International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1245-1253 www.ijaem.net ISSN: 2395-5252

New Hybrid Image cryptography algorithm based on new 10D chaotic system

Haider K. Hoomod

Mustansiriyah University college of Education, computer science Dept, Baghdad, Iraq

---

Submitted: 10-08-2022 Revised: 22-08-2022 Accepted: 24-08-2022

ABSTRACT:
With the proliferation of data transfers across networks and the internet, it is now possible to keep these files secure through the use of various forms of electronic communication. Since images are so widely utilized in all kinds of visual media, the process of encrypting them is a valuable approach for preserving image information and an efficient means of sending various sensitive data. In order to meet the needs for protected and high-quality image storage and transmission. This paper proposes a method for encrypting images that is both efficient and effective, employing a key generation technique that makes use of a 10D chaotic system to generate chaos keys in accordance with the PRESENT-SPECK algorithms. As part of the proposed solution, the picture data was requested into the block before encryption. The combined blocks formed a secret picture. The generated key and the proposed procedure have both passed several testes across a number of use cases.

Keywords: Image Encryption, Hybrid PRESENT-SPECK Algorithm, 10D chaos Key generation, lightweight cryptography

I. INTRODUCTION

In today's environment, instant and safe communication is a need. Third-, fourth-, and fifth-generation technologies are steadily expanding the available bandwidth. Because of the belief in a global village, digital content is freely accessible from anywhere in the world. Smart and simple information that can be accessed from any remote station causes a large vulnerability of digital information as a result of developing technologies [1]. One of the most important issues in the field of information science is ensuring the safety of digital multimedia. The growing dissemination of digital information via the internet, especially through social media such as Facebook and Twitter, has made it crucial to safeguard our most sensitive data from unauthorized access, duplication, transmission, and use [2]. Thanks to developments in digital media and other multimedia-related technology, I may now follow several tried-and-true protocols to lessen the likelihood that our private digital photos, songs, and movies will be stolen and used illegally online [3].

There is no fundamental aspect of human life that has not been profoundly altered by the advent of multimedia communication[4]. Increases in the amount of multimedia data that must be transferred via insecure networks are an inevitable consequence of the proliferation of IoT and its numerous uses in areas as diverse as sensing, healthcare, and industry[5]. However, because of their diminutive stature, IoT-driven installations have resource constraints. With limited resources, an IoT platform precludes the use of traditional algorithms for data encryption [6,7,8]. A number of works[9,10,11] analyze the efficiency of the SPECK/SIMON cryptographic algorithm and suggest an IoT-friendly lightweight-cryptography algorithm based on SPECK/SIMON. As opposed to traditional studies that mostly reflect hardware implementations, this one centers on how speed might be improved from a software standpoint. The contribution investigates the properties of the SPECK/SIMON cipher, with an eye toward employing it for IoT healthcare applications [11,12,13], with the goal of improving its performance in a practical context.

A newly designed encryption technique depending on AES and RSA is proposed in this study [14] for use in Bluetooth data transfer. The authors provided an in-depth breakdown of their proposed encryption method. The 128-bit key will be encrypted by RSA during the operation. The message from the sender will be encrypted using AES. In the same vein, the encrypted values will be used to create a convoluted message. The process of decryption can be thought of as the inverse of encryption. While this hybrid encryption approach can provide a hash function and a digital signature, it is not intended to detect non-repudiation versus cipher-text or origin authenticity.

The authors of [20] presented a new method that combines elements of AES, RSA, and SHA-1. Three separate algorithms' strengths Ire combined in this one to improve security. The authors further claim that the suggested technique is safe and reliable because it takes full advantage of the strengths of existing algorithms. For digital signatures in particular, the author used SHA-1, and RSA was used for its superior key management.

In [21], the authors contrast the security provided by algorithms using public and private keys, RSA and DES, respectively. The researchers concluded that the major feature distinguishing RSA public key based algorithm from DES secret key optimization Technique was linked to the incoming plain text rate throughout the process of encryption and decryption. The authors also noted that the RSA method required less time for execution overall compared to the DES algorithm when carrying out the same tasks of encryption and decryption. Notably, the DES algorithm can encrypt and decrypt data more quickly than the RSA method can [21].

This research aims to draw attention to, and offer a solution for, the flaws in the Bluetooth encryption method. The Bluetooth E0 algorithm has been the target of several assaults, the goal of which is to interpret the faults in the previous design; it has been demonstrated that the algorithm can be cracked in only 264 operations [14, 15], [16].

The structure of the proposed method is laid out in full, and it will be used to encrypt photos taken by like a security camera. Some many set images sequences in the IoT framework are used to regulate the catching activity and move Images securely to the server site (and sent with encrypted data image and organized in the receiver side), and PRESENT calculation is improved by merging it with SPECK calculation, increasing the degree of safety. To further lower the encryption time while keeping the realistic trade-off among security and efficiency, this work proposes enhancing the implementation of the original SPECK encryption using the PRESENT method. The execution time and memory usage of the proposed work have been compared to those of the classic SPECK block cipher algorithms. The outcomes demonstrate that the suggested approach is effective for protecting information in an IoT-driven environment.

II. THE PROPOSED SYSTEM

The two ideas for picture encryption are based on the idea of combining the PRESENT and SPECK methods in different scenarios to address the limitations of each technique and thwart various attacks.

The proposed encryption method described in this system's initial concept for protecting stored photos. In order to encrypt the taken image with the suggested technique, the image is first divided into 256-bit blocks, then the Speck technique is used for different rounds, and finally the S-box and P-Value stages are applied to the result. After going through this process 10 times, I have what need to send towards the data center.

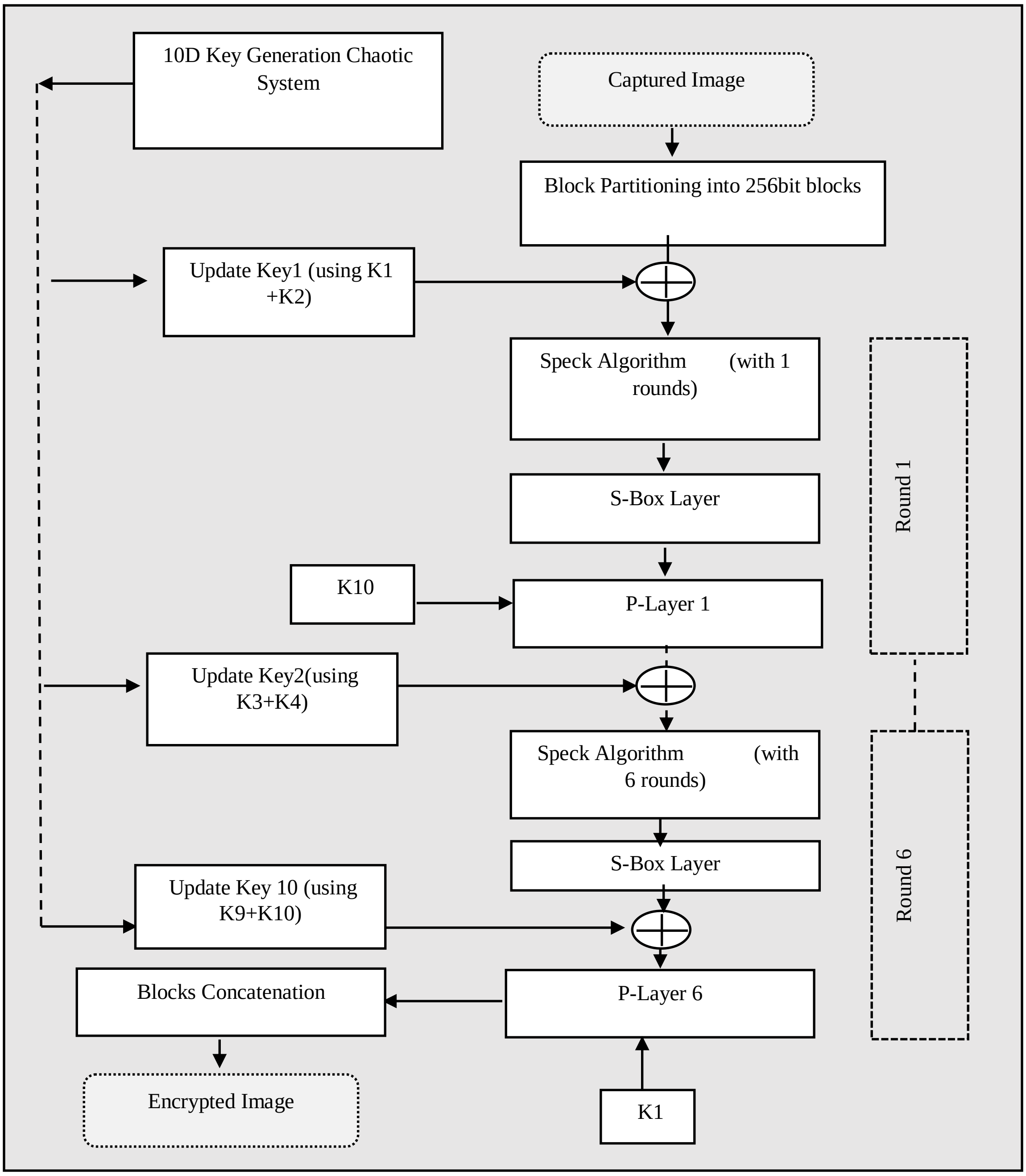
The proposed encryption algorithm, known as a hybrid Present-Speck, is developed by fusing the Speck algorithm (containing 1 to 6 rounds to shorten the Speck encryption time) and the Present algorithm. The combination Present-Speck algorithm is depicted in Figure 1.

The difficulty of the current encryption results has been increased by adding a Speck algorithm as a layer to the Present round layers, and also the proposed algorithm was updated to enhance the Present algorithm to prevent numerous attacks. In the proposed method, two distinct kinds of chaotic systems are joined to generate keys. As encryption keys, they Ire dispersed between both the Present algorithm as Ill as the Speck algorithm. A higher degree of randomness in the cipher text output was achieved with the help of these chaotic keys, which also provided the best possible strength here to encryption algorithm.

As seen in figure 1, the first step involves separating the image into its component color channels (RGB). Each of these bands is divided into 256-bit squares before being encrypted and delivered. If the integer is not a multiple of 256, zeros are added to the beginning and end before encryption, and zeros are removed before decryption.

The encryption Stage starts with the Modified Lightweight PRESENT algorithm with SPECK Algorithm. Here, I suggest a hybrid approach to cut down on both the algorithm's complexity and the time it takes to build it. The round calls for using the SPECK with one round, the Speck rounds increased while global number round of the proposed hybrid algorithm increased. By combining the PRESENT method and the SPECK algorithm, the proposed system is able to perform an improved operation. The keys Ire generated in a 10D hyper-chaotic system and used to improve the algorithm's efficiency by increasing the number of randomly encoded results.

The PRESENT Algorithm employs the SPECK Algorithm, which is a secure lightweight method that offers security solutions for necessary applications even when operating under constraints. The proposed hybrid method is a set of lightweight rectangular codes designed for low-power devices with a need for cryptographic protection. The proposed hybrid algorithm with various key and block sizes. For each block, there are two different words, each of whom is 256 bits in length. As can be seen in Figure 2, this plan uses a total of 6 rounds.



International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1245-1253 www.ijaem.net ISSN: 2395-5252

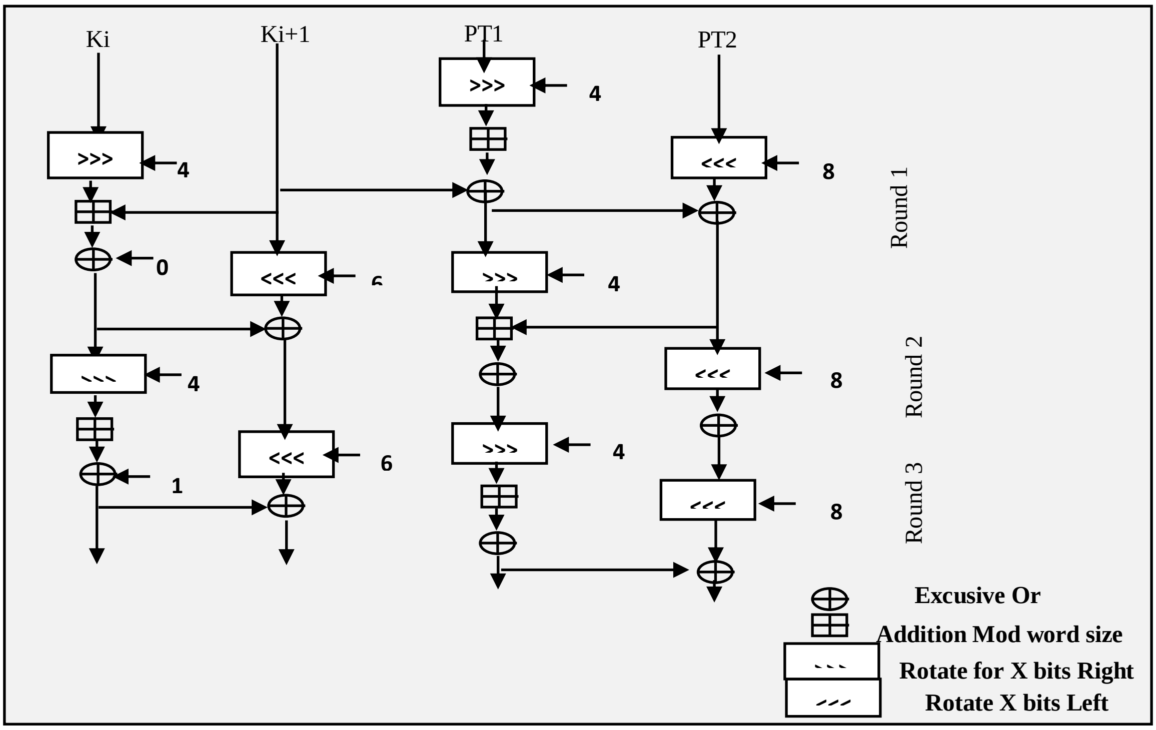


Figure 2: The proposed Speck Algorithm structure

Using a 10-dimensional novel chaotic system (the Haider10 chaotic system) with varying initial and parameter values, random numbers I generated them using the chaos keys generation technique. Proposed hybrid encryption method that uses chaos keys(K1,….,K10).

To investigate chaotic features (like randomness, dynamics, and sensitivity to the (initials and equation parameters) in the generation of a set of numerical output sequence), a novel 10-dimensional system of differential dynamic chaotic equations has been investigated (checked) and implemented using the of chaos theory. New equations for a chaotic system in 10 dimensions are:

$x_{i+1} = (r\,(x_i^{\,2} - p_i - y_i^2) - u(z_i - x_{i\,+}\,k_i)) - \exp\,(y_i - u\,x_i)$

$y_{i+1} = s\,(y_{i-}\,x_i^3) + (\exp(r\,z_i\,x_i - s\,y_i\,k_i) - j_i\,p_i)/\exp(1+y_i^2)$

$z_{i+1} = (u\,(y_{i\,+}\,z_i) - j_i\,y_i\,/(s\,j_i - x_i) + \exp(u(w_i - r\,k_i))/(\,j_i + z_i - m_i))$

$k_{i+1} = (m_i - u\,j_i - r\,y_i\,w_i - b\,k_i - u\,x_i\,j_i)/\exp(u\,x_{i\,+}\,j_i)$

$p_{i+1} = \exp(b\,(j_i\,k_i - u\,y_i\,m_i - z_i\,y_i^u)/(\,m_i - x_i))$

$w_{i+1} = |\exp(w_i - m_i) + j_i\,k_i\,|$

$m_{i+1} = u\,(w_i - k_i) - z_i$

$j_{i+1} = j_i^2 - p_i\,m_i - x_i^2$

$q_{i+1} = q_i - k_i$

$h_{i+1} = j_i\,q_{i\,-}\,x_i\,m_i$

Where: $h_i, q_i, j_i, m_i, w_i, p_i, k_i, z_i, y_i, x_i$ are selected to be numerical values start with initials values with interval (-1.0, 1.95), s=(0.1, 65), r=(10,100), b=(7.0,11.5), and u=(1.0, 11.1)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1245-1253 www.ijaem.net ISSN: 2395-5252

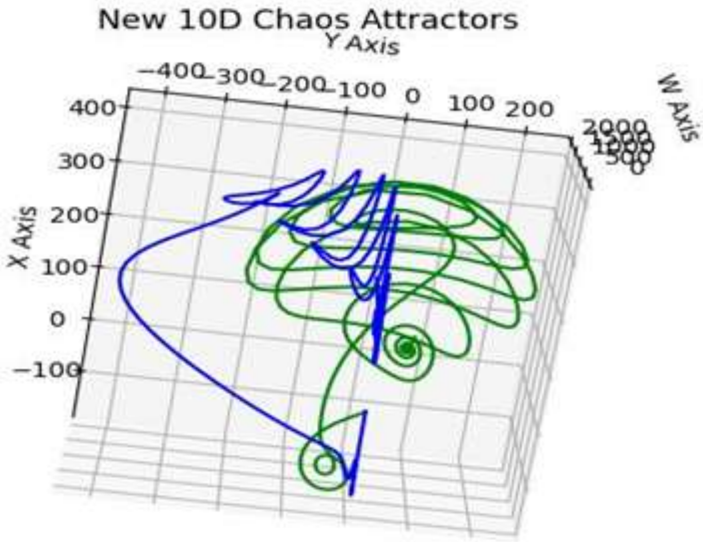


Figure 3: Chaotic System output behavior.

Lyapunov exponents Ire determined for a variety of initial conditions and parameters using an implemented and tested version of the proposed unique 10D chaotic system (called the Haider10 chaos system). Maximum Lyapunov values for the suggested novel 5-dimensional chaotic system at the given parameter values (s=10, r=45, b=4, and u=1.25) are (0.4453), (0.5556), (1.9077), (0.8756), (-0.4566), (-0.9899), (-2.1290), (1.3280), (-0.7844), and (-2.9076), where 5 of which are positive.

III. EXPERIMENTAL RESULTS

IoT picture security is an emerging area of study. To put the proposed system into action, I need a variety of hardware and software components. You'll need some rather standard hardware, like a camera, Raspberry Pi gadgets, a capable computer, and an accessible network. I need to meet software requirements in (Python-language, Raspbian system, and Windows10 for the control computer).

To make the IoT image better safe and resistant to a wider range of assaults, I implement and test a Hybrid Speck-Present method, a modified Present algorithm, and a modified Speck algorithm. Figure 4 shows an example of the output of the proposed algorithm. NIST tests, humming-distance, and Entropy are used to evaluate the performance of these suggested algorithms.

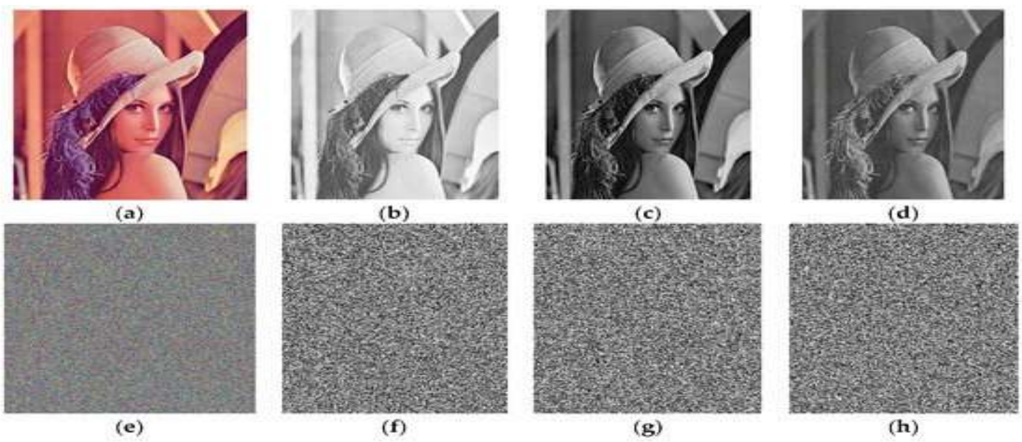


Figure 4: The result of image bands encryption using the proposed hybrid methods: a) plain image , b) plain red band , c) plain green band, d) plain blue band
e) ciphered image, f) ciphered red band, g) ciphered green band, h) ciphered blue band.

Table (1) displays the results of benchmark and applied testing on the suggested ciphering algorithms (NIST tests), contrasting the proposed HSPA, MPS, and MSA with their original algorithm's execution time.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1245-1253 www.ijaem.net ISSN: 2395-5252

Table (1) The Average time Results (in sec)

Image size pixel	HPSA time (sec)	PA time (sec)	SA time (sec)
Encrypt (128*128)	0.455	0.342	0.565
Decrypt (128*128)	0.456	0.344	0.568
Encrypt (256*256)	0.933	0.822	0.977
Decrypt (256*256)	0.933	0.823	0.979
Encrypt (512*256)	1.116	1.109	1.186
Decrypt (512*256)	1.117	1.108	1.189
Encrypt (512*512)	2.940	2.879	3.564
Decrypt (512*512)	2.946	2.889	3.569
Encrypt (800*600)	6.897	6.866	7.675
Decrypt (800*600)	6.897	6.889	7.679

From table (1), the proposed algorithms have close execution-time in (encryption, decryption) with Present algorithm and fast from the Speck algorithm. To ensure that the suggested Hybrid Present Speck Algorithm (HPSA) has the best security from the Present Algorithm (PA) and Speck Algorithm (SA), the results of NIST tests of the encryption methods are shown in Table (2). (SA). The HPSA is also resistant to a variety of attacks. All of the NIST tests for the suggested encryption methods have been successful.

Table (2) NIST Tests Results of the proposed cipher algorithms

Test Name	HPSA	PA	SA
Frequency (Monobit) test	0.812	0.455	0.329
Runs test	0.778	0.690	0.436
Discrete Fourier transform	0.760	0.056	0.129
Block frequency	0.609	0.304	0.043
Longest runs test	0.574	0.008	0.005
Cumulative sums test	0.856	0.566	0.231
Serial test	0.960	0.764	0.562
Matrix rank test	0.809	0.002	0.046
Overlapping template test	0.934	0.762	0.855
Linear complexity test	0.860	0.787	0.078
Nonoverlapping template test	0.895	0.006	0.034
Random excursions variant test	0.799	0.631	0.723
Random excursions test	0.989	0.978	0.800

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1245-1253 www.ijaem.net ISSN: 2395-5252

Many cryptanalytic techniques that target blocks devices and chaotic systems are useless against the solutions I propose. A table shows that the suggested system is safe and reliable enough for use (2). There were examples of buzzing distance, entropy, MAE, NPCR, and UACI in Tables 3, 4, and 6.

Table (3) Correlation Coefficients of Encrypted image.

image Size (KByte)	**HPSA**	**PA**	**SA**
100	0.00544	0.00231	0.00208
200	0.00783	0.00532	0.00420
300	0.00760	0.00677	0.00675
400	0.00690	0.00599	0.00651
500	0.00788	0.00675	0.00459

Table (4) Entropy Results of Encrypted image.

image Size (KByte)	**HPSA**	**PA**	**SA**
100	7.899	7.338	7.121
200	7.897	7.655	7.109
300	7.978	7.708	7.124
400	7.988	7.721	7.175
500	7.981	7.689	7.231

Table (5) hamming distance Results of Encrypted images.

image Size (KByte)	**HPSA**	**PA**	**SA**
100	608	455	412
200	990	776	709
300	1080	900	879
400	1290	980	980
500	1690	1090	998

Table (6) Plaintext sensitivity in terms of MAE, NPCR and UACI.

Measure type	**HPSA**	**PA**	**SA**
MAE	41.453	27.908	34.223
NPCR	64.675	45.221	47.853
UAC1	21.690	15.889	18.980

Apparently, the HPSA, PA, and SA have a sensitivity to the plain data; and indicates they more sensitivity to changing in output results.

IV. CONCLUSIONS

In this paper, I present an encryption scheme for IoT-captured image data that makes use of robust chaotic maps and a hybrid of the cryptographic algorithms (PRESENT-SPECK) with some modifications. This scheme achieves satisfactory results in terms of the NIST, Correlation Coefficients, Hamming-distance, Entropy, MAE, NPCR, and UACI, and it avoids the degradation that would otherwise result from the computer's finite precision. By encrypting and decrypting a string a total of times, the proposed approach combines effective confusion and diffusion qualities. An exceptionally vast key space, as shown by the research, gives the proposed cryptosystem a better level of security. Results from experiments show that it is possible to reconstruct the original image even when noise is present, demonstrating its robustness versus noises and tiny external perturbations. Symmetric techniques for both encryption and decryption make this a good choice for protecting color images.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1245-1253 www.ijaem.net ISSN: 2395-5252

REFERENCES

[1]. Pradyumna Gokhale, Omkar Bhat and Sagar Bhat" Introduction to IOT", International Advanced Research Journal in Science, Engineering and Technology, Vol. 5, Issue 1, January 2018.
[2]. Ahmed Majed, Haider Kadhim Hoomod:" Secure Email of Things Based on Hyper Chaotic system", Al-Mustansiriyah University, Baghdad, Iraq, M.Sc. Thesis ,2020.
[3]. Bogdanov, A, Knudsen, LR, Leander, G, et al. "Present: an ultra-lightweight block cipher". In: Proceedings of the international workshop on cryptographic hardware and embedded systems, Vienna, 10–13 September 2007, pp.450–466. Berlin: Springer.
[4]. Ling Song, Zhangjie Huang, Qianqian Yang, "Automatic Differential Analysis of ARX Block Ciphers with Application to SPECK and LEA", Australasian Conference on Information Security and Privacy, 9723. 379-394. 10.1007/978-3-319-40367-0_24
[5]. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan weeks, and Louis Wingers," Simon and Speck: Block Ciphers for the Internet of Things", ACR Cryptol. ePrint Arch. 2015 (2015): 585
[6]. Beaulieu, R, Treatman-Clark, S, Shors, D, et al. The Simon and speck lightweight block ciphers. In: Proceedings of the 52nd ACM/EDAC/IEEE design automation conference (DAC), San Francisco, CA, 8–12 June 2015, pp.1–6. New York: IEEE.
[7]. Yang, G, Zhu, B, Suder, V, et al. The Simeck family of lightweight block ciphers. In: Proceedings of the international workshop on cryptographic hardware and embedded systems, Saint-Malo, 13–16 September 2015, pp.307–329. Berlin: Springer.
[8]. Dinu, D, Perrin, L, Udovenko, A, et al. Sparx: a family of ARX-based lightweight block ciphers provably secure against linear and differential attacks. In: Proceedings of NIST workshop on Lightweight Crypto CRYPT'16, 18 October 2016, p.121. Gaithersburg, MD: NIST.
[9]. Banik, S, Pandey, SK, Peyrin, T, et al. Gift: a small present. In: Proceedings of the 19th international conference on cryptographic hardware and embedded systems, Taipei, Taiwan, 25–28 September 2017, pp.321–345. Berlin: Springer.
[10]. Koo, B, Roh, D, Kim, H, et al. Cham: a family of lightweight block ciphers for resource-constrained devices. In: Proceedings of the international conference on information security and cryptology, Seoul, South Korea, 29 November–1 December 2017, pp.3–25. Berlin: Springer.
[11]. Sawant, A. G. et al. "Implementation of SIMON & SPECK Algorithm." Journal of emerging technologies and innovative research (2019).
[12]. Leander G., Paar C., Poschmann A., Schramm K., "New lightweight DES variants.", Fast Software Encryption. FSE 2007. Lecture Notes in Computer Science, vol 4593. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-74619-5_13.
[13]. nasour bagheri & Ebrahimpour, Reza & Ghaedi Bardeh, Navid," New differential fault analysis on PRESENT", EURASIP Journal on Applied Signal Processing,2013. 145-. 10.1186/1687-6180-2013-145.
[14]. Rege, K., Goenka, N., Bhutada, P. and Mane, S. (2013) Bluetooth Communication Using Hybrid Encryption Algorithm Based on AES and RSA. International Journal of Computer Applications, 71, 10-13.
[15]. Armknecht, F. and Krause, M. (2003) Algebraic Attacks on Combiners with Memory, in Advances. In: Boneh, D., Ed., Advances in Cryptology—CRYPTO 2003, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 162-175.
[16]. Hermelin, M. and Nyberg, K. (2000) Correlation Properties of the Bluetooth Combiner. In: Song, J., Ed., Information Security and Cryptology—ICISC'99, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 17-29.
[17]. Lu, Y. and Vaudenay, S. (2004) Faster Correlation Attack on Bluetooth Keystream Generator Eo. In: Franklin, M., Ed., Advances in Cryptology—CRYPTO 2004, Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 407-425. https://doi.org/10.1007/978-3-540-28628-8_25
[18]. Albahar, M., Haataja, K. and Toivanen, P. (2016) Towards Enhancing Just Works Model in Bluetooth Pairing. International Journal on Information Technologies & Security, 8, 67-82.
[19]. Parsharamulu, B. and Krishnaiah, R.V. (2013) A New Design of Algorithm for Enhancing Security in Bluetooth

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 8 Aug. 2022, pp: 1245-1253 www.ijaem.net ISSN: 2395-5252

Communication with Triple DES. International Journal of Science and Research, 2, 279-283.

[20]. Najar, J.M. and Dar, S.B. (2014) A New Design of a Hybrid Encryption Algorithm. International Journal of Engineering and Computer Science, 3, 9169-9171.

[21]. Singh, S., Maakar, S.K. and Kumar, S. (2013) A Performance Analysis of DES and RSA Cryptography. International Journal of Emerging Trends & Technology in Computer Science, 2, 418-423.