International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Hybrid Cryptographic Approach for Secure Communication

Dr. Gifty Arora[1], Deepali S. Hirolikar[2], Dr. Shailesh Shivaji Deore[3], Mr. K. K. Bajaj[4], Dr. Praveen Kumar Gupta[5], Dr. Uruj Jaleel[6], Vidya R.[7]

Submitted: 09/10/2023 **Revised**: 28/11/2023 **Accepted**: 08/12/2023

Abstract: This paper introduces a novel hybrid cryptographic system designed to enhance the security and integrity of Device-to-Device (D2D) communication in wireless networks. The system combines Huffman coding and binary encryption to secure data transmission over open public channels. Huffman coding provides efficient block encryption, while binary encryption offers robust key management. The proposed algorithm is tested using Java programming, demonstrating its efficiency in maintaining the integrity of various data types with zero Root Mean Square Error (RMSE) in decryption. The research highlights the importance of secure communication in the modern digital age and offers a solution that addresses the key drawbacks of current communication methods, such as complex network design and high power requirements.

***Keywords**: Hybrid Cryptographic System, Device-to-Device (D2D) Communication, Huffman Coding, Binary Encryption, Wireless Network Security, Data Transmission Integrity, Public Channel Encryption, Root Mean Square Error (RMSE).*

1. Introduction

The key infrastructure for low-cost, high-speed data transmission in the modern digital age is wireless, and various cutting-edge technologies are continually developing to guarantee that wireless is the dominant communication route. It is obvious that a widespread infrastructure is required to provide an efficient communication route that can transport a sizable volume of data between two authorised persons [1]. The need for a certain mode of communication changes considerably when new technologies emerge. There are several advantages to using smaller packets, including as increased transmission range, faster data transfer rates, and more reliable and secure communication [2]. Complex network design and high power need for processing and transmitting data packets are key drawbacks of current communication methods.

Thus to effective address the above difficulties of the present wireless networks, a unique open-public channel is necessary that gives considerably high number of viable pathways and energy at each node but needs minimal energy for transmission. Since, device-to-device (D2D) communication is independent of current wireless network design but can function in tandem with the systemhas lately emerged as a potential technology that may considerably increase the performance of existing wireless networks [1]. Using the public channel instead of the licenced band was the original concept behind integrating D2D communication with the current infrastructure.Since D2D communication relies on already-existing neighborhood-user equipment, operators anticipate it will provide high data rates despite its short operating distance compared to the current communication infrastructure's long one [2]. Therefore, a lot of effort is being put into studying how to make D2D communication better in every way to guarantee its complete growth.This method of communicating is convenient because of its easy design, fast data transfer speeds, and exact transmission with approved users. Unfortunately, the security of information being communicated plays an essential part in the viability of D2D communication systems, since the means of communication is centred on the maximisation of public nodes rather than private nodes, and also the number of nodes would be expanded substantially. Despite being superior to current systems in terms of energy efficiency, infrastructure security/safety, packet loss, and throughput [3]. As the number of people who own and use smart devices (phones, tablets, etc.) continues to expand, so

[1]Assistant Professor, lovely Professional University, Phagwara, aroragifty797@gmail.com
[2]PDEA'S College of Engineering Manjari Bk, Pune
Email : hirolikar.ds@gmail.com
[3]Associate Professor Department of Computer Engineering, SSVPS B S DEORE College of Engineering,Dhule, Maharashtra
shaileshdeore@gmail.com
[4]RNB Global University
Place - Bikaner
Email - vc.bajaj@rnbglobal.edu.in
[5]Professor Department of Computer Science & Engineering, Alliance College of Engineering & Design,
Alliance University, Central Campus Bengaluru
Karnataka, India
Onlinepg@gmail.com
[6]Associate Professor Department of Computer Science & Engineering, Alliance College of Engineering & Design
Alliance University, Central Campus Bengaluru
Karnataka, India
dr_urujjaleel@yahoo.com
[7]Former Asst. Professor in ComputerScience
Institution name: Gokulam S.N.G.M Arts and Science College, Alappuzha
Email ID: vidhubsc@gmail.com

does the likelihood that a communication route that takes use of optimum energy, has a high data rate, and provides excellent coverage.

As a result, ensuring the viability of the D2D communication channel is dependent on the provision of an effective data security and integrity methodology. In this research, we examine how to maximise the use of available spectral bandwidth while yet ensuring the privacy of data during transmission via open D2D networks. The primary goal of this study was to design and develop a novel, innovative framework that takes advantage of a number of factors to improve packetstransfer rate and provide reliable, robust D2D communication within the constraints of existing networks. Despite the fact that multiple methods for improved D2D communication have been offered, it has become a subject of study with applications in a wide range of disciplines. Unfortunately, as research activity increased, much of the effort went into protecting the physical layer, rather than the D2D communications channel. The sheer high expense and complexity of device use make it hard to create and commercialise smart devices with a secure physical layer [1]. This has spurred the development of a new field of study focused on designing a framework to protect the channel (i.e., the method of communication) rather than the device itself.

Cryptography

Cryptography, or "secret writing," is the practise of making information unintelligible to an observer who has not been given the decryption key. Information may be encrypted digitally, and the authenticity of those with access can be verified. Within the realm of information security and assurance, it has become a highly concentrated topic of study [4].A lot of people are interested in cryptography these days because of how much data is being sent across public channels like D2D communication and how quickly it's growing. We focus attention on crypto technologies that may safeguard data integrity during transmission or provide secure connection via unencrypted routes. One of the fundamental notions of every crypto system is shown in Figure 1 and elaborated upon below [5].

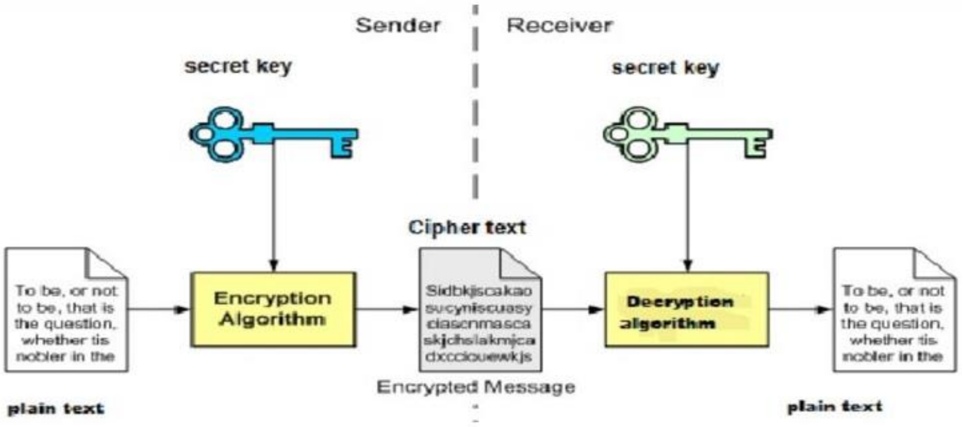

Sender
Receiver
secret key
secret key
Cipher text
To be, or not to be, that is the question, whether tis nobler in the
Encryption Algorithm
Sidbkjiscakao sucyniscuasy clascnmasca skjchslakmjca dxccicuewkjs
Decryption algorithm
To be, or not to be, that is the question, whether tis nobler in the
Encrypted Message
plain text
plain text

Fig 1. Model for a Cryptographic System in General

DataManipulation: This framework modifies the original information based on a transform / code or look-up tableinto appropriate crypto information. Because their inversion is so easy, these methods are widely used. It was possible to reassemble the data with little to no change from the original.

Permuting the order in which bits of data are stored in response to a transform, code, or lookup table yields cryptographic hashes of the original data, as proposed by this approach. The recovered data was identical to the original in every respect. By using inverse permutation on encrypted data, the original information may be reconstructed.

It is common knowledge that each of the aforementioned methods has both benefits and drawbacks. Currently major effort is focused in integrating both the methodologies to develop a hybrid model as stated in this work.

D2D communication between two or more public devices is made secure by the proposed technique's usage of Huffman coding and the Binary algorithm. While the Binary safely codesthe key management benefits, the Huffman method provides superior efficiency in block encryption. Therefore, the data transfer is safe due to the twofold protection. The remainder of the study is organised as follows: Section 2 provides historical context about several current hybrid algorithms. Huffman and binary coding are presented in Section 3 for the first time. In Section 4, we discuss the suggested method, and in Section 5, we show how it was tested and analysed using simulation. In Section 6, the report's final conclusion is laid forth.

2. Background

Because of these fast improvements in network technology and signal processing, there is a broad variety of situations that call for the use of secure communication channels. The term "safety" most often refers to a location that is free from dangers presented by individuals or groups with the intention of causing damage. The majority of today's technologically advanced communication systems have, as their main objective, the prevention of the unlawful destruction of physical assets and data [6]. In this article, our primary attention is on the sequences of physical (mainly shared) equipment that guarantee the safety of data flow between allowed individuals.

Nesterenko, A. Y. E., et al. [7] came up with the idea for a novel amalgamation encryption method that is based on the ElGamal asymmetric encryption system and uses secret keys that are disseminated across the network. The keys were used to protect the encrypted communications from being accessed by unauthorised parties. The solution to the issue is modelled after a discrete logarithm in the plan, which also includes the security that is based on an elliptic curve. Even if the most fundamental level of communication is not represented by a dot or curved ellipse, the system is nevertheless capable of encoding a significant quantity of data, which is its defining characteristic. In the actual world, the cryptographic characteristics of the system were evaluated and tested. The post-quantum world is taken into consideration in the cryptographic approach that was proposed by E. Persichetti [8]. The fusional concept of the algorithm takes use of the Niederreiter formation, which provides a stochastic model focusing on the safety approach of the IND-CCA.

Shen, W., et al. [9] have come up with a novel idea for a key exchange that is both secure and resilient. Their concept makes it possible for any two intelligent communicative devices to start a D2D communication without having prior public hidden key information. They came up with this idea by researching the various factors and constraints of the protocols that are currently being used in the D2D communications channel.The design of this protocol was influenced by the Diffie-Hellman key exchange protocol as well as the assurance architecture. The suggested method was built on devices that are based on Android, and its resiliency as well as the effective execution of the protocol have been shown via simulations that make use of the Wi-Fi communication channel.

Proximity Services and transmission phases were the primary areas of attention for Abd-Elrahman, E. and colleagues' [10] examination of the safety of direct-to-device (D2D) communications. Group Key Management (GKM) was established by the authors to surreptitiously swap messages throughout the D2D processing, transmission, and receiving phases of the communication system. It was built with the current restrictions and needs in mind throughout the development process. Analyses, simulations, and comparisons were performed on the suggested technique with state-of-the-art approaches that emphasise localised communication such D2D (also known as spontaneous communication) [11]. In addition, the findings of the simulations indicate that the concept of Cluster Key Administration, also known as CKA, is an efficient key administration framework for Device-to-Device, or D2D, communication. An amalgamated encryption method that combines AES and RSA was described by Rege, K., et al. [12] as a way to enhance the safety of data that is being sent via Bluetooth between two or more devices that are being used in conjunction with one another.

Lu, X., et al. [13] show that Tag-DEM (i.e., Tag Data Encapsulation Mechanism) that protects the authentic cryptotext from the prior stage is resistant to key associated attacks if the cryptotext is protected with KEM (i.e., Key Encapsulation Mechanism) and provides key adaptability and verification. Tag-DEM protects the authentic cryptotext by encapsulating it in a tag that can be used to verify its authenticity. The findings of the simulations indicate that the suggested merged encryption system is safe and able to withstand RKA attacks. In order to provide more evidence that they satisfy these two requirements, simulations of previously developed KEM techniques were also carried out.

Kwon, H. [14] suggested a novel D2D authentication method that integrates a hidden key establishment phase. This method uses cryptogram-guideline characteristic-based encryption (CP-ABE), which was developed by Kwon. This strategy makes use of CP-ABE to provide a consensus protocol and information sharing across nodes in a multi-hop network (which is analogous to communication from device to device). Additionally, a number of additional modifications of the protocols were developed in order to address certain use cases inside multi-hop networks that did not have any underlying network support. Simulation findings reveal that the plan has a logical processing cost in D2D cellular multi-hop networks, but it is safe against MITM and replay attacks.

3. Coding Techniques

Huffman coding: Entropy-based coding techniques are often employed to compress data without compromising quality. This approach employs the occurrence frequency as a guide in the development of a lookup table with keys of varied lengths to encode the original data. The effectiveness of the coding relies heavily on the lookup-table obtained from the original data, which is constructed based on the frequency of occurrence for each possible value. Figure 2(a) and Figure 2(b) depict the Huffman encoding and decoding procedures, respectively.

Huffman coding makes use of a general approach for picking each probable value and then constructing a prefix code that can grasp all the values in the original data. The coding starts with a shorter prefix code used for more regularly occurring values, and the coding string rises as the frequency of the value declines [15]. This approach devised a coding system in which no two things may have the same prefix code based on the lookup table, hence increasing efficiency. The code may be deciphered [16-17] when the true value frequencies are recognised using the prefix-codes in the look-up table. The original data was far larger, and this one is significantly smaller.

To create a prefix code that can understand all the values in the original data, Huffman coding uses a generic strategy for selecting each likely value. The prefix code is shorter for more often occurring values, and the string length increases with decreasing frequency [15]. In order to maximise productivity, this method came up with a coding scheme in which no two items may share the same prefix code derived from the lookup database. When the real value frequencies are detected using the prefix-codes in the look-up table, the code may be cracked [16-17]. The size of the original data set was much bigger than this one.

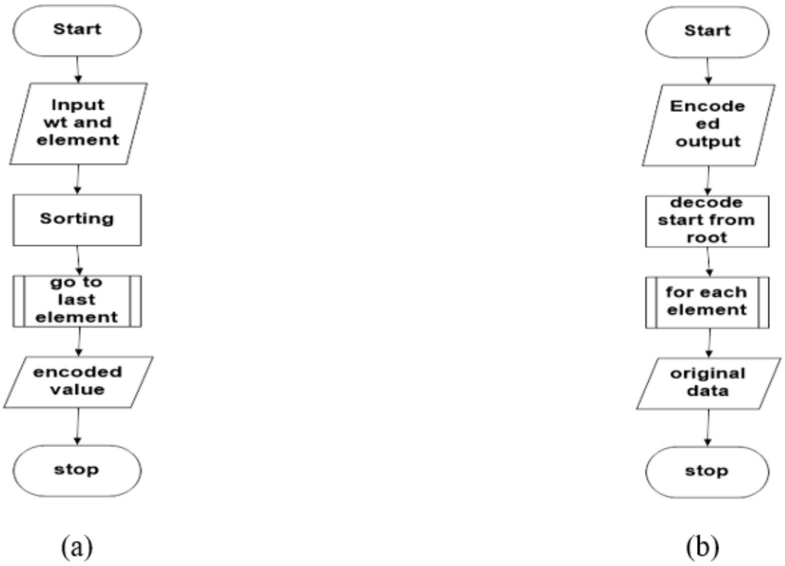


Fig 2. (a) Huffman Encoding (b) Process Flow Diagram Huffman Decoding Flow Diagram

Encoding in Binary: When it pertains to encoding information in binary, one efficient technique is to utilise a fusion of a confidential key and a communal key. This technique, recognised as asymmetric encryption, enables the safe encoding and decoding of confidential data. By employing binary encryption methods, the information can be converted into a structure that is not readily understandable by unauthorised individuals. This procedure entails the utilisation of a secret key, which is maintained in secrecy and recognised solely by the intended receiver, and a communal key, which is openly accessible to everyone. By employing these keys, the safeguarded information can be safely encrypted and subsequently decrypted when needed. This dual encryption method provides an additional stratum of security, guaranteeing that the data remains protected from potential hazards or unauthorised entry. One facet that can be observed when scrutinising the system is its innate intricacy, which is further demonstrated by the gradual decrease in its comprehensibility. As one explores further into the complexities of the system, it becomes progressively evident that its framework and elements are intricately interconnected, resulting in a tangled and elaborate network of interconnections. This elaborate nature of the system presents a noteworthy obstacle when trying to grasp and interpret its diverse components and operations. Accordingly, the comprehensibility of the system decreases as one navigates. The procedure stream diagrams for encoding and decoding binary information are visually portrayed in Figure 3(a) and 3(b), correspondingly. These illustrations offer a lucid and succinct synopsis of the stages implicated in both the encoding and decoding procedures. By scrutinising Figure 3(a), an individual can acquire a more profound comprehension of how binary information is altered and encoded into a particular structure. Likewise, Figure 3(b) demonstrates the inverse procedure of deciphering binary information into its authentic configuration. These illustrations function as precious visual tools in understanding the complex procedures of encoding and deciphering binary information.Utilising a confidential key and a communal key, akin to an asymmetric encryption method, binary encryption can be employed to cypher and decipher the safeguarded information. The intricacy of the system is mirrored in its diminishing legibility. The procedure stream charts for encrypting and deciphering binary information are displayed in Figure 3(a) and 3(b), correspondingly.

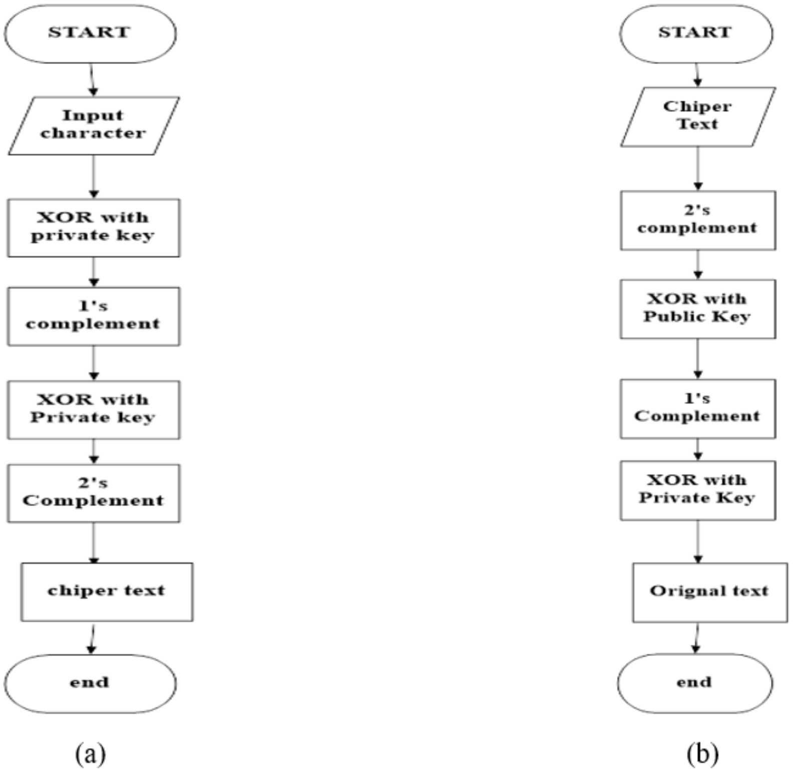


Fig 3. (a) The Flow Chart of Binary Encoding (b) The Flow Chart of Binary Decoding

PROPOSED ALGORITHM

The primary emphasis of this Section was to create and establish a groundbreaking original structure that utilises diverse elements to offer dependable and resilient D2D communication founded on the current network limitations and enhance data transfer speed while reducing the burden on the prevailing communication infrastructure. The fundamental process for encoding and decoding the digital data using suggested algorithm is illustrated in Figure 4 and Figure 5 correspondingly. Furthermore, the methodology produces a binary cypher utilising the specific designated input variables.

HYBRID ENCRYPTION ALGORITHM

Step: 1 Enter the input data.

Step: 2 Input data goes to binary mode.

Step: 3 In binary first is xor private key.

Step: 4 find the 2’s complement.

Step: 5 find the 1’s complement.

Step: 6 find the xor with public key .

Step: 7 chipper text .

Step: 8 Now applying Huffman on chipper text.

Step: 9 Read character from database

Step: 10 Replace the character match in data base.

Step: 11 Save that in file.

Step: 12 chipper text got.

HYBRID DECRYPTION ALGORITHM

Step: 1 input the chipper text.

Step: 2 search the encode from database.

Step: 3 match the code and paste in place of that character and put required character.

Step: 4 find the xor with public key.

Step: 5 find the 1’s complement.

Step: 6 find the 2’s complement.

Step: 7 find the xor with private key.

Step: 8 Original texts found.

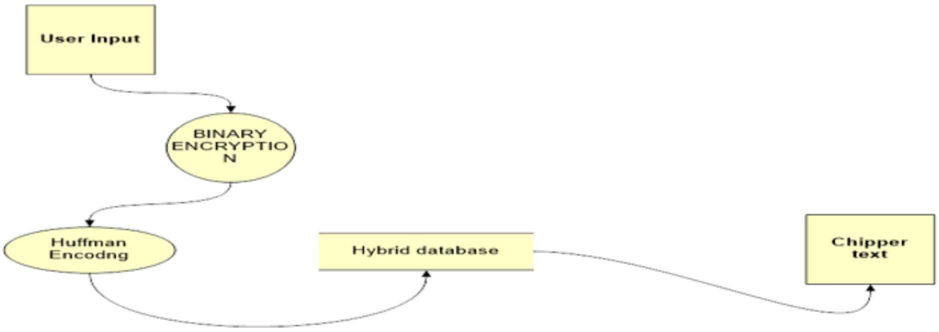


Fig 4. Encoding Process of the Hybrid Cryptographic System

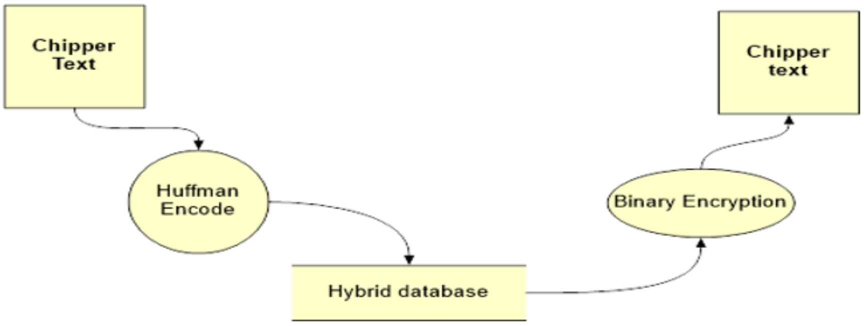


Fig 5. Decoding Process of the Hybrid Cryptographic System

4. Simulation and Results

In this portion, we explore the captivating realm of the proposed Composite encryption system. We commence on a voyage of discovery, scrutinise its complexities and reveal its possibilities. Through arduous experiments and scrupulous examination, we are disclosing the results of this groundbreaking encryption mechanism. Come and join us as we unravel the enigmas and potentials that reside within the domain of Composite encryption. The simulations are duplicated using a JAVA programming-based development environment. This permits for the precise replication of the simulations, guaranteeing that the outcomes acquired are dependable and uniform. By employing the potency and adaptability of JAVA, the simulations are capable of being executed with accuracy and effectiveness. The JAVA programming language offers a resilient platform for developing and executing the simulations, enabling a smooth and uninterrupted experience for the users. Overall, the utilisation of a JAVA coding-oriented development platform is pivotal in effectively replicating. The assessment and investigation process follows a methodical approach, where diverse written data of varying scales and types of traits are meticulously examined. This consecutive style permits for a comprehensive inquiry, guaranteeing that every fragment of data is meticulously scrutinised and verified. By arranging the assessment and exploration in this fashion, I attain a thorough comprehension of the topic, as it encompasses a broad array of written information. This systematic approach ensures that no facet is disregarded, and that all pertinent data is considered. The proposed algorithm undergoes a comprehensive evaluation to gauge its resilience.

Phase-1 Class Diagram

In object-oriented modelling, the class diagram is the fundamental element. As the diagram represents the processes as code, it is used for both conceptual and detailed modelling of the application. Additionally, they might be put to good use in applications dependent on conceptual data modelling. Figure 6 depicts the class-diagram implementation of the link between the hybrid encryption algorithm's suggested properties and operations. Classes in a class diagram are representations of the application's primary objects, interactions, and target classes.

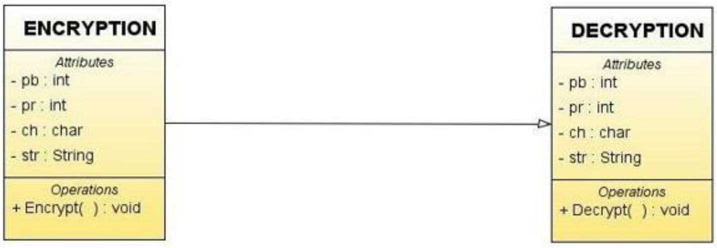


Fig 6. Class Diagram of the Hybrid Encryption Algorithm

Phase 2 Snap Shots

In this stage, the simulation's outcomes are shown in the form of still images. An authorised user's name and password are shown in Figure 7 as the first phase in the simulation process, which is necessary for encoding and decoding the information using the suggested technique. Figure 8 depicts the subsequent simulation process, which involves choosing between the encoding and decoding phases. The last phase, shown in Figure 9 and Figure 10, involves implementing the suggested hybrid cryptographic method for encoding or decoding.

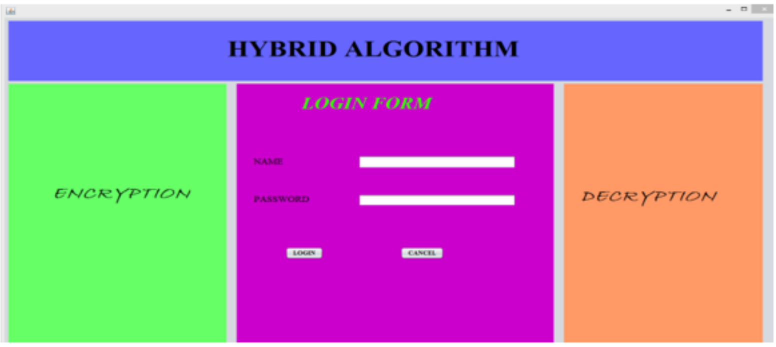


Fig 7. GUI of Hybrid Cryptographic System

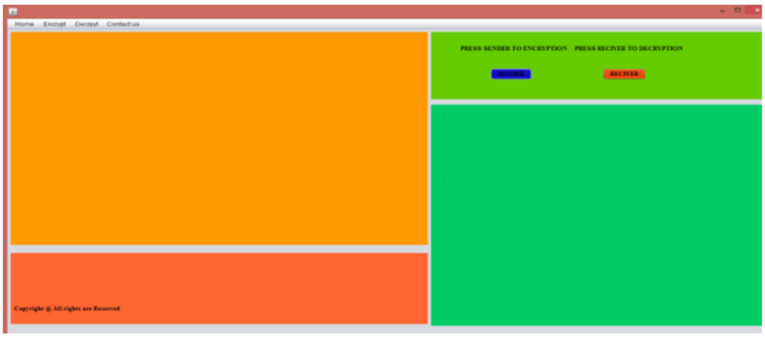
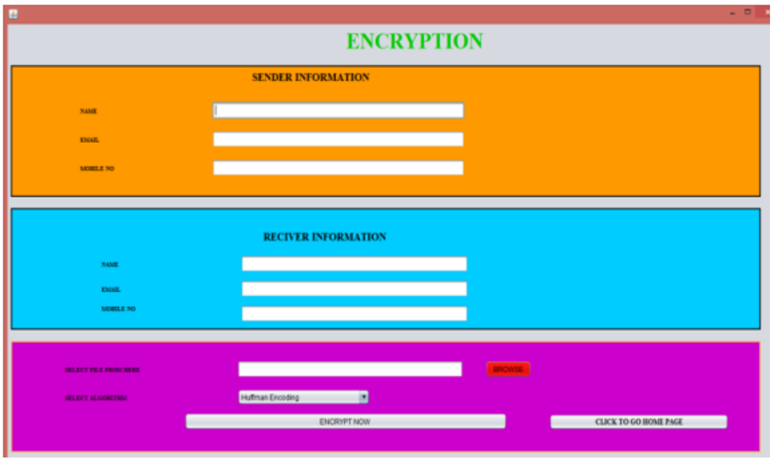
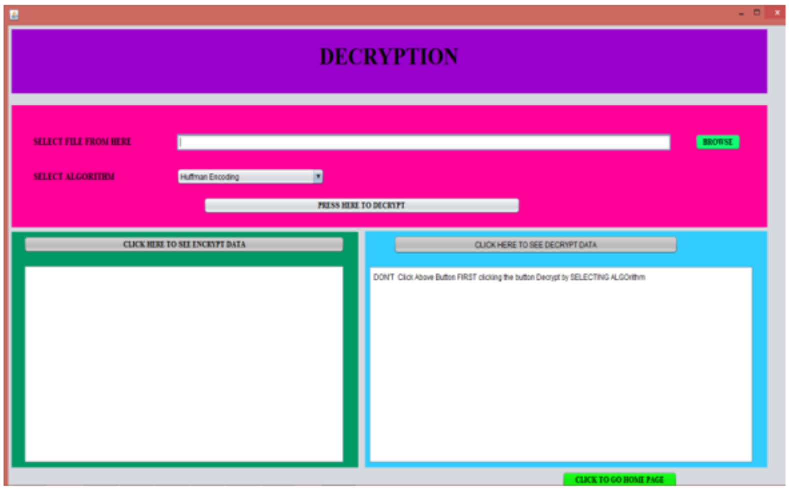

Home
Encrypt
Decrpyt
Contact us
PRESS SENDER TO ENCRYPTION
PRESS RECIVER TO DECRYPTION
SENDER
RECIVER
Copyright @ All rights are Reserved

Fig 8. Basic GUI of Selection of Sender and Receiver Algorithm



SELECT ALGORITHM: Huffman Encoding

Fig 9. GUI of Encoding Process for Hybrid Cryptographic System



SELECT ALGORITHM: Huffman Encoding

DONT Click Above Button FIRST clicking the button Decrypt by SELECTING ALGOrithm

Fig 10. GUI of Decoding Process for Hybrid Cryptographic System

Phase 3 Numerical analysis

Table 1 presents the comparative study of the proposed approach with well-known RMSE algorithm for information containing: just letters, only integers or both.

Table 1. Comparison of RMSE of the Color Images between Binary Coding and Proposed Hybrid Algorithm

File Size	RMSE Encrypt			RMSE Decrypt			Binary Encrypt
	Numbers	Char	Both	Numbers	Char	Both	
2KB	11.7150	11.2900	10.7950	0	0	0	9.7709
5KB	12.0010	11.4710	11.1560	0	0	0	10.1848
10KB	11.6590	11.4720	11.2560	0	0	0	9.6624
20KB	13.2430	13.4360	13.2440	0	0	0	10.1311
36KB	13.4140	13.7040	13.5670	0	0	0	10.3210
50KB	12.5470	12.5590	12.2390	0	0	0	8.6801

In the realm of secure digital communication, particularly when evaluating encryption algorithms, the Root Mean Square Error (RMSE) serves as a crucial metric for assessing the integrity of data post-encryption and decryption. In "Table 1," we see a comprehensive comparison of RMSE values for both encryption and decryption phases using Binary Coding and a Proposed Hybrid Algorithm, across various file sizes ranging from 2KB to 50KB. The data is categorized based on the type of content encrypted - numbers, characters, or a combination of both. Focusing on the encryption phase, the RMSE values for the Hybrid Algorithm show a consistent pattern across different file types and sizes. For instance, in a 2KB file, the RMSE values are 11.7150, 11.2900, and 10.7950 for numbers, characters, and both, respectively. This trend of RMSE values indicates the algorithm's consistent performance in encrypting different data types. As the file size increases, there's a noticeable increase in RMSE values, peaking at 13.4140, 13.7040, and 13.5670 for a 36KB file containing numbers, characters, and both, respectively. This suggests a proportional relationship between file size and RMSE, indicating how the complexity of the encryption process scales with the amount of data. The decryption phase, however, paints a different picture. Remarkably, the RMSE values for all file sizes and types are zero, signifying a flawless recovery of the original data post-decryption. This is a critical aspect of any cryptographic algorithm, as it underscores the ability to maintain data integrity and fidelity after the encryption-decryption cycle. On the other hand, the Binary Encrypt column provides a baseline comparison. For instance, a 2KB file shows an RMSE value of 9.7709, and this value increases with file size, reaching 8.6801 for a 50KB file. This ascending trend differs from the hybrid algorithm, suggesting variances in how each method handles data encryption scalability. In essence, the tabulated data offers insightful perspectives into the performance of the proposed hybrid cryptographic algorithm, particularly when contrasted with conventional binary encryption.

The zero RMSE values in decryption across all scenarios underscore the hybrid algorithm's efficiency in preserving data integrity, a crucial factor for secure and reliable communication systems. At the same time, the varying RMSE values during the encryption phase reflect the algorithm's adaptability and responsiveness to different data types and sizes, an attribute vital for versatile applications in modern digital communication.

5. Conclusion

In this study, we introduced a novel Huffman-Binary hybrid cryptographic system that may strengthen data transmission security across a distributed-to-distributed (D2D) network. The suggested methods improved the performance of block encryption and covertkey agreement protocols by combining the Huffman algorithm with the Binary algorithm. Huffman coding and the Binary algorithm's many benefits mean that data sent via the D2D channel may now be transferred more stealthily. The experimental findings show that the suggested method is reliable, lossless, and capable of solving the traffic problems in the network. The suggested algorithm also demonstrates the viability of D2D communication both on its own and in tandem with the preexisting infrastructure-based communication system.

Also, when a media file is encrypted, it is converted to a binary format that is easily understood by the system and algorithms based on these binary numbers can encrypt and decrypt the file quickly. The suggested approach is also lossless, which means that the decrypted and original data are identical.

References

[1] F. C. Cheng and S. Tatesh. “Secure Device-to-Device (D2d) Communication,” U.S. Patent No. 20,150,326,537, 2015.

[2] L. Goratti, et al., “Connectivity and security in a D2D communication protocol for public safety applications,” in Wireless Communications Systems (ISWCS), 2014 11th International Symposium on, pp. 548-552, 2014.

[3] J. L. Massey, “Some applications of source coding in cryptography,” Euopean Transaction on Telecommunication, vol. 5, pp. 421–429, 1994.

[4] J. Knudsen, “Java Cryptography,” O’Reilly and Associates, Inc., 1998.

[5] H. Delfs and H. Knebl, “Introduction to Cryptography,” Springer, 2007.

[6] “Huffman coding and encryptions methods,” International Journal of Computer Science and Information Security, vol/issue: 8(9), pp. 195–199, 2010.

[7] A.Y. E. Nesterenko and A. V. E. Pugachev, “A new hybrid encryption scheme,” Prikladnaya Diskretnaya Matematika, vol. 4, pp. 56-71, 2015.

[8] E. Persichetti, “Secure and anonymous hybrid encryption from coding theory,” in Post-Quantum Cryptography, Springer Berlin Heidelberg, pp. 174-187, 2011.

[9] W. Shen, et al., “Secure key establishment for device-to-device communications,” in Global Communications Conference (GLOBECOM), 2014 IEEE, pp. 336-340, 2014.

[10] E. A. Elrahman, et al., “D2D group communications security,” in Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on, pp. 1-6, 2015.

[11] E. A. Elrahman, et al., “Fast group discovery and non-repudiation in D2D communications using IBE,” in Wireless Communications and Mobile Computing Conference (IWCMC), 2015 International, pp. 616-621, 2015.

[12] K. Rege, et al., “Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA,”

[13] International Journal of Computer Applications, vol/issue: 71(22), 2013.

[14] X. Lu, et al., “Related-key security for hybrid encryption. InInformation Security, Springer International Publishing, pp. 19-32, 2014.

[15] H. Kwon, et al., “Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks,” Multimedia Tools and Applications, pp. 1-15, 2016.

[16] R. L. Rivest, et al., “On breaking a huffman code,” in Proc. IEEE Transactions on Information Theory, vol/issue: 42(3), 1996.

[17] N. Lee, et al., “Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis,” Selected Areas in Communications, IEEE Journal on, vol/issue: 33(1), pp. 1-13, 2015.

[18] Y. Liu, et al., “Secure D2D communication in large-scale cognitive cellular networks with wireless power transfer,” in Communications (ICC), 2015 IEEE International Conference on, pp. 4309-4314, 2015.

[19] H. Kwon, et al., “Secure authentication using ciphertext policy attribute-based encryption in mobile multi-hop networks,” Multimedia Tools and

Applications, pp. 1-15, 2016.

[20] S. Nagaraj, et al., “A Bio-Crypto Protocol for Password Protection Using ECC,” Bulletin of Electrical Engineering and Informatics, vol/issue: 4(1), pp. 67-72, 2015.

[21] C. Meshram, “Discrete Logarithm and Integer Factorization using ID-based Encryption,” Bulletin of Electrical Engineering and Informatics, vol/issue: 4(2), pp. 160-168, 2015.

[22] T. N. Babu, et al., “Ortho Linear Feedback Shift Register Cryptographic System,” Journal of Telematics and Informatics, vol/issue: 3(2), 2015.