Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

Design of Extended Hamming Code Technique Encryption for Audio Signals by Double Code Error Prediction

R. Asokan[1], T. Vijayakumar[2]

[1]Professor and Principal, Kongunadu college of Engineering and Technology, Tholurpatti, Tamil Nadu, India
[2]Professor, Department of CSE, Jai sriram engineering college, Avinashipalayam, Tamil Nadu, India

E-mail: [1]asokece@yahoo.com, [2]vishal_16278@yahoo.co.in

Abstract

Noise can scramble a message that is sent. This is true for both voicemails and digital communications transmitted to and from computer systems. During transmission, mistakes tend to happen. Computer memory is the most commonplace to use Hamming code error correction. With extra parity/redundancy bits added to Hamming code, single-bit errors may be detected and corrected. Short-distance data transmissions often make use of Hamming coding. The redundancy bits are interspersed and evacuated subsequently when scaling it for longer data lengths. The new hamming code approach may be quickly and easily adapted to any situation. As a result, it's ideal for sending large data bitstreams since the overhead bits per data bit ratio is much lower. The investigation in this article is extended Hamming codes for product codes. The proposal particularly emphasises on how well it functions with low error rate, which is critical for multimedia wireless applications. It provides a foundation and a comprehensive set of methods for quantitatively evaluating this performance without the need of time-consuming simulations. It provides fresh theoretical findings on the well-known approximation, where the bit error rate roughly equal to the frame error rate times the minimal distance to the codeword length ratio.

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

Moreover, the analytical method is applied to actual design considerations such as shorter and punctured codes along with the payload and redundancy bits calculation. Using the extended identity equation on the dual codes, decoding can be done at the first instance. The achievement of 43.48% redundancy bits is obtained during the testing process which is a huge proportion reduced in this research work.

Keywords: Hamming code, double code error prediction, audio signal, encryption, parity check

1. Introduction

The analog signals in digital systems are converted to bits, which are a digital sequence. A "Datastream" refers to this particular collection of bits. Catastrophic (major) data mistakes may be caused by a single bit being moved. Errors may be found almost everywhere in electronic equipment, and error detection and repair methods can be used to obtain an exact or close result [1].

The data mistakes will result in the erasure of crucial or confidential information. Even the smallest change in data may have a significant impact on the overall system performance. Digital systems often use 'Bit – transfer' for data transmission. If this is the case, the data inaccuracy is more than likely to be located between 0 and 1 [2-4]. Figure 1 shows simplified block diagram of digital communication system.

Cryptographic security against unauthorized intrusion is most often provided via encryption, both on Earth and in space. When transmitting data between a satellite and a ground station, encryption has become standard on the EO satellites themselves [5]. In practice, however, the most often used encryption algorithms are proprietary or obsolete, such as DES. An issue with the existing and newest encryption standard is raised since the encryption algorithms safeguarding potentially extreme sensitive information do not satisfy those already in place [6].

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

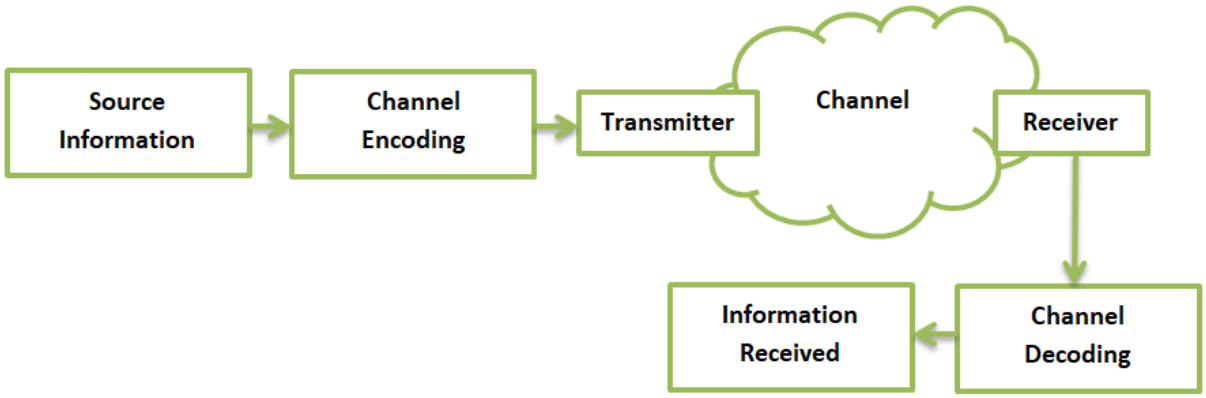

Figure 1. Simplified block diagram of communication channel

Using Hamming code, which is an error correction code, single-bit mistakes can be identified and fixed while propagating binary data from one unit to the next. Using basic parity, a single-bit error in a received message may be identified. Correcting these detected errors require the inclusion of some extra data and hence the erroneous bit location must be recognized. When a mistaken bit is found, it may be corrected by simply flipping or inverting the bit value to get it back to its original value. In this case, the repair is impracticable since there is only one parity bit after each bit mistake, regardless of bit position [7-10]. A source data message with extra bits may assist in detecting incorrect bits if the bits can be arranged in such a way that distinct incorrect bits produce unique error consequences.

As part of the military's digital communication facility systems, the forward error correction (FEC) must function accurately and reliably even when subjected to noise and interference. Forward error-correction coding is the most effective and efficient method to achieve this goal out of all the possibilities [11]. While the term "forward error correction" may be confusing, it refers to the use of digital signal processing to improve the reliability of data by adding a known structure to it before transmission. This structure gives the accepting system the

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

ability to identify and, if necessary, rectify mistakes caused by debasement of the supplied data channel and the applied receiver on the other end of the communication chain. By avoiding a request for retransmission of the original data, the coding method used in this system gives the decoder the ability to fix any mistakes it finds [12-14].

2. Organization of the Research

The remainder of the paper is structured as follows: Section 3 summarizes prior research on the extended hamming code method. Section 4 covers the structure suggested for developing a novel method to hammering code. Section 5 summarizes the findings. Section 6 addresses the conclusion and potential extension.

3. Preliminaries

Richard Hamming, a computer scientist, invented the Hamming error correcting and detection code in 1950. The early work on Hamming codes enabled massive computer machines to carry out a huge number of operations without encountering a single mistake [15].

The redundant bits are placed at the end of the data in enhanced Hamming code. Since the redundant bits are interspersed and ejected later at the receiver end, the overhead is reduced substantially. There is also a smaller amount of overhead bits used in the calculation of redundancy bits. [16].

To prevent data corruption or loss due to single-bit mistakes, Hamming code is an EDAC technique. The encoder receives errorless information that is k bits long as the input. The decoder uses Hamming theorems to create a n-bit code word by calculating the parity bits and adding them to the incoming data. Added parity bits have been added to the processed data, and is ready for storage [17].

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

Because of this, the onboard computer (OBC) of a nanosatellite uses RAM as its primary storage instead of flash memory. When data is stored, mistakes are more likely to happen than when it's being used. Typically, errors arise when radiated particles enter the RAM's memory cells [18].

The decoder's job is to look for and fix any mistakes in the data being sent. The Hamming theorem is used to determine the syndrome using a parity check matrix. Before extracting the new, error-free data, the decoder searches and corrects any mistake found in the codeword [19].

4. Methodologies

4.1 Design of an extension version of hamming code

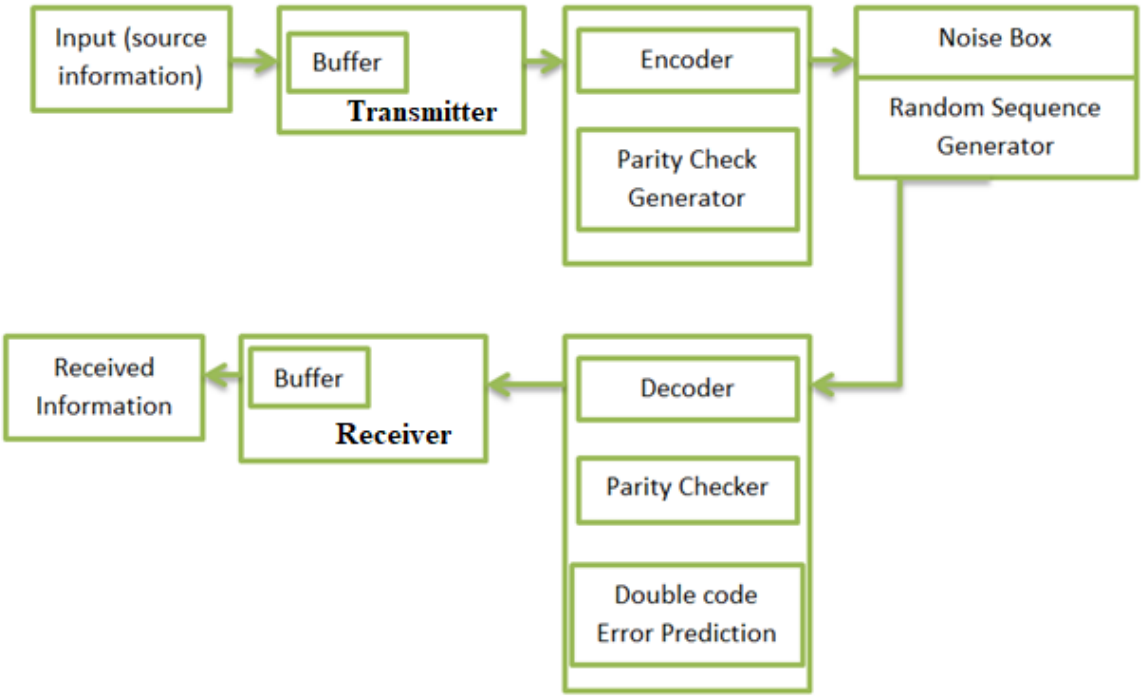

Figure 2. Double code error prediction decoder model

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

4.1.1 Construction of generator matrix

While encoding data to create a code word, the generator matrix (G) is utilised. The Hamming code is built on top of G, one of its foundational elements. The Hamming code is capable of SECSED because of the connection between the generator matrix and the parity-check matrix.

4.1.2 Construction of Parity-Check Matrix

When decoding and correcting the code word, a parity-check matrix (H) is utilised to extract an error-free message. The Hamming code is built on the basis of H. The Hamming code is capable of SECSEC because of the connection between the parity-check matrix and the generating matrix.

4.1.3 Relationship between G and H

$$G * H^T = 0 \tag{1}$$

As a last remark on G and H, basic matrix operations may be used to transform this matrix from a system to a non-systematic equivalent (for error free). Then each row's (or column's) value is multiplied by this number. The result of multiplying one row by a nonzero integer is added to another row (or column).

4.2 Hamming Encoder

This encoder generates the codeword (n-bits long) from the message (M) and the generator matrix using a Hamming encoding algorithm (G). Once the codeword has been produced, it includes the message's data as well as the parity bits

.

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

4.3 Hamming Decoder

In the Hamming decoder, a codeword (n-bits long) indicated by C and a parity-check matrix is decoded to produce a syndrome (r-bits long) (H). Once created, the syndrome includes the pattern of errors that may be used to identify and fix the problem.

4.4 Extended Hamming Code

An extra parity bit is used in the expanded Hamming code. As a result of this additional bit, the Hamming code's capabilities have been raised to SECDED. Both systematic and non-systematic implementations of the expanded Hamming code are possible [20].

4.4.1 Double Code Error Prediction (DCEP)

Figure 2 shows proposed double code error prediction (DCEP) decoder model which is an enhanced version of Hamming code. The advantage of this DCEP is that the algorithm can identify two types of errors due to the double error detection (DED). As a result of the code's non-systematic implementation, duplicate mistakes are easier to spot. DCEP performance may be estimated in part using standard formulae. This demonstrates that DCEP outperforms hamming code in terms of code rate and bit overhead when combined with SECSED's capabilities [21-25].

Remarks: Improving stage

The enhanced hamming code method uses the same amount of redundancy bits as the conventional hamming code method for some value of n. In any event, the necessary number of redundancy bits will sometimes be only one more than Hamming code raised in its count. According to statistics mathematical equation number 1, n-bit data requires "r" redundancy bits to get a single error correction. The following equation number 1 is defined for improved version,

$$2^{(r-1)} - 1 = n(2) \tag{2}$$

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

Owing to this, codewords that may be used with a 16-bit wide data bit and six redundancy bits will have a single error correction as well as two error detections. Areas 15, 14, 13, 12, 11, and 10 are used to set these six bits. Using the equations as a guide, the parity bits can be figured out.

5. Results and Discussion

The use of basic parity allows the identification of single-bit mistakes in a message that has been received. The bit position of the erroneous bit must be recognised in order for it to be rectified by adding more data. This table 1 contains input data information for testing. Besides, it depicts the codeword format for the sample data 10'b1100110011.

Table 1. Sample input data word format

0	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**

As long as the proposed system is in use, the coding process gives the decoder the ability to fix any mistake that is discovered without taking the risk of requesting retransmission of the original data [26]. The Hamming code is a common example of forwarding error correction that everyone is familiar with. In any case, when it comes to a communication system that makes use of forward error correction coding, the digital data source delivers a message data sequence to a systematic data encoder unit in the first step, which is described in the below table.

P [5] is selected in such a way that the entire bit position, including the redundant ones P [4:0], have the same amount of parity. Positions 15, 14, 13, 12, 11, and 10 include the parity bits. Even parity checks were per-shaped on 5, 5, 4, 3, 4 & 16 bits correspondingly for the calculation of parity bits. When hammering bits are computed, a total of 37 bits are added. Table 3 contains final results obtained by this proposed DCEP approach in extended hamming code.

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

Table 2. Original erroneous bit positions of input data

Input position sequence	Bit Position			
	P[0]	P[1]	P[2]	P[3]
0	0	0	0	0
1	1	0	0	0
2	0	1	0	0
3	1	1	0	0
4	0	0	1	0
5	1	0	1	0

Table 3. Final results obtained by DCEP

Received Information	Status of parity check in DCEP	Overall obtained Result comment
0000111100110011	000000	No Error
0000111100110111	100011	Odd Error type
0000111000110011	101011	Even Error type

Calculated results:

$$Payload = \frac{No.of\ data\ bits}{Total\ number\ of\ bits\ transmitted} \quad (3)$$

Obtained results data bits = 52 bits

Bits transmitted = 92 bits

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

$$Payload = \frac{52}{92} X\ 100(\%)$$

Payload = 56.52%

Redundancy bits = 43.48%

Payload and redundancy bits are calculated in percentage. To transmit or store data, the device uses a codeword like the one displayed. The parity bits are uprooted at the other end. The transmitted parity and the received codeword parity are compared using a parity check. The outcome of the test determines the direction of the mistake. If a single bit error has occurred, a mask will be generated and the data will be fixed [27]. Table 3 outlines the hamming code fault detection and repair procedure by giving odd or even type error for further testing.

6. Conclusion

An analytical assessment of extended Hamming product code with DCEP performance has been analysed, as well as a comprehensive collection of methods for dealing with all conceivable scenarios, including conventional, shorter, and punctured scheme implementations have been reviewed. These codes are often used in low-error wireless applications. Designers and researchers may now assess code performance without having to resort to time-consuming and, in many cases, impractical simulations. The proposed system is an improvement of the traditional hamming code method and the drawback which was surpassed is the single-bit error correction. This proposed system can be further improvised to detect and correct more than one-bit errors. Furthermore, due to its role as a starting point for continually pushing the limits of both space and technology, this will be important in the future in the field of nanosatellite research which is developing and expanding at a dizzying rate besides the fact that the memory chip cell design is becoming denser due to the advancement in nanotechnology.

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

References

[1] Shakya, Subarana. "An efficient security framework for data migration in a cloud computing environment." Journal of Artificial Intelligence 1, no. 01 (2019): 45-53.

[2] T. Fujiwara et al., "Error Detecting Capabilities of the Shortened Hamming Codes Adopted for Error Detection in IEEE Standard 802.3," IEEE Trans. Communications, vol. 37, no. 9, pp. 986-989, Sep 1989.

[3] Manoharan, J. Samuel. "A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits." Journal of Innovative Image Processing (JIIP) 3, no. 01 (2021): 36-51.

[4] D. De Villiers and R. Van Zyl, ZACube-2 : the Successor to Africa's First Nanosatellite, French South African, Institute of Technology, Bellville, South Africa, 2018.

[5] Sathesh, A. "Enhanced soft computing approaches for intrusion detection schemes in social media networks." Journal of Soft Computing Paradigm (JSCP) 1, no. 02 (2019): 69-79.

[6] W. Xiong, and D. W. Matolak, "Performance of Hamming Codes in Systems Employing Different Code Symbol Energies," IEEE Communications Society, pp. 1055-1058 [Wireless and Communications and Networking Conference (WCNC)].

[7] Manoharan, Samuel. "An improved safety algorithm for artificial intelligence enabled processors in self driving cars." Journal of Artificial Intelligence 1, no. 02 (2019): 95-104.

[8] Wyner, "Recent results in the Shannon theory", IEEE Trans. Inf. Theory, vol. 20, pp. 2-10, 1974.

[9] Mugunthan, S. R. "Soft computing based autonomous low rate DDOS attack detection and security for cloud computing." J. Soft Comput. Paradig.(JSCP) 1, no. 02 (2019): 80-90.

[10] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): design and construction", Proc. DCC, pp. 158-167

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

[11] Smys, S., and Haoxiang Wang. "Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework." Journal of Artificial Intelligence 3, no. 02 (2021): 90-100.

[12] V. Stankovic, A. D. Liveris, Z. Xiong and C. N. Georghiades, "On code design for the Slepian-Wolf problem and lossless multiterminal networks", IEEE Trans. Inf. Theory, vol. 52, no.4, pp. 1495-1507, 2006

[13] Sharma, Rajesh, and Akey Sungheetha. "An Efficient Dimension Reduction based Fusion of CNN and SVM Model for Detection of Abnormal Incident in Video Surveillance." Journal of Soft Computing Paradigm (JSCP) 3, no. 02 (2021): 55-69.

[14] S. Pradhan and K. Ramchandran, "Generalized coset codes for distributed binning", IEEE Trans. Inf. Theory, vol. 51, no.10, pp. 3457-3474, 2005.

[15] Haoxiang, Wang, and Smys Smys. "Soft Computing Strategies for Optimized Route Selection in Wireless Sensor Network." Journal of Soft Computing Paradigm (JSCP) 2, no. 01 (2020): 1-12.

[16] Satyanarayan NV, Sujatha NL, Ramaraju JSS. Detecting and Correcting Multiple Upsets with 64-bit Decimal Matrix Code in Memories, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (IJAREEIE). 2014; 3(8):11496–504.

[17] B. Umashankar. "Improved Hamming Code for Error Detection and Correction", 2007 2nd International Symposium on Wireless Pervasive Computing, 02/2007.

[18] Suma, V. "Community Based Network Reconstruction for an Evolutionary Algorithm Framework." Journal of Artificial Intelligence 3, no. 01 (2021): 53-61.

[19] Baek S-S, Won Y-S, Han D-G, Ryou J-C. The Effect of Eight-Shuffling AES Implementations Techniques against Side Channel Analysis. 2015 Mar; 8(5):91–7.

[20] Shakya, Subarna, and Lalitpur Nepal Pulchowk. "Intelligent and adaptive multi-objective optimization in WANET using bio inspired algorithms." J Soft Comput Paradigm (JSCP) 2, no. 01 (2020): 13-23.

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

[21] Vignesh B. Pipelined Quadratic Equation Based Novel Multiplication Method for Cyptographic applications. 2014; 7(4):34–9.

[22] Jacob, I. Jeena, and P. Ebby Darney. "Artificial Bee Colony Optimization Algorithm for Enhancing Routing in Wireless Networks." Journal of Artificial Intelligence 3, no. 01 (2021): 62-71.

[23] Nagalakshmi, Malathy, Tanya Sharma, and N. S. Kumar. "Flexible Language-Agnostic Framework To Emit Informative Compile-Time Error Messages." In Inventive Computation and Information Technologies, pp. 859-868. Springer, Singapore, 2021.

[24] Sanyal, Hrithik, and Rajneesh Agrawal. "Study of Holoportation: Using Network Errors for Improving Accuracy and Efficiency." In Proceedings of International Conference on Sustainable Expert Systems: ICSES 2020, vol. 176, p. 107. Springer Nature, 2021.

[25] Biswas, Abhishek, and Pushan Kumar Dutta. "Novel Approach of Automation to Risk Management: The Reduction in Human Errors." In International Conference on Mobile Computing and Sustainable Informatics, pp. 683-696. Springer, Cham, 2020.

[26] Sugi, S. Shinly Swarna, and S. Raja Ratna. "Survey on the Security Threats in IoT System." In International Conference on Mobile Computing and Sustainable Informatics, pp. 721-728. Springer, Cham, 2020.

[27] Prasanna, I. Philo, and M. Suguna. "Detection of Distributed Denial of Service Attack Using NSL-KDD Dataset-A Survey." In International conference on Computer Networks, Big data and IoT, pp. 866-875. Springer, Cham, 2019.

Author's biography

R. Asokan received his B.E degree in electronics and communication from Bharathiar University and MS degree in electronics and control from Birla Institute of Technology. He obtained an M.Tech degree in electronics and communication from Pondicherry Engineering College, with

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021

Journal of Information Technology and Digital World (2021)
Vol. 03/ No. 03
Pages: 179-192
https://www.irojournals.com/itdw/
DOI: https://doi.org/10.36548/jitdw.2021.3.003

distinction. He obtained PhD in information and communication engineering from Anna University, Chennai. He is currently the Principal, Kongunadu College of Engineering and Technology, Thottiyam, TamilNadu, India. He has published more than 65 papers in national and international journals and conferences. He has over 25 years of teaching experience. He is a member of various scientific and professional societies. His areas of interest include wireless networks, network security and image processing.

T. Vijayakumar is currently working as Professor in the Department of ECE at Jai Shriram Engineering College, Avinashipalayam, Tamil Nadu, India. His research includes Computer Vision, Motion Analysis, Stereo Vision, Object Recognition, computer graphics, photo interpretation, image retrieval, Embedded Image Processing and Real-time image and video processing applications.

ISSN: 2582-418X
Submitted: 13.08.2021
Revised: 28.09.2021
Accepted: 16.10.2021
Published: 27.10.2021