].	1-Dimensional cosine fractional map	Not clearly discussed	40ms
6.	[35]	Cosinus Arcsinus, Sinus-Power Logistic, Coupled Map Lattice	Construct the Dynamic S-Box based on the generation of two none using PRNG; initialize chaotic sequence C; C was iterated N_T Times; chaotic sequence was initiated bad C; C_k was calculated based on conditions such as C_o=0 where 1≤K≤#1. Then, encrypted images will be produced	91.4MB/s,
7.	[36]	3-dimension Piecewise Linear chaotic map	Read Plain Image; Divide to Sub Block; Perform whitening by XOR; Divide to sub-Block to 4 sub block; Perform 2-Key XOR, 2Permutation; Create diffusion by XOR intra blocks; intermediate image is divided to sub-blocks; Perform whitening to sub-blocks; Perform intra block module 256; divide sub-blocks to 4 sub-blocks; create alternate 4 key XOR, 2 Permutation; 4-su-blocks are combined to obtain the cipher images	45s
8.	[37]	1_Dimensional logistic and discrete cosine function	The operations of the algorithm is based 5 steps such as DCT processing; Compression; Displacement Encryption; Symbol Encryption; Repeat step 3-4 until encryption sequence is obtained.	NIL
9.	[39]	2-Dimensional Tent-Logistic-Tent Map	select random integer k, then compute K; the cipher image C was produced from medical images I; Hash Function was utilized to produce a signature; G′ was computed from the value of H; Finally, the cipher can be sent to the authority	332ms
10	[41]	Combination of tent, piecewise and hyper chaotic maps form 3_Dimensiona	Input plain images; Decomposed P to RGB; Generate three sequence(s_1, s_2 s_3); Apply XOR operation to RGB binary; Calculate hamming distance between RGB; Perform condition shift algorithm; Diffusion operation using bit xor; Finally, obtain the Cipher Images C.	0.126985s
11	[43]	4-Dimensional chaotic map	Iterate Eq-1 with (x_0, y_0, z_0, w_0), current state produces current variable using DSVSM continuously for n_0 times; calculate pixel stream using Eq-2; use Eq-3 To figure the pixels swap positions; the pixel swap will be initiated based on Eq-4 and 5; when the pixels are not confused, then repeat step 2; apply DSVSM to confused images to obtain state variable; get the key stream using Eq-6; Eq 9 mask the value of the processing image; when the image is not encrypted, repeat step 7.	NIL

1≤K≤#1. Then, encrypted images will be produced. But, the supported chaotic maps were not discussed during the encryption development. To address the drawback, Sathishkumar et al., [57] proposed encryption algorithm based 3-dimension Piecewise Linear chaotic map. The researcher record execution of 45s, it was observed that the execution was not that effective than earlier algorithms, even though it was expected that higher dimensional recorded better execution time. Recently, a researcher used a hybrid of 1-diemnsional and 2-dimensional logistic to generate 2-diemnsional Tent-Logistic-Tent Map [52]. The researcher, proved that higher dimension maps produces better performance, as 332ms was recorded as the execution time. A Proposed encryption algorithm was generated based on 5 steps: select random integer k, then compute K; the cipher image C was produced from medical images I; Hash Function was utilized to produce a signature; $G^{/}$ was computed from the value of H; Finally, the cipher can be sent to the authority. Therefore, due to the existence of higher chaotic maps, it was investigated that the use of 2-dimensional was considered to be out of date and drawback to the encryption algorithm

Chengqi et al., [11] proposed an encryption scheme based on three segments, which utilized three dimensional chaotic systems. At the **initialization** stage is as follows: iterates $\frac{L+4}{4}$ for the CPLM taking initial values as (x, y, z, v_0) to produce sequence that appear to be pseudo-random in nature; positive and integer sequence such as b_i and x_i are obtained. The **Permutation,** real sequence is obtained; circular operation were executed with matrix $B_{(i,j)}$ =0;. The **diffusion** stage, it is required to obtain $t_3=(t_1-\lfloor t_1 \rfloor)*10^8$ mod256) and $t_4=(t_2-\lfloor t_2 \rfloor)*10^8$ mod256); then acquire; k_i= (bitxor(k_{i-1},t_3)+ bitxor(k_{i-1},t_4)mod256); if sequence is not acquired, then repeat step 1-3; compute the value t_5 and t_6 based on $t_i = x_{i+1}$ + ki/2*256; similarly, compute $t_7 = (t_5-\lfloor t_5 \rfloor)*10^8$ mod256) and $t_8 = (t_6-\lfloor t_6 \rfloor)*10^8$ mod256); Obtained C_i == (bitxor(k_{i-1},t_7)+ bitxor (k_{i-1},t_8)mod256); Repeat 5-7 until sequence is acquired. Therefore, it was observed that the researcher record 133ms execution time that perform better than those encryption algorithms developed based 2-dimensional maps. However, it was investigated that most of the earlier mentioned encryption algorithm used single chaotic map, which was considered as drawback. In contrast, Xiao et al., [57] addressed such difficulty by introducing an encryption algorithm that was initiated through the combination of tent, piecewise and hyper chaotic maps. The maps were based on one to three dimensions. The authors adopts the same methodology as that of Chengqi et al., [11] for the algorithm based on three stages such as Initialization(3 steps), Permutation(3 steps) and Diffusion (8 steps). But, it was discovered that the execution speed 147 ms is little higher than that of Chengqi et al. As such, the algorithm was not effective when comparing with earlier algorithm.

In addition, Karim et al., [3] developed an encryption algorithm based on 5 steps, with use of 3-dimensional chaotic map. The algorithm was stated based on the following steps: Histogram equalization, Row Rotation, Colum Rotation, XOR logical operation. The author record 0.15827, without specifying the required unit. But, atleast the performance was discovered to be better than Xiao et al. These brought the idea of considering higher dimension chaotic maps during the formulations of encryption algorithms. Now, the presence of 4-dimensional maps had to override the efficiency and security of the earlier encryption algorithm. In another development, Zia et al., [56] developed encryption algorithm with 4-dimensional chaotic map based on dynamic state variable section mechanism. The algorithm was developed based on 12 steps as follows: Eq 1 will be iterated with (x_0, y_0, z_0, w_0), current state variable is expected to produce current variable using DSVSM continuously for n_0 times; The pixel stream is to be calculated using Eq-2; To figure the pixels swap positions is done through Eq-3; the pixel swap will be initiated based on Eq-4 and 5; when the pixels are not confused, then repeat step 2; apply DSVSM to confused images to obtain state variable; get the key stream using Eq-6; Eq 9 mask the value of the processing image; when the image is not encrypted, repeat step 7. It was discovered that, the researcher failed to describe the execution time within the result. As such, the performance of the algorithm cannot be identified. Further work need to be undergone to identify the performance of utilizing higher dimensional maps during the encryption algorithm development. Even though the research was based on 4-dimensional, the researcher utilized Lena gray image for the experimental simulation. As such, coloured

image encryption schemes should be considered for future research. Table 10 present a summary on the formulated algorithms based gray images

B. COLOURED IMAGES

Recently, it was discovered that coloured based encryption schemes have addressed some difficulty made by the gray images. In other words, gray image encryption schemes were meant for the gray images cannot be applied to coloured images due to the RGB features and formats. In 2019, Ahmed et al., [3] introduced a proposed encryption algorithm based 2-diemnsional chaotic maps such as Arnold, Baker and Henon. During the encryption, the plain images were expected to be divided in to format of RGB. The channels components were expected to be enciphered using a chaotic map. The baker enciphered then red component, Arnold enciphered the green and Henon consider the enciphering of the blue components. However, the researcher failed to discuss the stepwise approach of the encryption scheme, together with the execution time for the experimental simulation. Similarly, Majid and Fawad [31] failed to describe the execution time for the experimental simulation. But, have clears the earlier limitation by presenting a detail discussion on the proposed encryption algorithm. The researcher combines the circle, Henon and duffing maps for the generation of the encryption algorithm as follows: plain image will be transform to RGB; divide the RGB Channel to 32 x 32 cells, considering 8 x 8 sizes of each cell; use Henon to shuffle the Pixels; Permute the channel blocks; take pixel distortion using circle Map; confusion will be created by apply XOR to the channel using duffing map. But, the researcher failed to highlights the diffusion process at the level of encryption. Moreover, the researcher considers only 1 and 2 dimensional map for development of its encryption algorithm, as higher dimensional maps are in existence.

Fatma et al., [16] clears the arguments by introducing a coloured based encryption scheme, considering of both confusion and diffusion properties. The confusion stages permute the plain images without affecting the pixel values, considering chaotic parameters as the key; the relationship of the adjacent pixels were de-correlated at the permutations rounds of $n > 1$; take $m\,rounds$ for the confusion to be achieved. The diffusion stage changes the pixels values, to diffuse all surrounding pixels; control parameter was used as the key, repeating $m\,rounds$ to obtain the diffuse image. However, the researcher records execution of 0.5642s contrary to the earlier literatures that failed to describe their execution time. In 2020, Nestor et al., [41] also introduced proposed encryption algorithm based on 2-dimensional chaotic maps such as logistic, sine and cosine. The researcher records a 0.5911s as a execution time, which is closely related to the earlier execution time mentioned by Fatma et al. But, the claim of using 2-Dimensional chaotic map has created arguments despite the existence of higher chaotic map. Ami et al., [4] have addressed the earlier limitations, by introducing a proposed encryption algorithm with a new developed chaotic map based on the 3-dimensional chaotic map. The map was considered based on the Lyapunov exponent value of 20.58. The steganography is as follows: the initial state conditions are considered to the input; the map will be iterated$s\ times$; randomly select 2L elements, select the remaining element using the same process; the triple sequence of random pairs were used to embedded MSBs and LSBs; the values of the elected and secret messages, were converted to eight binary digits and split to MSBs/LSBs; MSBs and LSBs will be embedded to LSBs to obtain the final steganography. It was discovered that literatures reveals that image encryption algorithm based on logistic maps have some drawback. Considering the literatures, investigations narrated that Interwining logistic map records better chaotic behaviour than other related logistic map. But, even though the researcher used three dimensional chaotic maps, the execution time was not presented. As such, the performance of the encryption algorithm cannot be monitored.

In contrast, Muhammad et al., [37] addressed such difficulty by introducing an encryption algorithm, which records 1.9543s as the average execution time of six (6) input images. The algorithm was initiated through the combination of tent, piecewise and hyper chaotic maps. The maps were based on one to three dimensions. The researcher formulates its algorithm based on 4 steps as follows: The image is to be decomposed; during confusion stage, the rows and columns are shifted; then, diffusion is operated to test the efficiency of the encryption algorithm. Similarly, Nadeem et al., [40] adopted a mixed map known as interwining logistic map that appears to be 3-dimensional, which was obtained by the combination of 2-Dimensional

maps. As such, the proposed encryption scheme was based 9 steps as follows: the RGB component that was splinted was combined to produce single gray scale images; The pixels appears to be in form of arrays after conversion; Then the initialization process should be embedded; the block level is to be permuted; then permute the pixels; encode the DNA; take the conversion of the Decimal; finally, then the spitted images are combined to The RGB. After simulation, the researcher records 0.0053MBps for execution time, that outperformed the earlier literature. Moreover, Muhammad et al., [37] proposed an encryption scheme by the use of Interwining logistic map. The encryption was developed based on four stages as follows: The input image was considered to be coloured images; Decomposed the input images to obtain bigger ones; applied the confusion process by the use of column and row shift; the encrypted images is obtained by employing the diffusion operation. The authors discovered that the use of 3-dimensional interwining logistic map have addressed the earlier limitations of the logistic map as reveal by [24]. However, it was investigated that some of the problem that governs logistic maps were, key, window stability, sequence distribution for the un-even, to mention a few. But, it was reveal that Ja afar et al., [24] have developed an encryption scheme based on a combination of 2-dimensional singer, sine and logistic maps, with 4 dimensional piecewise map. The algorithm was obtained based on 7 steps as follows: 'C' is considered the selected image for the vedio sequence; the image is divided to RGB after unsigned variety conversion; the bits of the input which was choosing after substitution is chosen; Apply the AND operations to R and n bits substitution; after that then apply the OR Operations; repeat the same steps for section of the blue; if you want to be obtain the RGB back, apply similar method to the chosen frames before the changing the vedio file.

However, the second challenged of the logistic maps as stated earlier, was addressed by Ekhlas et al., [15]. This difficulty reveals that 2-diemnssional logistic maps are considered to be having weak keys during encryption. Therefore, the authors introduced 3-dimensional with combination of 2-dimenisonal standard map, 1-dimensional Guess iterated and 4-dimensional Lorenz, for the proposed encryption scheme. The formulation of the algorithm was undergone using 6 steps: obtain the block sizes; Generate the key sizes; Permutation using the Lorenz; take the number of the rounds; obtain the number of halves; Finally, Generate then round functions. The researcher records average of 117second of the three images after two rounds of execution. It was discovered that performance of the execution was not effective, when compaired to the earlier encryption algorithms. Recently, Kaishi et al., [28] introduced its proposed encryption algorithm using the combination of 1-dimensional logistic map together with 4-dimensional Chen's chaotic map. The researcher failed to describes the execution time for its experimental simulations. Even though the researcher used higher Map, but the performance cannot be assess. The algorithm was made of 6 steps as follows: Separate the coloured image to RGB formats; The input should be made up block; The iteration of chaotic logistic map formed random matrix; the matrix are subdivided in to V x V block sizes; obtain the chaotic sequence using the chen's system; Apply the DNA encoding to the sub-blocks, in order to monitor the performance of encryption algorithm based on the RGB Channel. Table 11 present a summary on the formulated algorithms based on coloured images

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 11: Algorithm for Coloured based Images

	Authors	Maps	Algorithm	Execution Time
1.	[3]	2-Dimensional Arnold, Baker and Henon	The plain images divide to RGB; The channels components enciphered using a chaotic map; The baker enciphered the red component; Arnold enciphered the green; Henon enciphered the blue.	NIL
2.	[4]	3-Dimensional chaotic map	The initial state conditions are input; the map iterated $s\,times$; randomly select 2L elements, select the remaining element; embed MSBs and LSBs the triple sequence of random pairs; elected and secret messages, were converted to eight binary digits and split to MSBs/LSBs; MSBs and LSBs embedded to LSBs to obtain final steganography	NIL
3.	[9]	Combination of 2-dimenisonal standard map, 1-dimensional Guess iterated and 4-dimensional Lorenz	Obtain the block sizes; Generate the key sizes; Permutation using the Lorenz; take the number of the rounds; obtain the number of halves; Finally, Generate then round functions	117s average of three images
4.	[10]	NIL	The confusion stages permute the plain images without affecting the pixel value; adjacent pixels were de-correlated at the permutations rounds of $n > 1$; take $m\,rounds$ for the confusion; diffuse all surrounding pixels; repeating $m\,rounds$ to obtain the diffuse image	0.5642s
5.	[16]	Combination of 2-dimensional singer, sine and logistic maps, with 4 dimensional piecewise map	C' is selected image for vedio sequence; Divide the image to RGB; choose the bits input; Apply the AND operations to R and n bits substitution; apply the OR Operations; repeat the same steps for section of the blue; to be obtain the RGB back, apply similar method	NIL
6	[19].	Combination of 1-dimensional logistic map together with 4-dimensional Chen's chaotic map	Separate the coloured image to RGB formats; Make input to block; The iterate chaotic logistic map to formed random matrix; the matrix subdivided in to V x V block sizes; obtain the chaotic sequence using chen's system; Apply the DNA encoding to the sub-blocks	NIL
7.	[22]	2-Dimensional circle, Henon and duffing maps	Transform plain image RGB; divide the RGB Channel to 32 x 32 cells, considering 8 x 8 sizes of each cell; use Henon to shuffle the Pixels; Permute the channel blocks; take pixel distortion using circle Map; confusion will be created by apply XOR using duffing map	NIL
8.	[28]	Combination of tent, piecewise and hyper chaotic maps	The image are decomposed; confusion stage, the rows and columns are shifted; diffusion is operated to test the algorithm	1.9543s
9.	[31]	3-Dimensional interwining logistic map	The RGB component was combined to produce single gray scale images; The pixels appears to be in form of array; embed the initialization process; permute the block level; permute the pixels; encode the DNA; convert the Decimal; then the spitted images are combined to The RGB	0.0053MBps
10	[33]	2-Dimensional logistic, sine and cosine	Not Discussed in details	0.5911s

4. CONCLUSION

The review article have discovered some of the existing literatures based on chaotic systems, the literatures were analysed and discovered that most of the surveys failed to take a comparative analysis on components of the cryptosystems as giving at Table 2. The researcher adopted a developed framework known as YAFSU, which served as the guide to the experimental review based on the aforementioned research field. Little was discussed on the relationship of chaotic and cryptography at the introductory section of the paper. The discussed was based on the properties of both the cryptography and chaotic systems, as presented within Table 1. However, the review article looks in to the components of the cryptosystems that were utilized during the experimental simulations. The input images were

observed, which are considered to be the inputs to be utilized during the experimental simulations, the images were classified in to both gray and coloured images based on their respective sizes. Along the way, the researcher discovered some challenges, which lead to some difficulty or drawback, as discussed within the section of the limitation. In addition, the hardware and software facilities of a computer system need to be determined before running any experiment. Due to mentioned reason, the present review carried investigations on the hardware and software components of the computer devices being utilized during the experimental simulations, with regard to time complexity of various reviewed articles, considering gray images first then followed by the coloured. Similarly, some limitation were discovered and stated within the section as well. Moreover, the review article considers the algorithm formulation for the reviewed literatures, considering the individual performance. Later, a comparative analysis was taken based on the execution time It is believed that the review may put impact on the researcher's with interest on chaotic cryptosystems based on images, to discover the input images, hardware and software facilities that should be considered for the experimental simulations. In addition, performances of existing encryption algorithms were analysed, to highlights ways to be followed in developing robust image encryption algorithm that may outperform the existing ones. The review may assist those willing to undergone research within the field of image encryption based chaotic systems. The review can be able to give highlight on input images, hardware and software components, algorithms that can be suitable for experimental simulations

4.1. Limitations

It was observed that some image encryption algorithm simulations suffered from fewer input images utilizations, which in many cases resolved to poor performance or in-efficiency of the encryption algorithm. Therefore, when the performance of the encryption algorithm is not efficient, it can be concluded that encryption scheme is said to be un-secured that can be attacked easily by an intruder, in order to obtain the secret Informations. As such, the use of fewer input images can said to be a thread to the security of any experimental simulation of encryption algorithm. As the saying goes, the efficiency of the encryption algorithm can be obtained, when many input images regardless of the size and nature were utilized for the experimental simulation.

Considering the literatures, it was discovered that the hardware component that were utilized for gray scale images experimental simulations. Investigations reveal that Saleh et al., [35] and Mohamed et al., [24] encryption algorithms, were considered to have better performance with values such as 91.4MB/s and 40Ms. In Contrast, Nadeem et al., [31] used coloured images for its experimental simulations. The simulation records 0.053 MBps as it time complexity, showing better performance than the earlier gray encryption algorithms. But, it was observed that their exist no research that proved the claim "The effectiveness of the execution time depends on the Hardware capacity of the computer systems". Considering reviewed literatures, it was discovered that both Saleh et al and Mohamed et al. Used high capacity computers than that of Nadeem et al. But, various execution time obtained by the researcher's disproving the earlier claim.

The use of older version software's during experimental simulation by most encryption algorithms were considered part of the limitation of some of the recent articles [30, 31]. Moreover, it was discovered that some research articles failed to present the software versions or the supporting operating systems [13, 20 and 26]. However, investigations reveal that MATLAB version 2018 was in existence, when Nadeem et al., [31] used the version 2016. The Review, further analysed, that most of the researcher's failed to take comparative analysis on the execution time with respect to the utilized software's.

However, the present survey limit its review based on articles that happen to be between years 2015-2022, considering 1-4-Dimensional chaotic maps, while 5-dimensional chaotic maps are into existence. Therefore, more work need to be done with research article of year 2023 inclusive, which should consider beyond 4- dimensional chaotic maps.

© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.2. Suggestions For Future Research:

Authors are expected to be utilizing many input images during the experimental simulation, which will assist in monitoring both the security and performance of the proposed encryption schemes. If the proposed encryption schemes can execute its simulations on many images regardless of the size and the nature. Then the algorithm is said to be efficient, due to the fact that different images exhibit different features.

Recent work based on Gray images need to be introduced that may outperform the performance of sale et al.,[35] and Mohamed et al., [24] with the regard to the latest computer system. Moreover, the coloured image need faster encryption schemes based on higher capacity computers that will outperformed Nadeem et al., [31] encryption scheme. Both the Gray/Coloured Images need a discovery that may clear the claim which said "The effectiveness of the execution time does not depend on the Hardware capacity of the computer systems".

Based on the investigation by the existing literature. It is clearly shown than recent articles used older version of the software tool being utilized during the experimental simulation [30]. In addition Haotian et al., [13] introduce MATLAB as software tool for the experiment without taking any concern on the version, while Karim et al., [20] present the operating system without discussing the Software tool used for its simulation. In addition, Nadeem et al., [31] undergone coloured based experimental simulation with MATLAB version 2016 that operates on 64 bit Operating system. It was noticed that the researcher used an old version of the MATLAB since version 2018 was in to existence. Manjit et al, [23] used the MATLAB version 2018a for simulation without giving consideration on the operating system that computer device operates on. As such, recent researches need to be undergone, which should consider both latest operating system and Software tool for the simulations. Some authors should consider other simulations software's, to undergo some performance comparison with MATLAB.

When formulation of any encryption scheme, the researcher need to consider higher chaotic maps. [37] Suggested that use of wavelet fractal transformation and feasibility of combining use of predictive coding and chaotic encryption should be considered. Furthermore, the researcher suggests the use of the algorithm in testing real time applications such as wireless communication and ad-hoc networking [36].

5. DECLARATION

We declared no conflict of interest.

6. AKNOWLEDGEMNT

This research was funded by the collaboration of the below listed organizations.

A. Annual Funding track by the Deanship of scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University , Saudi Arabia(Project No. Grant No. 5357)

B. Ministry of Education of Malaysia, grant number FGRS/1/2020/STG06/UNISZA/02/2. Centre for Research Excellence & Incubation Management, Universiti Sultan Zainal Abidin.

REFERENCES

[1] Abir Lassoued, Olfa Boubaker. (2016). "On New Chaotic and Hyper-Chaotic System: A Literature Review". *International Journal of Non-Linear Analysis Modelling and Control*. Vol-2(6): Pg(770-789)

[2] Ahmed Hussain Ali, L. E. G., A. A. Zaidan, Mohd Rosmadi Mokhta (2018). "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain." *Journal of Multimedia Tools and Applications*Vol-77: Pg(31487-31516).

[3] Ahmed M. Elshamy, Aziza. I. Hussein, Hesham F. A. Hamed, M. A. Abdelghany, Hamdy M. Kelash (2019). "*Color Image Encryption Technique Based on Chaos* " Proceedia of 16th International Learning and Technology ConferenceVol-163: Pg(49-53).

[4] Ami Sharif , M. M., Mahboubeh Nazari (2017). "A Novel Method for Digital Image Steganography Based on a New Three-Dimensional Chaotic Map." *Journal of Multimedia Tools and Applications*Vol-76: Pg(7849-7867).

[5] Anandkumar R, Kalpara R. (2019). "A Survey on Chaos Based Encryption Techniques" *Journal of Enabling and*

Architecture for Next Generation Networking Capabilities. Pg (147-149).

[6] Aytekin Yildizhan, N. T. (2019). "Chaotic Encryption and Privilege Based Visual Secret Sharing Model for Color Images." *International Journal of Computing and Informatics*Vol-38: Pg(701-727).

[7] Behrouz Vaseghi, S. M., Sayedeh Somayeh Hashemi, Afeh Fekih (2021). "Fast Reaching Finite Time Synchronization Approach for Chaotic Systems with Application in Medical Image Encryption " *Journal of Digital Identifier*Vol-9: Pg(25911-25925).

[8] Berg Danielle A, Richard W Pogge, Evan D Skillman, Kovin C Croxall, John Moustakes, Ness Mayker. (2018)." *The chaos Survey*" 30 Proceeding IAU Symposium. Vol-14(30): Pg(246-248).

[9] Bouguessa et al., [15]. "A New Techniques of Steganography Based on the Theory of Chaos". *Malaysian Journal of Computing and Applied Mathematics*. Vol-4(1). Pg (1-12)

[10] Chetana Singh, Binay Kumar Pandey, Dr H.L Mandoria, Ashok Kumar. (2018). "A Review Paper on Chaotic Map Image Encryption Techniques". *International Research Journal of Engineering and Technology*. Vol-5(4): Pg (1882-1886)

[11] Chengqi Wang, Xiao Zhang, Zhiming Zheng (2016). "An efficient image encryption algorithm based on a novel chaotic map." *Journal of Multimedia Tools and Applications*Vol-76: Pg(24251-24280).

[12] Chunhu et at al., (2017). "Chaotic Image Encryption Schemes: A Review". 2th International Conference on Electrical, Automation and Mechanical Engineering. Pg (260-263).

[13] Darrel Hankerson, A. M., Scott Vanstone (2006). "Guide to Elliptic Curve Cryptography." Book on Professional Computing.

[14] Divya Singh. (2020) "*A Brief Survey of Chaos Theory in Spread Spectrum System*.". Proceeding of the International Conference on Innovative Computing and Communication. Pg (1-7)

[15] Ekhlas Abbas Al-Bahr, R. N. J. K. (2019). "A New Cipher Based on Feistel Structure and Chaotic Maps " Journal of Baghadad ScienceVol-16(1): Pg(270-280).

[16] Fatma Elgendy, Amany. M. Sarhan, Tarek E. Eltobely,S. F. El-Zoghdy,Hala S. El-sayed,Osama S. Faragallah (2015). "Chaos-based model for encryption and decryption of digital images." *Journal of Multimedia Tools and Applications*Vol-75: Pg(11529-11553).

[17] Gulden Gunay Buluti, M. C. C., Hassan Guler (2020). "Chaotic System Based Real-Time Implementation of Visual Cryptography Using LabView." International Journal of Information and Engineering TechnologyVol-37(4): Pg(639-645)

[18] G Avarez, S. J Li(2006). "Some Basic Cryptographic Requirements for Chaos Based Cryptosystems". *International Journal of Bifurcation and Chaos.* Vol-16: Pg(2129-2151)

[19] Hai-Yan Gu1, W.-Q. Y., Jing-Hui Zhang (2020). "Novel Image Encryption Scheme Based on Hyperchaotic Cellular Automaton." Journal of ComputersVol-31(6): Pg(155-168).

[20] Haotian Liang, Guidong Zhang, Wenjin Hou, Pinyi Huang, Bo Liu, Shouliang Li (2021). "A Novel Asymmetric Hyperchaotic Image Encryption Scheme Based on Elliptic Curve Cryptography." *Journal of Applied Science*Vol-11(12): Pg(1-23).

[21] Hassan Elkamchouchi , W. M. S., Yasmine Abouelseoud (2019). "New Video Encryption Schemes Based on Chaotic Maps." *IET Image Processing*: Pg(1-16).

[22] Hossam Diab, A. M. E. (2017). "A Secure Image Cryptosystem with Unique Key Streams via Hyper-Chaotic System." *Journal of Signal Processing*: Pg(1-18).

[23] Houssem Mhiri, Moyi Tian, Erin Wynne, Sean Jones, A Mareno. (2019). "An Experimental Survey of Chaos and Symmetry Breaking in Coupled and Driven logistic map" *European Journal of Physics.*Vol-40(6): Pg (1-14)

[24] Ja afar A.Alzubi, Omar A. Alzubi, G.Susendran, D. Akila (2019). "A Novel Chaotic Map Encryption Methodology for Image Cryptography and Secret Communication with Stegnography." *International Journal of Recent Technology and Engineering*Vol-8(1): Pg(1122-1128).

[25] Jiayu Sun, C. L., Tianai Lu, Akif Akgul, Fuhong Min (2019). "A memristive chaotic system with hypermultistability and its application in image encryption." *Journal of Digital Identifier*Vol-20: Pg(1-9).

[26] K.Busawan, P.Canyellas-pericas, R.Binns, I-Elliot, Z.Ghassembloy. (2018). "*A Brief Survey and Some Discussions on Chaos Based Communication Schemes*". 11th International Symposium on Communication System Network and Digital Signal Processing. Pg (1-5)

[27] K-Shankar, Mohamed El-Hoseny, E.Dhiravida Chelvi, S.K Lakshmanaprabu, WanQing Wu (2018). "An Efficient Optimal Key Based Chaos Function for Medical Image Security." *Journal of Digital Identifier. IEEE Explore.*Vol-6: Pg(77145-77154).

[28] Kaishi Li , Z. S. (2019). "*Research on an Image High Intensive Encryption Way Based on the Chaos Theory and DNA Coding* " 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics: Pg(1-7).

[29] Karim H. Moussa, A. I. E. N., Heba G. Mohamed (2021). "Non-Linear Hopped Chaos Parameters-Based Image Encryption Algorithm Using Histogram Equalization." *Journal of Entropy*Vol-23(535): Pg(1-15).

[30] M.K. Shukla, B. B. S. (2018). "Secure communication and image encryption scheme based on synchronisation of fractional order chaotic systems using backstepping." *International Journlal of Simulation and Process Modelling*Vol-13(5): Pg(473-485).

[31] Majid Khan, F. M. (2019). "A novel chaotic image encryption technique based on multiple discrete dynamical maps." *Journal of Multimedia Tools and Applications*Vol-78: Pg(26203-26222).

[32] Manjit Kaur, D. S., Kehui Sun, Umashankar Rawat (2020). "Color Image Encryption using Non-Dominated Sorting Genetic Algorithm with Local Chaotic Search Based 5D Chaotic Map." *Jounal of Generation Computer Systems*Vol-105: Pg(333-350

[33] Manish Kumar, Amogh Saxena, Sai Satvik Vuppala (2020). "A Survey on Chaos Based Image Encryption Techniques". *Journal of Multimedia Security:Using Chaotic Maps Principles and Methodologies*. Vol-884: Pg(1-26)

[34] Mohamed Zakariya Talhaoui, X. W., Abdallah Talhaoui (2020). "A new one-dimensional chaotic map and its application in a novel permutation-less image encryption scheme." *Jounal of Visual Computer*Vol-37: Pg(1757-1768).

[35] Mollaeefar, M., .Sharif, Amir, Nazari, Mahboubeh (2017). "A novel encryption scheme for colored image based on high level chaotic maps " *Journal of Multimedia Tools and Applications*Vol-76: Pg(607-629).

[36] Mozhgan Mokhtai, M. A., Hassan Naraghi (2016). "Image Encryption Using Hyper Chaos and Symmetric Cryptography." *International Journal of Innovative Research in Science & Engineering*.

[37] Muhammad Hanif, S. A., Muhammad Adnan Khan, Nadeem Iqbal, Zia ul Rehman, Muhammad Anwar Saeed, Ehab Mahmoud Mohamed(2017). "A Novel and Efficient Multiple RGB Images Cipher Based on Chaotic System and Circular Shift Operations " *Journal of Digital Identifier. IEEE Explore.* Vol-8: Pg(146,408-146,427).

[38] Musheer Ahmad, Z. A. (2018). "Random Search Based EfficientChaotic Substitution Box Design for Image Encryption." *International Journal of Rough Sets and Data Analysis*Vol-5(2): Pg(131-147).

[39] Nadeem Iqbal, S. A., Muhammad Adnan Khan, Areej Fatima, Aiesha Ahmed, Nida Anwer (2020). "Efficient Image Cipher Based on the Movement of King on the Chessboard and Chaotic system." *Journal of Electronics Imaging*Vol-29(2): Pg(1-19).

[40] Nadeem Iqbal, Sageer Abbas, Muhammed Adnan khan, Tahir Alyas, Areej Fatima (2019). "An RGB Image Cipher Using Chaotic Systems, 15-Puzzle Problem and DNA Computing." *Journal of Digital Identifier. IEEE Explore.*Vol-7: Pg(174,051-174,071).

[41] Nestor Tsafack, S. S., Bassem Abd-El-Atty,Jackques Kengne,Jithin K.C, Akram Belazi,Irfan Mehmood, Ali Kashir Bashir,Oh-Young Song, and A. A. A. A. El-Latif (2020). "A New Chaotic Map With Dynamic Analysis and Encryption Application in Internet of Health Things." *Journal of Digital Identifier*Vol-8: Pg(137731-137744).

[42] PenFei Fang, Han Liu, Chengmao Wu, Min Liu, (2022). "A Survey of Image Encryption Algorithm Based on Chaotic System". *Journal of Visual Computers*. Vol-38(6): Pg()

[43] Ping Zhen, Lequan Min, Geng Zhao, Xiaodong Li. (2014). "*A Survey of Choas-Based Cryptography*". 9th International Conference on P2P Parallel, Grid, Cloud and Internet Computing. Pg(237-244)

[44] Roayat Ismail Abdelfatah (2019). "Secure Image Transimission using Chaotic Enhanced Elliptic Curve Cryptography." *Journal of Digital Identifier.*Vol-8: Pg(3875-3890).

[45] Sabah Fadhel, Mohd Shafryy, Omar Farook. (2017). "Chaos Image Encryption Method: A Survey Study". Bulleting of Electrical Engineering and Informatics.Vol-6(1): Pg (99-104)

[46] Saleh Ibrahim, H. A., Mehedi Masud, Sultan S Alshamrani, Omar Cheikhrouhou, Ghulam Muhammad, M Shamim Hossan, Alaa M Abbas (2020). "Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps." *Journal of Digital Identifier*Vol-8: Pg(160433-160434).

[47] Sathishkumar Arthanari1, M. M. a. B. B. (2015). "Chaotic Image Encryption using Modular Addition and Combinatorial Techniques." *International Arab Journal of Information Technology*Vol-12(2): Pg(110-116).

[48] Shafali Agarwal (2018). "A Review of Image Scrambling Technique using Chaotic Maps". *International Journal of Engineering and Technology Innovation*. Vol-8(2): Pg(77-98)

[49] ShanJun Yan, Junli Mi. (2018). "*An Encryption Algorithmof Image Based on Chaotic Sequences and DCT*."Procedding of 4thInternational Conference on Virtual Reality: Pg(70-73).

[50] Sheela S, Sathyanarayana S. V. (2016). "Application of Chaos Theory in Data Security". *Journal of Accent Transactions on Information Security*. Vol-2(5): Pg (1-15).

[51] Shuqin Zhu, Congxu Zhu, Huanqing Cui, Wenhong Wang. (2019). "A Class of Quadratic Polynomial Chaotic Maps and Its Application in Cryptography." *Journal of Digital Identifier. IEEE Explore.*Vol-7: Pg(34141-34152).

[52] Tahir Sajjad Ali, R. A. (2020). "A Novel Medical Image Singncryption Scheme Using TLTS and Henon Chaotic Map." *Journal of Digital Identifier*Vol-8: Pg(71974-71989).

[53]Tipirneni Venugopal, V. S. K. R. (2018). "Image Watermarking Using Two Level Encryption Method Based on Chaotic Logistic Mapping and Rivest Shamir Adleman Algorithm " *International Journal of Intelligent Engineering and Systems*Vol-11(6): Pg(271-281).

[54] Veena and Ramakrishna. (2021). "A Survey on Image Encryption using Chaos-Based Techniques". *International Journal of Advanced Computer Science and Applications*. Vol-12(1): Pg (379-384).

[55] Yahaya Garba Shawai, Mohamad Afendee Mohamed, Usman Haruna[3], Mohammed Amin Almaiah , AbdalWali Lufti, Sulaiman Ibrahim Muhammad. (2023). "Foundation of Chaotic Maps Based on Dimension with Relations to the Property of Cryptography and Mathematical Expressions: A Systematic". *International Journal of Theoretical and Applied Information Technology*-Accepted, will be Published 15 September 2023

[56] Zia Bashir, TabasamRashid, Sohail Zafar (2016). "Hyperchaotic Dynamical System Based Image Encryption Scheme with Time-varying Delays." *Jounal of Natural Science and Engineering*Vol-18: Pg(254-260).

[57] Xiao Zhang,Wang Chengqi, Zhiming Zheng (2017). "An Efficient Chaotic Image Encryption Algorithm Based on Self-adaptive Model and Feedback Mechanism " *Journal of Transaction on Internet and Information Systems*Vol-11(3): Pg(1785-1801).

[58] Zilan Pan, L. Z. (2017). "Optical Cryptography Based Temporal Ghost Imaging with Chaotic Laser." *Journal of Phonotics Technology Letters*Vol-29(6): Pg(1-4).

[59] Zhu HongFeng, Wang Rui (2018). "A Survey to Design Privacy Preserving Protocol using Chaos Cryptography". *International Journal of Network security*. Vol-20(2): Pg (313-322)