Journal of Image Processing and Intelligent Remote Sensing
ISSN 2815-0953
Vol: 02, No. 04, June-July 2022
http://journal.hmjournals.com/index.php/JIPIRS
DOI: https://doi.org/10.55529/jipirs.24.1.7

A Study and Analysis on Color Coded Cryptography on Textual Data

Ms. Ritu Bhatiya*

**Assistant Professor Vimal Tormal Poddar BCA College*

*Corresponding Email: *ritubhatiya6194@gmail.com*

Received: 03 March 2022 **Accepted:** 19 May 2022 **Published:** 02 June 2022

Abstract: In today's network and internet applications, security is the most important factor. The value of data transmitted over the internet grows in lockstep with the relevance of network and Internet applications. As a result, one of the most important solutions in security related applications is offering vital protection against data threats. In data security systems, block cypher symmetric key cryptography is widely utilised. The symmetric key encryption methods DES (Data Encryption Standard), TDES (Triple Data Encryption Standard), PRESENT and KLEIN are compared in this study. The algorithms produce state-of-the-art results in their respective areas, with attacks, key size and block size compared.

Keywords: Block Cipher, DES, Triple DES, Mono Alphabetic Cipher, Substitution Cipher.

1. INTRODUCTION

In today's networks, cryptographic techniques and procedures are used in a variety of applications.
The essential objective of cryptography is to accomplish network security prerequisites like verification, non-renouncement, and privacy. Present day cryptography is partitioned into two sorts: symmetric key, which involves a solitary key for both encryption and unscrambling, and uneven key, which utilizes two unmistakable keys exclusively for encryption. block codes and stream figures are two sorts of symmetric key encryption.

Asymmetric Encryption key: To solve the key distribution problem, use asymmetric key encryption cast-off. Two types of keys are used in asymmetric key encryption:
There are two types of keys: public and private. The public key is used for encryption and is recognised by everyone, but the private key is used for decryption and is only known by the user.

Symmetric Encryption Key: Symmetric key encryption is a term used to portray secret key calculations. This is used for encryption as well as unscrambling. The symmetric key calculation is safer than the unbalanced key calculation, which is almost impervious. The size of the pre-owned key decides the strength of a symmetric key. DES, AES (Advanced Encryption Standard), TDES and other symmetric key calculations are a couple of models.

Literature Review

Deepti Sehrawat et al. (2019) offered a comparative analysis of various lightweight block cyphers based on their advantages, disadvantages, and future scope, which is required for IoT purposes and can be applied to restricted devices. The findings could aid in the development of a 32-bit ultra-lightweight cypher security technique for IoT-based domains.

Shashidhara Vyakaranal et al. (2018) advocated that tradeoff performance be taken into account. When compared to other algorithms, the results reveal that the Blowfish algorithm takes less time to decode and encrypt files and has a higher throughput. DES is well-suited for security-based domains with low bandwidth requirements. AES is highly suited for performance-based applications such as mobile phones, as it uses the least amount of energy while providing maximum security.

Anusha R et al. (2018) proposed utilizing close to handle correspondence (NFC) to permit clients to do touchless methods with their cell phones. The incorporation of a calculation in NFC confounds things, and it could prompt encryption for troublesome cryptographic strategies, which is great for security however not for future applications that need streaming information.

Achmad Solichin et al. (2017) depicted how to utilize the DES calculation and the discrete cosine change (DCT) approach with steganography to make advanced information security. Because of steganography with a worth of 46.9db, this kind of use is utilized to safeguard information records like word, pdf, succeed, and PowerPoint design, and the highlights of picture that has been embedded in the information documents are still in best quality.

Salah A. k. Albermany et al. (2017) introduced the RBC algorithm, a new random block cypher secret key with a 128-bit key length and a 64-bit block length that is suited for wireless networks, as an applicant for response automata direct graph (RADG). The RBC method generates different cypher text for the same plaintext, indicating that breaking down the code in a big system will be extremely difficult.

Tapan Kumar Hazra et al. (2017) described how to use the Blowfish algorithm and Diffie Hellman techniques to decrypt and encrypt text files and images. In this method, a computer user encrypts text files using a secret key generated by the blowfish algorithm, while Diffie Hellman generates a shared private key for two computer users. If the second user wants to decrypt the text files encrypted by the first user, he or she must first obtain permission from the first user. It can be decrypted using the Blowfish algorithm after gaining approval.

Shraphalya B. Nalawade et al. (2017) portrayed FPGA execution of Blowfish block figure calculation on reconfigurable stage to assess the presentation of throughput and power utilization, which can be utilized for constant applications like Audio, Video, ECG and other sensor applications.

Saptarshi Mitra et al. (2017) demonstrated the use of Triple DES to secure electronic transactions such as debit/credit, net banking, and mobile banking, and compared the results to other commonly used algorithms, demonstrating that while TDES is slower than DES in terms of encryption time, it is much more secure.

Jasvir Kaur et al. (2017) suggested a wireless sensor network that can be utilised for medical monitoring, industrial control, military surveillance, and environmental monitoring, among other things. Tempering, Blackmail attack, and Blackhole wormhole assault are some of the types of attacks addressed in wsn. To counteract this attack, different block cyphers are compared based on block size, key size, and rounds/cycles. They require little complexity and great throughput, according to the comparison.

Deepthi et al. (2016) proposed that other block cyphers such as Blowfish and MD5 be presented. They are compared on a number of factors, including fuse utilisation and CPU fuse usage. Finally, when compared to the Blowfish algorithm, the MD5 algorithm is described as an excellent algorithm. If the Blowfish algorithm is used in hardware, it is the best option.

Salah A.K. Albermany et al. (2016) compiled a summary of symmetric key block cyphers for a variety of algorithms. Feistel network is classified according to cryptographic categories such as DES, Towfish, and Blowfish. CLEFIA, MACGUFFIN, and HIGHT are members of the Feistel network's generalised unbalanced category (GUFN). In substitution-permutation networks, AES, ARIA, and AEGIS are classified.

Karima Dichou et al. (2015) Finding and comparing FPGAs (Field Programmable Gate Arrays) that are most suitable for DES algorithms, proposing papers for protecting smart cards and perpetuating hardware under limited conditions such as performance and area. We have selected the best FPGA for your DES implementation.

Poonam Jindal et al. (2015) provided a method for evaluating the symmetric key block cypher algorithm. With the help of DES, RC5, RC6,AES-128,Blowfish, Triple DES, and Towfish, the performance of the bock cypher was supported in terms of avalanche effect, encryption time, throughput, power consumption, and CPU time, indicating that there is a compromise between network performance and security. In comparison to other algorithms, the conclusion demonstrates that triple DES is the most secure algorithm to date, and AES is the second most safe method.

Hassan Noura et al. (2015) developed a dynamic structure arrangement of Nonlinear function and Artificial Neutral Network. The design of block cyphers has three layers: input layer, hidden layer, and output layer. It contains a number of nonlinear functions as well as dynamic invertible matrices. The number of hidden layers can be increased to improve the security function. The artificial neutral network's dynamic topology prevents parallel network and attack operations, resulting in lower energy consumption and lower computational complexity.

Monika Agarwal et al. (2014) proposed an analysis of symmetric encryption techniques such as DES, Blowfish, Triple DES, and AES based on their limitations and advantages over one another, and the results show that Blowfish algorithm is superior to Triple DES and DES, and also provides a high level of security when encrypting plaintext of 64 bits.

Prabhat Kumar Kushwaha et al. (2014) Suggested to compare symmetric block ciphers: PRESENT, TWINE, Puffin, KLEIN, KATAN, LED, LBlock, EPCBC, PRINT, and RECTANGLE. We highlighted the area, throughput, and cycle-to-cycle parameters of various algorithms that can be further implemented for lightweight block public key crypto system.

Jun Peng and colleagues (2014) proposed The Fiestal network, a 256-bit symmetric block cypher, is proposed as a chaotic system with a Fiestal network structure. As a result, the searchable key gap will be 2256 characters long. Finally, the result shows that the suggested block cipher's security function has the qualities of confusion and diffusion. This chaotic function characteristic will increase the plain text's unpredictability function.

Using DES and Amplitude Modulation approaches, Kushal S. Patel (2013) developed a study based on picture encryption to be secure during transmission against any form of assault. This technique generates a key depending on the image's pixel value. The value of this key is hidden from unauthorised third parties, and the value of key calculation varies per each block.
Sirwan A. Mohammed et al. (2013) proposed to involve Fuzzy rationale in MATLAB to portray the security execution of square codes utilized in remote organizations utilizing DES, RC5, and Blowfish calculations in light of the quantity of rounds, key length, and square length, and afterward analyze the security levels of Blowfish-86.9%, RC5-8.7%, and DES 48%.Using the DES cryptographic algorithm engine.

William C. Barker et al. (2012) described the Triple DES algorithm. It has a 64-bit key length and a 64-bit block size. Permutation, key dependent calculation, and initial opposite permutation are some of the operations performed by the DES engine. The DES cryptography engine works in both reverse and forward directions. Triple DES uses a key bundle to secure a large number of blocks.

Harshali D. Zodpe et al. (2012) proposed using exhaustive keys based on loop unrolling and iterative architecture to create Field Programmable Gate Arrays for the DES algorithm. In comparison to loop unrolled architecture, iterative architecture identifies the total space in a short time and requires a minimal area.

Multiple Recursive Generator (MRG) was proposed by Alina Olteanu et al. (2011) to generate pseudo random orders. The mrg created a block cypher that satisfies important requirements such as lengthy duration, security, unpredictability, and efficiency. This requirement is compared using a linear congruential generator (LPG), which is valuable in wireless sensor networks and RFID tags where power consumption, storage space, and memory are important.
Gaoli Wang et al. (2010) investigated the strength of the current approach in comparison to dfa. This method can recover 51 bits of related round keys with a sufficient number of samples, and an additional 29 bits can be generated through thorough search and computation. The attack can retrieve the computation complexity prices of the 229 and 64 pairs of faulty and perfect ciphers.

Proposed Algorithm:
The AES algorithm with its symmetric key is employed in cryptography, and the encrypted text is turned into two extra keys for great security, after which colour, blocks are added to the text. To hide the text, the technique is built with three steps.

Steps for Algorithms:
(a) Enter Plain Text
(b) Apply Substitution Cipher and Monoalphabetic Cipher
(c) Convert Cipher Text in to Colour Blocks.
(d) Image Generation

- **Substitution:** Using modified Caesar cipher

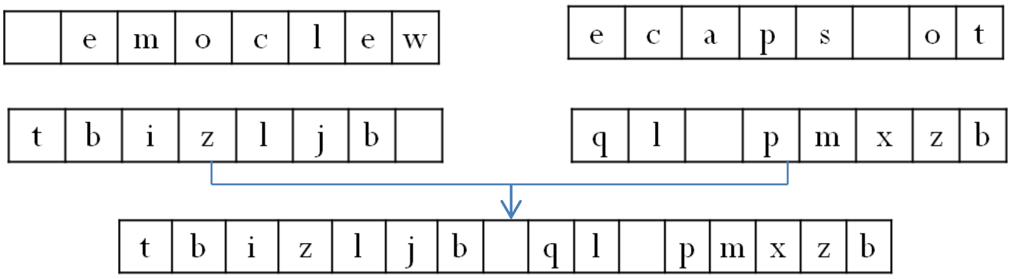

Fig 1.1 Modified Cipher

- **Transposition:**

t	b
i	z
l	j
b	
q	l
	p
m	x
z	b

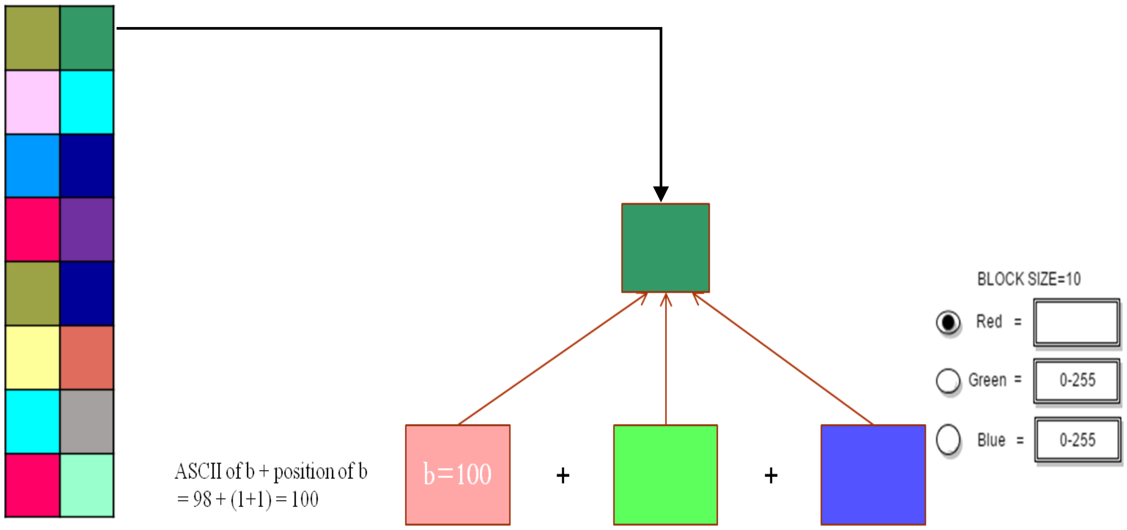

Fig 1.2 Apply color blocks to each text using ASCII code.

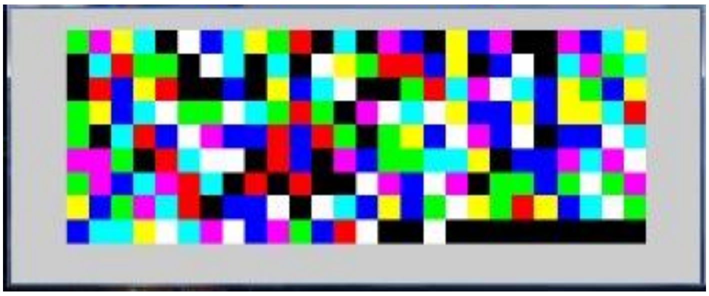

Fig 1.3 Proposed Model Visualization

2. CONCLUSION

In this research proposal the major focus is on tokenization of text and encryption and decryption through colors. The combination of matrices from the mathematics and cryptography may help to create the secure and useful application for small organization.
As per study I have identified that in DES, AES, RSA algorithms there are total 64 rounds, 128 round, 256 rounds applied on any text for encryption. If text size is small then this methods are became time consuming unnecessarily. So to overcome this issue, we can apply information security by color substitution method. This experiment demonstrates the technique's potential by removing important attacks such as brute force, man in the middle known plain text and known cipher text assaults.

3. REFERENCES

1. Douglas R. Stinson, Chapman and Hall/CRC," Cryptography: theory and practice," third edition (Discrete Mathematics and Its Applications),2005
2. Hans Delfs & Helmut Knebl, "Symmetric-Key Encryption", Springer Berlin Heidelberg, Introduction to Cryptography, Information Security and Cryptography, pp. 11-31, 2007.
3. Derrick Rountree, "Security for Microsoft Windows System Administration", 2011.
4. George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papaefstathiou, Charalampos Manifavas, "A Review of Lightweight Block Ciphers", Journal of cryptographic Engineering. April 2017.
5. Deepti Sehrawat, Nasib Singh Gill, Munisha Devi, "Comparative Analysis of Lightweight Block Ciphers in IoT-Enabled Smart Environment", 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN).
6. Shashidhara Vyakaranal ,Shivaraj Kengond, "Performance Analysis of Symmetric Key Cryptographic Algorithms", 2018 International Conference on Communication and Signal Processing (ICCSP).
7. Anusha R, Veena Devi Shastrimat V, "Qualitative Assessment on Effectiveness of Security Approaches towards Safeguarding NFC Devices & Services", International Journal of Electrical and Computer Engineering (IJECE) Vol. 8, No. 2, April 2018, pp. 1214~1221 ISSN: 2088 -8708.

8. Achmad Solichin, Erwin Wahyu Ramadhan, “Enhancing Data Security Using DES-based Cryptography and DCT-based Steganography”, 2017 3rd International Conference on Science in Information Technology (ICSITech).
9. Salah A. k. Albermany, Fatima Radi Hamade, Ghazanfar Ali Safdar, “New Random Block Cipher Algorithm”, 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani – Iraq.
10. Tapan Kumar Hazra,Anisha Mahato, Arghyadeep Mandal, Ajoy Kumar Chakraborty, “A Hybrid Cryptosystem of Image and Text Files Using Blowfish and Diffie-Hellman Techniques”, 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON).
11. Shraphalya B. Nalawade, Dhanashri H. Gawali, “Design and implementation of blowfish algorithm using reconfigurable platform”, 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE).
12. Adviti Chauhan & Jyoti Gupta, “A novel technique of cloud security based on hybrid encryption by Blowfish and MD5”, 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC).
13. Saptarshi Mitra, Bappaditya Jana, Jayanta Poray, “Implementation of a novel security technique using triple DES in cashless transaction”, 2017 International Conference on Computer, Electrical & Communication Engineering (ICCECE).
14. Jasvir Kaur and Brahmaleen Kaur Sidhu, “A Survey on Lightweight Block Ciphers for Wireless Sensor Network”, International Journal of Advanced Research in Computer Science. Volume 8, No. 5, May – June 2017.
15. Deepthi, Pradyumna G.R, “Comparison of MD5 and Blowfish Algorithm”, International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 5, Special Issue 9, May 2016.
16. Jaber Hosseinzadeh, Maghsoud hosseinzadeh, “A Comprehensive Survey on Evaluation of Lightweight Symmetric Ciphers: Hardware and Software Implementation”, Advances in computer science: An International Journal, Vol.5, Issue 4, No. 22, July 2016 ISSN :2322- 5157.
17. Salah A. k. Albermany and Fatima RadiHamade, “Survey: Block cipher Methods”, International Journal of Advancements in Research & Technology, Volume 5, Issue 11, November-2016.ISSN 2278-7763.
18. Karima Dichou, Victor Tourtchine, Faycal Rahmoune, “Finding the Best FPGA Implementation of the DES Algorithm to Secure Smart Cards”, 2015 4th International Conference on Electrical Engineering (ICEE).
19. Poonam Jindal, Singh,”Analyzing the Security-Performance Tradeoff in Block Ciphers”, International Conference on Computing, Communication & Automation.
20. Hassan Noura, A.E Samhat, Y. Harkouses and T.A. Yahiya, “Design and realization of a New neutral block cipher” In Applied Research in Computer Science and Engineering (ICAR), 2015 International Conference on (pp.1-6). IEEE.
21. Monika Agrawal, Pradeep Mishra, “A Comparative Survey on Symmetric Key Encryption Techniques”, International Journal on Computer Science and Engineering (IJCSE).
22. Prabhat Kumar Kushwaha, M. P Singh, “A Survey on Lightweight Block Ciphers”, International Journal of Computer Applications, vol. 96, issue 17, pp. 1-7.