Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 2, No. 4, 2024, Pages 104-112
DOI:

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage:
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE – COMPUTER SCIENCE

Enhance Key Stage Generation for Developing Kasumi Encryption Algorithm

[1*]Ahmed Ali Salih, [2]Ali Shakir Mahmood

[1,2]Computer Science Department, College of Education, Mustansiriyah University

[*] Corresponding author E-mail: ahmedali@uomustansiriyah.edu.iq

Article Info.

Article history:

Received
10 February 2024

Accepted
21 April 2024

Publishing
30 September 2024

Abstract

Data security is a critical component of the efficient performance of every organization's diverse requirement, one of the important requirements is to provide a secure connection for data transmission in the organization's networks. Cryptography algorithms are used to protect transmitted data from unauthorized access. Every day, a great deal of research is being done. The process of encrypting data is currently under development. Therefore, a substantial technological or research effort is still required. Cellular networks and secure communication. This proposal calls for developing a KASUMI algorithm that depends on Using random keys in all the rounds. These keys were generated by generating a random number in a range (0 to 1) by using the standard function, then assuming a zero-bit value if the random number is less than 0.5 or assuming a one-bit value if the randomly generated number is greater than 0.5 this operation is repeated until obtaining a desired key length to use it in a round of the algorithm. That means we generated random keys as 128 bits for each round and saved it in an array with size (8×8) because we have 8 rounds, and each key is divided into 8 subkeys as 16 bits for each to use in encryption and decryption. The developed random keys and traditional algorithm keys were tested with statistical tests of NIST, which made up a comparison and conclusion that the developed keys have a higher randomness especially when passed almost all tests successfully. that’s means we can conclude that our modified Kasumi algorithm achieved more secure data in its resulting cipher text which evaluated by several statistical metrics.

The official journal published by the College of Education at Mustansiriya University

Keywords: Cryptography, Block cipher, Kasumi, Key Schedule, NIST statistical test.

1. Introduction

The importance of data, including text, images, audio, video, and so forth, is increasing in daily life due to the quick development of digital technology and communication media [1]. The world is currently experiencing the information era. Information is typically kept on the Internet by people. They must be confident that their communications over the Internet are protected. Cryptography is the most widely used tool for security [2]. There are two kinds of cryptographic algorithms Symmetric and Asymmetric. The symmetric type utilizes the same key for encrypting and decrypting processes, while the asymmetric type utilizes a public key and a private key [3]. Before cryptography definition, cryptology could be defined as the scientific study of cryptography and cryptanalysis. One practical way to guarantee data security is through cryptography [4]. One of the most common definitions of cryptography term is: "the science and art of transforming messages to make them secure and immune to attacks". Cryptanalysis is the science and art of breaking codes. Another definition considers cryptanalysis as the procedure of deriving the plaintext from the cipher text (breaking a code) without having the key or the system (code breaking). Some of these attacks are active, causing data to be altered, while others are passive which releases data. The degree of success of the attack is determined by the system's vulnerability [5-6]. Symmetric key cryptographic algorithms have a single key for both encryption and decryption. These are the most widely used schemes. They are preferred for their high speed and simplicity. However, they can be used only when the two communicating parties have agreed on the secret key. This could be a hurdle when used in practical cases as it is not always easy for users to exchange keys. Kasumi is a block cipher used in Universal Mobile Telecommunications System UMTS, GSM, and GPRS mobile communications systems.

In UMTS, Kasumi is used in the confidentiality (f8) and integrity algorithms (f9) [7-8]. There are several attempts to develop the Kasumi algorithm, which depends on the use of the random property in the algorithm so that the efficiency and complexity of the algorithm increases this property that's why development in a specific part by using randomness was used, 8 ×128 random keys were generated to be used in the encryption 8 rounds, which increased the complexity of the cipher text and made it difficult to be attacked by unauthorized people [9].

2. Related Works

The studies listed below were selected because they are pertinent to the topic of this paper. As elaborated below, the construction and development of the Kasumi algorithm is the main subject of these investigations, and M. Madani, and C. Tanougast [10], proposed improved and efficient implementation of the Kasumi block cipher. The goal is to maintain standards while creating an effective ciphering method with improved performance and strong security. Using several Xilinx Virtex Field Programmable Gate Arrays (FPGA) technologies, the suggested design was put into practice. The synthesis findings and a comparison with other efforts demonstrate that the suggested cipher block performs better in terms of throughput, hardware logic resource usage, and resistance to most cryptanalysis techniques. The suggested designs have been implemented using FPGA Virtex technology. C. De Silva [11] proposed a new method that discusses the A5 encryption method and is based on a critical investigation of the A5/1, A5/2, and A5/3 partial systems, along with some potential vulnerabilities to them. A thorough discussion was held on how to attain integrity and secrecy in the GSM network. The A5 algorithm achieves great speed because of its streamlined design. Even though the A5/x algorithms have been the target of several theoretical and real-world assaults. The LFSR structure, Recursive Feistel structure, and register-level pseudo-bit-stream encryption architecture of the A5 method demonstrate greater resilience than its drawbacks. This provides it greater flexibility in patching its weaknesses and adjusting to changes in technology.

Salami, V. Khajev and, E. Zenial [12] Given that cryptographic algorithms are divided according to the kind of cryptographic structure they belong to symmetric (SYM) and asymmetric (ASYM). Substitution-permutation network (SPN) and Feistel network (FN) structures are primarily used by SYM algorithms, whereas mathematical structures are followed by ASYM algorithms. Based on this, investigated the effectiveness of various encryption techniques, and conducted a thorough comparison of key sizes. the number of rounds, and the block size. Further reading is offered in each category to further explore the vulnerabilities of each algorithm against attacks and open challenges. It was noted throughout the investigation that Brute-Force assaults might be used against any of the algorithms under examination. Because of the kind of mathematics that goes into designing some algorithms, the algorithm becomes susceptible. The findings of the examination of the suggested algorithms demonstrate that the structure of the designing of the algorithms, like the RSA created by common people with an explicitly stated structure, permits the algorithm users to employ a variable key size and block size, a low number of rounds, and flexibility, all of which are very well-liked by the users and can be used for lightweight authentication in the Internet of Things.

Ibrahim, Y.abbas, and Ali [13], suggested architectures of lightweight block cipher algorithms to design an FPGA that is very suitable for prototyping, thereby reducing the cost of block cipher algorithms. Based on this, the performance and efficiency of block cipher algorithms (AES, Kasumi, XXTEA192, Roadrunner based on R, LED, XTEA, etc.) were examined. Algorithm design: Depending on the standards applied, the study's findings demonstrated each algorithm's level of success as well as the degree of cost and security it possessed. Jiexian, Y. Khizar, Z. Ali, et al. [14] suggested a new method to improve the performance of cryptographic chips for safe Internet of Things applications, novel hardware designs for the dynamically reconfigurable implementation of 64-bit MISTY1 and Kasumi block ciphers are presented in this work state. If the single round MISTY1 / Kasumi algorithms are reconfigured at runtime using (SRL32&DPR), The hardware designs are ideal for wireless sensor networks and military applications. The suggested approaches may be expanded to include security architecture for UMTS networks that use several methods for integrity and confidentiality in 3G and 4G systems. All things considered, this study represents a major advancement in cryptography and circuit design that will influence security architectures of the future, the summarization of discussed related works stated in Table 1.

Table 1. Summarization of Related Works

Authors	Methodology	Features	Measurements and Results
Mahdi Madani and Camel Tanougast., 2021, [10]	Involves putting forth a better and more optimized KASUMI block cipher implementation that uses a chaotic generator.	The paper's features include an in-depth explanation of the suggested chaotic-KASUMI architecture and related techniques, the proposed simplified functions and optimized KASUMI architecture, and the security evaluation and analysis, which includes the dynamic chaotic behaviors examined using Lyapunov exponents.	The suggested architecture's statistical analysis is presented in the paper, along with the findings of NIST statistical tests that show how resilient the suggested algorithm is to common tests like linear, frequency, serial, and randomness tests.
S. De Silva, 2021, [11]	According to the paper, W3G, ZUC, and AES are three promising cryptographic algorithms that can be used with current mobile technologies.	The A5/1, A5/2, and A5/3 variants as well as the sections of the ciphering algorithm and the GSM implementation of the A5 cryptographic algorithm are covered in this paper. A5/1, A5/2 and A5/3 algorithm 1.1 theoretical and practical attacks are also covered. It also gives information about the A5 algorithm family's Recursive Feistel structure and LFSR structure.	The topic of achieving integrity and secrecy in the GSM network was thoroughly discussed. The A5 algorithm's streamlined design allows for exceptional speed.
Yashar Salami, Vahid **Khajehvand,** Esmaeil Zeinali, 2023, [12]	The methodology of the paper entails a thorough examination of symmetric (SYM) and asymmetric (ASYM) algorithms according to several parameters, such as the number of rounds, flexibility, structure, production year, key size, block size, and algorithm developer. The purpose of the study is to highlight the vulnerabilities in encryption algorithms and to pinpoint unresolved issues in the field of cryptographic algorithms.	The paper's features include an in-depth categorization of symmetric (SYM) and asymmetric (ASYM) cryptographic algorithms, a summary of encryption techniques, a study of techniques based on different parameters, and the detection of vulnerabilities against various attacks. The paper also poses open challenges concerning cryptography-related encryption techniques.	The results of the analysis of the proposed algorithms show that the design structure of the algorithms, like the publicly available RSA, allows algorithm users to use variable key and block sizes, fewer rounds, and flexibility—all of which are highly favored by users and can be applied to lightweight authentication on the Internet of Things.
Marwa Subhi Ibrahim, Yasir Amer Abbas, and Mudhafar Hussein Ali., 2022, [13]	This paper examines a lightweight block cipher (LWBC) that uses XTEA's round function operation. It takes the form of a Feistel structure with 64 encryption and decryption rounds, a 128-bit key size, and a 64-bit block size. The implementation of the AES algorithm with less FPGA hardware, lower power consumption, and improved cryptosystem throughput is also covered in the paper.	When discussing security, don't forget to include the idea of ubiquitous computing, which includes non-repudiation, confidentiality, integrity, and authentication (p. 1). Additionally, the paper covers the round function operation of XTEA in the form of a Feistel structure with 64 rounds for encryption and decryption, involving a 128-bit key size and a 64-bit block size. This is known as the lightweight block cipher (LWBC).	We looked at the effectiveness and efficiency of various block cipher algorithms, such as AES, Kasumi, XXTEA192, and Roadrunner based on R, LED, and XTEA. Algorithm design: The results of the study showed the degree of cost and security, as well as the success rate of each algorithm, based on the standards used.
Huang Jiexian, Yasir Khizar, Zain Anwar Ali, Raza Hasan, and Muhammad Salman, 2023, [14]	The RLUT-based MISTY1/KASUMI architecture was designed and configured, and SRL32 implemented the S-boxes and MISTY1/KASUMI transformation functions as part of the methodology used in this paper.	Adopted as a fruitful defense against malevolent attacks, the suggested adaptive reconfiguration also has the benefit of requiring less reconfiguration time (RT).	Performance evaluations of the suggested hardware architectures for the KASUMI and MISTY1 block ciphers were presented in the paper.

3. Kasumi Block Cipher

Kasumi Block Cipher is a block cipher with eight rounds and a 128-bit generated key. Its input and output have 64 bits apiece Using a key scheduling method, eight 16-bit sub-keys are generated for each round. Additionally, each round serves the FL and FO purposes. FO comes first in even-numbered rounds and FL comes first in odd-numbered rounds. Both FL and FO generate a 32-bit output after receiving a 32-bit input. The following notations are used in this work. The first round's 32-bit inputs, L and R, are each. The input for the FL function is XL. The key utilized in the FL function is KL. XO stands for the input to FO. The left and right 16 bits of XO in round i are represented by XOi, l and XOi, r (1 ≤ i ≤ 8), respectively. The key used in the FO function is indicated by KO. The input to the F I function in the jth round of FO is indicated by XIi, j. In the FI function, the key is indicated by KI. S9 and S7 indicate the S-boxes that are 9 × 9 and 7 × 7, respectively [15].

Kasumi Algorithm contains main three functions that form the basic structure of most encryption algorithms. Algorithms can vary greatly and vary depending on the purpose and field the algorithm deals with.

3.1. FO Function

FO refers to the "Nonlinear Function" or "Output Function"[16]. As shown in figure (1) This function operates in three rounds. It begins by splitting the 32-bit input into two equal 16-bit values. Then, it operates on the left 16-bit value by using the 48-bit key KO and the 48-bit sub-key KI used in the FI function. For every integer j (the number of rounds in FO), where ≤ j ≤ 3, Rj and Lj are provided as follows:

$$R_j = FI\left(L_{j-1} \otimes KO_{i,j}, KI_{i,j}\right) \otimes R_{j-1} \&, L_j = R_{j-1} \qquad Equ(1)$$

The 32-bit concatenated value obtained (L3 || R3) is then returned once the FO function has finished [17].

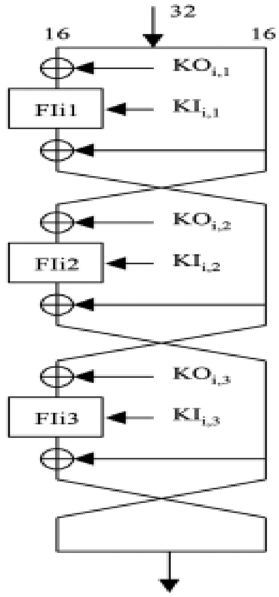

Fig. 1. FO Function [16]

3.2. FL Function

FL refers to "Linear Function" or "Feistel Functions" shown in Figure (2) It receives a 32-bit input, processes it with a 32-bit key, and outputs a 32-bit result using KL. The key and KL are split into two 16-bit values for each round [18].

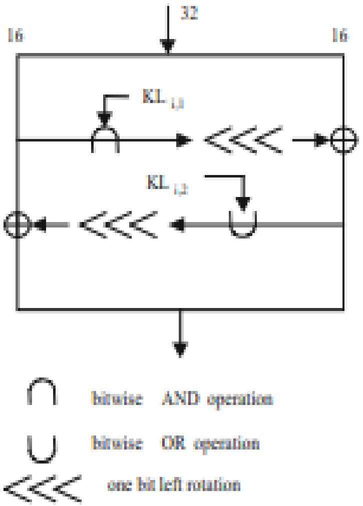

Fig.2. FL Function [17]

3.3. FI Function

FI refers to "Irregular Feistel" or "Feedback Input"[19]. As shown in Figure (3) Four rounds of operation are involved in this function. The FI function generates 16-bit output data from 16-bit input data. The input data is divided into two parts: the right 7-bit (R0) and the left 9-bit (L0). In an odd number of rounds, the left 9-bit (L0) is processed through the S9 box. In an even number of rounds, the right 7-bit (R0) is processed via the S7 boxوThe operations of this function p are defined as follows. The 16-bit value (L_4||R_4) is the function's return value [20].

$$L_1 = R_0 and, R_1 = S9[L_0] \otimes ZE(R_0) \square \quad \square \quad Equ(2)$$

$$L_2 = R_1 \otimes KI_{i,j,2} and, R_2 = S7[L_1] \otimes TR(R_1) \otimes KI_{i,j,1} \square \quad \square \quad Equ(3)$$

$$L_3 = R_2 and, R_3 = S9[L_2] \otimes ZE(R_2) \square \quad \square \quad Equ(4)$$

$$L_4 = S7[L_3] \otimes TR(R_3) and, R_4 = R_3 \square \quad \square \quad Equ(5)$$

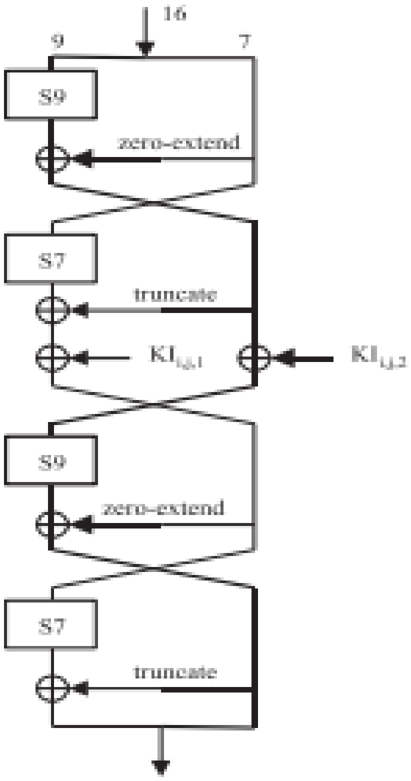

Fig.3. FL Function [16]

4. Proposed Method

Based on the Kasumi algorithm, we proposed modifying the used keys to improve the efficiency of the algorithm and obtain cipher text with higher security criteria.

Kasumi Block Cipher is a block cipher consisting of eight rounds, each of which requires a 128-bit key, which in turn is divided into eight parts with lengths of 16 bits for use in the functions of the Kasumi algorithm (FL, FO, FI). Therefore, as shown in Figure (4) the 16-bit key must be calculated before starting to execute the algorithm functions, as follows:

1) Use a computer standard function to generate a random number between 0-1.

2) Test the generated random number. If its value is greater than 0,5 this means that the added bit of the key is 1, otherwise 0.

3) Steps 1 and 2 are repeated 16 times until a 16-bit binary string is obtained

4) The binary string, which is 16 bits long, is recreated 8 times to form the total 128-bit key used in each round.

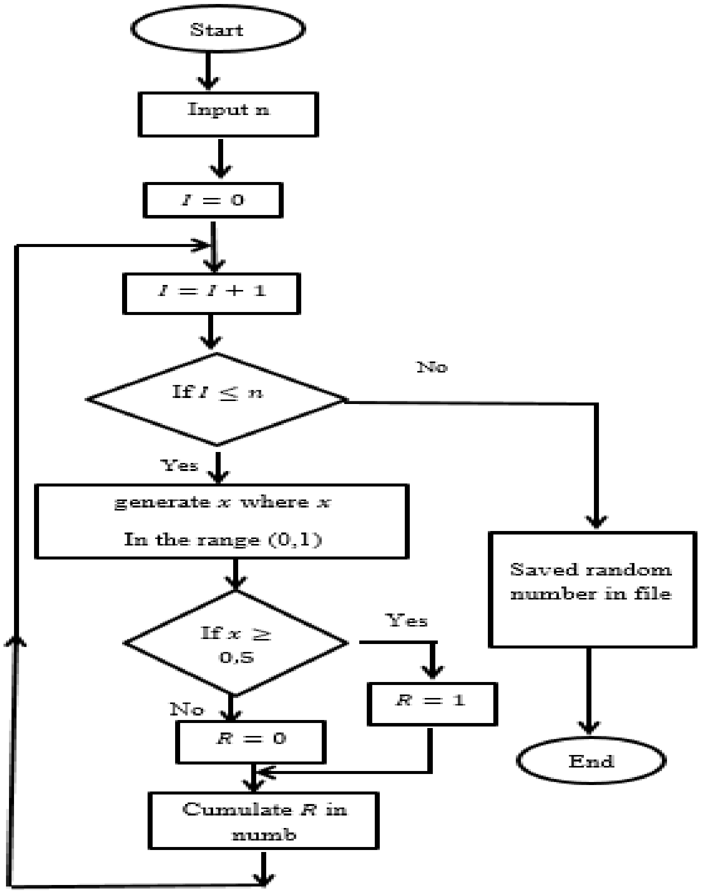

Fig.4. Modification of Key Generation in Kasumi Encryption Algorithm

5. Simulation Results and Discussions

Various statistical tests can be used to evaluate the randomness of the sequence, e.g., NIST, and NESSIE. In our system, National Institute of Standards and Technology (NIST) statistical tests are used to evaluate the modified Kasumi block cipher and to evaluate the evolved random keys and the keys of traditional algorithms. We tested about 15 times for the keys and 14 tests were passed. The developed random keys and the keys of traditional algorithms were tested with statistical tests of the National Institute of Standards and Technology (NIST), which included comparing and concluding that the developed keys have the highest randomness, especially in linear complexity, and frequency within the tests. Cluster and random exploration, leading to a better quality of encryption, that we tested about 15 times for the cipher text, where all 15 tests were passed, and the results of the NIST test for the cipher text resulting from the modified Kasumi algorithm were better, especially in the frequency within block test that was evaluated by (0.49590998713105255) and the approximate entropy test that was evaluated by (0.4922198616875501). We conclude from this that encryption using the modified algorithm achieved higher security. The encryption time required by the modified algorithm indicates a reduction of a few seconds compared to the original Kasumi at the rate of (0.686461384). We propose to replace the S-box equations with the chaotic map equations in future work.

The statistical tests of NIST are performed on the sequence of binary codes that represent the encrypted text files that size it is 2MB which are taken from a data set in the site (Plain Text Wikipedia 2020-11) after converting to the binary form. the below Table 2 below shows the test results of NIST.

Where statistical metrics were also conducted on the sequence of binary codes that represent the encrypted text files that different sizes which are taken from a data set in the site (Plain Text Wikipedia 2020-11) after converting to the binary form. Table 3 and Table 4 show the results of statistical metrics.

Table 2. Shows NIST Testing Results

Seq.	Test	Testing Results for The Key Before Algorithm Development	Testing Results for The Key After Algorithm Development	Testing Results for The Cipher Text Before Algorithm Development	Testing Results for The Cipher Text After Algorithm Development	Status
1	Monobit	0.4121287067497929	0.5009264885803283	0.5034734879403018	0.4999823405432083	Pass
2	Frequency Within Block	0.5092146519237125	0.5033227868656565	0.502676550399881	0.49590998713105255	Pass
3	Runs	0.4271146870974245	0.4767447198238142	0.4998914313270481	0.49854899834934424	Pass
4	Longest Run Ones in a Block	0.44314236107833394	0.5105298483718963	0.495581297601395	0.4939496429620972	Pass
5	Binary Matrix Rank	0.4959255220843331	0.5059368498552044	0.5176467615837129	0.5119986617030785	Pass
6	DFT	0.4716617976318228	0.4829353668261361	0.480712008602264	0.4764733150453246	Pass
7	Non-Overlapping Template Matching	0.46101849993077526	0.4473440173074974	0.4464604820985894	0.445468655070751	Pass
8	Overlapping Template Matching	0.4998914313270481	0.49854899834934424	0.7425641622108216	0.10860998334665199	Pass
9	Maurer’s Universal	0.9275231603850289	0.9987462061757786	0.9985704206503018	0.9994322452010559	Pass
10	Linear Complexity	0.7631806588283243	0.2620329750312008	0.47302528531042276	0.8672009104768315	Pass
11	Serial	0.33690997746885004	0.5113034583194324	0.5052977986233931	0.4994495816509583	Pass
12	Approximate Entropy	0.3467253771252111	0.49608572271478113	0.49744933195365243	0.4922198616875501	Pass
13	Cumulative Sums	0.4537721314254243	0.5159476585031055	0.5262396277808412	0.515107962803473	Pass
14	Random Excursion	0.5714016149762504	0.5046128801415981	0.41992825306722015	0.4345790470212821	Pass
15	Random Excursion Variant	0.203523916514654	0.2431332266534907	0.4116094464565782	0.6112017747591116	Pass

Table 3. Results of Statistical Tests for Traditional Algorithm

Text Size	Mean Square Error	Mean Absolute Error	Correlation Coefficient
1kb	7448.97370983447	71.7760533426766	0.0136514524231405
2kb	8015.99901768173	74.9935436688584	0.0286378316901072
10kb	7630.58673915154	72.5698089314024	0.00608243572418189
15kb	7841.65866333377	73.3866986647908	0.00263625112331851
25kb	7761.77049308432	73.0277848950357	-0.00422292863961755
30kb	7983.82122026345	73.7451172872013	-0.00215781139682037

Table 4. Results of Statistical Tests for Modified Algorithm

Text Size	Mean Square Error	Mean Absolute Error	Correlation Coefficient
1kb	7694.03310613437	72.7161173508994	0.00315337404103264
2kb	7845.6836935167	72.8914391946858	-0.0131114973313275
10kb	7677.78837006116	73.1154039463693	0.0196565282718839
15kb	7904.11722141823	73.6860665332863	-0.00157990512928648
25kb	7694.48652027819	72.7202914018201	-0.000901068175082584
30kb	7977.32066321515	73.9368288288471	-6.52493096844125E-06

6. Conclusions

Through developing a KASUMI algorithm that depends on Using random keys in all the rounds The developed random keys and traditional algorithm keys were tested with statistical tests of NIST, which made up a comparison and conclusion that the developed keys have higher randomness, especially in linear complexity, Frequency within the block, and random excursion tests, which leads to a better quality of encryption. Through testing the cipher text with frequency within the block test that was evaluated by (0.49590998713105255) and the approximate entropy test that was evaluated by (0.4922198616875501) for each cipher text which resulted from standard and modified Kasumi algorithm and Due to the quality of statistical metrics that were checked in this paper. Therefore, we can conclude that our modified Kasumi algorithm achieved more secure data in its resulting cipher text.

Acknowledgment

The authors would be grateful to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) in Baghdad, Iraq for its collaboration and support in the present work.

7. Reference

[1]. MEHDI, S.A., A novel steganography method based on 4 dominations standard chaotic map in the spatial domain. J. Theor. Appl. Inform. Technol, 2018. 96: p. 16.

[2]. Wang, X., et al., A new chaotic system with stable equilibrium: From theoretical model to circuit implementation. Ieee Access, 2017. 5: p. 8851-8858.

[3]. Linwa, A.C.B., and J.-M.D. Lebi, SURVEY OF CRYPTOGRAPHY ALGORITHMS FOR SUB-SAHARAN COUNTRIES. Information Technologist, 2020. 17(2).

[4]. Dhamodharan, G., S. Thaddues, and T. Manivannan. A new secure mapping scheme on elliptic curve cryptography for the Internet of things. in AIP Conference Proceedings. 2024. AIP Publishing.

[5]. Ismael, A.Y., Construct a Strong and High-Performance Algorithm to Generate Pseudorandom Number Generator (PRNG) for Stream Cipher. 2019, University of Baghdad.

[6]. Jabbar, K.K., Ghozzi, F., and Fakhfakh, A.: ‘Image Encryption Performance Analysis Using Reversible Logic Gates’, Mustansiriyah Journal of Pure and Applied Sciences, 2024, 2, (1), pp. 93–103-193–103.

[7]. Dilip Kumar, S.S., ASIC design of High-Speed Kasumi Block Cipher. INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT), 2014. 3(2): p. 398-401 DOI: 10.17577/IJERTV3IS20372.

[8]. Abbas, M.A.: ‘Secure authentication scheme to thwart known authentication attacks using Mobile Device’, Mustansiriyah Journal of Pure and Applied Sciences, 2024, 2, (1), pp. 46-61

[9]. Liu, L. and S. Miao, A new image encryption algorithm based on a logistic chaotic map with varying parameters. SpringerPlus, 2016. 5: p. 1-12.

[10]. Madani, M. and C. Tanougast, FPGA implementation of an enhanced chaotic-KASUMI block cipher. Microprocessors and Microsystems, 2021. 80: p. 103644.

[11]. De Silva, C.S., Implementation of A5 Confidentiality and Integrity Cryptographic Algorithms in GSM.

[12]. Salami, Y., V. Khajevand, and E. Zeinali, Cryptographic Algorithms: A Review of the Literature, Weaknesses and Open Challenges. Journal of Computer & Robotics, 2023. 16(2): p. 46-56.

[13]. Ibrahim, M.S., Y.A. Abbas, and M.H. Ali, The Performance of Various Lightweight Block Ciphers FPGA Architectures: A Review. Al-Iraqia Journal for Scientific Engineering Research, 2022. 1(1): p. 124-129.

[14]. Jiexian, H., et al., On the dynamic reconfigurable implementations of MISTY1 and KASUMI block ciphers. Plos one, 2023. 18(9): p. e0291429.

[15]. Gupta, D., S. Tripathy, and B. Mazumdar, Correlation power analysis of KASUMI and power resilience analysis of some equivalence classes of KASUMI S-boxes. Journal of Hardware and Systems Security, 2020. 4: p. 297-313.

[16]. Madani, M., S. Chitroub, and C. Tanougast. Two KASUMI components for an optimal implementation of the A5/3 algorithm. in 2017 International Conference on Circuits, System and Simulation (ICCSS). 2017. IEEE.

[17]. Muthalagu, R. and S. Jain, Improved KASUMI block cipher for GSM-based mobile networks. Journal of Cyber Security Technology, 2020. 4(4): p. 197-210.

[18]. Muthalagu, R. and S. Jain Reducing the time required by KASUMI to generate output by modifying the FL and FI functions. Iran Journal of Computer Science, 2019. 2(1): p. 33-40.

[19]. Elouafiq, A., Authentication, and Encryption in GSM and 3GUMTS: An Emphasis on Protocols and Algorithms. arXiv preprint arXiv:1204.1651, 2012.

[20]. Muthalagu, R. and S. Jain, A novel modified KASUMI block chiper for global system for mobile communications. International Journal of Computers and Applications, 2021. 43(8): p. 805-811.