International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 *Revised:* 20 May 2023 *Accepted:* 03 June 2023

A Novel Approach for Enhancement of Blowfish Algorithm by using DES, DCT Methods for Providing, Strong Encryption and Decryption Capabilities

Vikas Singhal[1], Devendra Singh[2], S. K. Gupta[3]
[1]School of Computer Science & Applications IFTM University, INDIA
vikassinghal@gniot.net.in
[2]School of Computer Science & Applications IFTM University, INDIA
devendrasingh@iftmuniversity.ac.in
[3]BIET, Jhansi, INDIA
guptask_biet@rediffmail.com

Abstract: Data safety has evolved into a critical requirement and a duty in modern life. Most of our systems are designed in such a way that it can get hacked, putting our private information at danger. As a result, for numerous safety motives, we utilize various approaches to save as much as possible on this data, regardless of its varied formats, words, photographs, videos, and so on**.** The data storage capacity of mobile devices is restricted owing to insufficient data storage and processing. In order to develop a safe MCC environment, security concerns must be studied and analysed. This study compares the most widely used symmetric key encryption algorithms, including DES (Data Encryption Standard), Blowfish, TDES (Triple Data Encryption Standard), PRESENT, and KLEIN. The assessment of algorithms is based on attacks, key size, and block size, with the best outcomes in their field.

Keywords: Data security, Blowfish, DES.

I. INTRODUCTION

Smartphones have made it easier for people to stay in touch and get entry to a wide variety of useful resources [1-4]. Cloud computing is a reliable method of service provision since it utilizes existing computer technology in a cohesive manner. There are three primary service delivery models that are used for cloud computing implementations. Customers have several entry points to cloud service delivery. Cloud computing in a wireless form is one such method. Key features of MCC, such as scalability, adaptability, availability, resource pooling, and user-based pricing, have led to its association with cloud computing. In addition, a hostile user is more likely to attack if the user is uninformed of the location of their data.

A number of MCC concerns include limited possessions in customer phones, mobility organization, channel bandwidth obtainability, stability, network access costs, resistance, faith, request facilities issues, process divesting, and so on. Despite the fact that it is a large topic, academics have decided to focus on its most serious issue, the "Complete absence of Security and privacy in MAC" [10]. Additionally, in order to address these issues, we will concentrate on the present methods for safeguarding user information in MAC.

Data Safety Control

Data protection refers to the protection of data from unauthorised users and corruption throughout its lifespan. This includes data encoding and critical organization deliveries. If a corporation need more security and secrecy, it might set up a dispersed scheme among many servers. Servers are the type of server that accomplishes just that. Data security is jeopardised since evidence about an organisation can be collective.

As a result, data defense in MAC systems is required to safe such critical info. [15] A cloud provider must have the following fundamental capabilities: An encryption technique for shared storing to keep data safe, highly stringent user access policies to guarantee that no unauthorised users have to get data, and the holdup must be planned.

Security is typically within these basic capabilities, although there are certain issues that might be addressed in attendance. Is information security simply the responsibility of the cloud provider, or is it also the obligation of the company leasing the possessions? Workers must build a system that is resistant to external attacks in order to maintain and safeguard data. The system's architecture and foundation should also be fault-tolerant. MAC contains a

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 Revised: 20 May 2023 Accepted: 03 June 2023

variety of variables, such as cloud data distribution privacy. These recommendations will help to safeguard from outside attacks. In the current study, we compare all of the available alternatives in this category.

In the second section, we present our contributions. The technique is outlined, and then its implementation is demonstrated. The procedure for the experiment is described. In the final section, we draw some conclusions and make some suggestions for future studies.

II. LITERATURE SURVEY

The author [1] proposed developing a digital security for data curated application. The software may be used to lock down files of many formats, including some text editors and tools for office works. After being encrypted with DES, the data is hidden in the cover image with the DCT method. Also, the average computational time per byte was 0.83 ms, the average size increased 6.85 times, and the success rate was 68%, according to the experiment results.

The objective of the author [2] was to identify a means of improving data privacy and client security in mobile cloud computing. The (EB) method is used to encode one's data, and a basic hash function is employed to hash the global private key. The security and confidentiality of user information can both benefit from hashing.

The author [3] presented a crypto approach for data encryption that uses Blowfish algorithm to protect sensitive data on the server from unauthorised access. As a result, maintaining privacy and safeguarding sensitive data saved in the cloud. The experimental findings show that all of the algorithms produce adequate stego picture quality. They can be used as cryptographic algorithms before applying steganography algorithms to encrypt a message.

The author [4] introduced a wavelet-based steganography system that combines encryption and scrambling to secure patient private data. The suggested technique conceals the ECG signal's associated patient personal data and other physiological information, ensuring the integration of the ECG and the rest. Two distortion-measuring metrics were employed to evaluate the efficiency of the planned method on the ECG signal: the percentage residual difference and the wavelet-weighted PRD.

One of the key answers in security-related requests was to offer the necessary protection against data assaults. Block cypher symmetric key cryptography is used extensively in data security systems. The author [5] compared the most widely used symmetric key encryption algorithms, including DES, Blowfish, and TDES.

The author [6] thoroughly examined steganography, spatial and frequency domain approaches combined with encryption, and error correcting techniques. A thorough examination of the published literature found that spatial domain approaches need less computing time for data embedding and give more data concealing capability than frequency domain methods. [7] The performance of such strategies was assessed using visual quality and robustness measures. The current issues and future developments in multi-layer data security in video steganography are explored in order to give a taxonomy for further exploration.

Information can be hidden in the least significant region of each pixel, as suggested by the author [8]. On the other side, this may be readily tampered with. This motivates the introduction of a new, safer approach. Blowfish is used as the initial layer of encryption for the data. After then, a fresh approach is introduced. This encrypted block is then split into 'n' smaller blocks, with each block being disguised by one of 'n' randomly selected images. The proper stacking of blocks is maintained using a hash table. The LSB algorithm is then used to encrypt this image, resulting in the hashing image.

Before embedding, [9] the secret messages were converted to an unreadable format using a cryptography technique. This algorithm prevent messages from being stolen or destroyed by undesired internet users and hence guarantee adequate security. The Blowfish algorithm was used for text message encryption and decryption utilising a secret-key block cypher. Blowfish is an evolutionary enhancement on DES, 3DES, and other algorithms meant to improve security and speed. This technique use a changeable key length of up to 448 bits.

The use of lossless compression approach given by the author [10] is to ensure that all data is reversible and may be returned to the original while keeping the high quality of reconstructed pictures and compression ratio. As a result, this notion is most useful where data accuracy is critical, such as with textual information, biological images, and legal data.

Based on variable temporal data permutation, the author [11] proposed a high-yield reconfigurable hardware implementation of the new (DES). The permutation selection changed over time. The ciphered data for the same data and key was modified over time, increasing the algorithm's security. In our design, we applied the pipelining notion.[13] Our DES is built on a Xilinx Spartan-3e processor. The final 18-stage pipelined architecture has a data throughput of 8.26 Gbps and 2342 CLB slices.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 Revised: 20 May 2023 Accepted: 03 June 2023

Enigma technology, pass points, and cued recall are just a few examples of image-based passwords designed to thwart these attacks, but they come at a performance cost because they need the download of big images during the password generation process an innovative, secure method described by the author [12] to circumvent this problem.

The author [14] presented text encoding, text embedding into images, and the fuzzy vault key generation method, as well as the RSA algorithm, for secure data storage. The author employed these methods to get access to protected areas of the system, so enhancing its defenses. (UACI) for the resulting encrypted image is 56.42 percent, and 96.32 percent, both of which are quite close to the ideal value.

The structure [15] was evaluated and assessed founded on the computing time and recall space required to perform each method under consideration because it only operated on a small section of the image rather than the entire image pixels. The filtered picture was compared to the original, as was the PSNR of the non-filtered input image. The filtered has a higher PSNR, which actually justifies the effect of adding filtering to the built system's image processing modules.

III. METHODOLOGY

The study deals with the discretion and safety of user data by employing an innovative clustering and security technique. We need to cluster the data and cyber security based on the similarity measure since the acquired data might initially be in either text or picture format. In the cloud, the clustered data are encrypted using the BE paradigm. Only those who are supposed to have access to the data have copies of the symmetric keys needed to decode it. After encryption, information is saved in the cloud or a strategic location, and then decrypted using the most suitable private key.

Client and server exchange cryptographic keys and an identifier for the file, which are required for decrypting the ciphertext. Users receive the secret key through email as part of the normal signup process after providing an email address and choosing a password. After receiving the cryptographic keys, the client can use them to decrypt the encrypted message and recover the plaintext. If the document ID is not the same as the unique code, an error will occur during the message's creation.

CRYPTOGRAPHY ALGORITHMS

The goal of cryptography algorithms is to change data such that only trustworthy users with access to the keys may read the sent data. Private and public cryptography approaches are distinguished. Private cryptography use the same opening for both encoding and decoding. Public cryptography, on the other hand, employs distinct keys for the encryption and decryption procedures. Steganography's symmetric and asymmetric algorithms have recently gained popularity.

1. DES

2. Blowfish

3. Triple DES

DES

The Data Encoding Standard (DES) is a symmetrical key block cypher that was disseminated by the (NIST).

DES was invented by IBM and was initially published in 1975 and standardized in 1977. It has been used for more than thirty years. DES employs a block unit of 68 bits and a key size of 52 bits.

The DES Algorithm is made up of the following phases, respectively of which is identified as a Round Algorithm.

1. The 64-bit plain text block was first sent across Initial Permutation in the first phase.

2. The first permutation is achieved on the specified plain text.

3. Basic permutation generates mutated blocks that are separated into two halfbacks: left and right plain text.

4. Right side of the basic change and Left plain text are now subjected to an 18-round cryptography method, each with its own factor:

Using the distinct key alteration, a separate 48-bit which are then permuted using Pbox permutation.

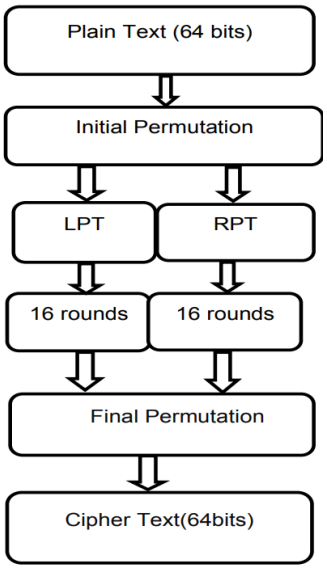


Fig. 1 DES Algorithm

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 Revised: 20 May 2023 Accepted: 03 June 2023

BLOWFISH

Blowfish is a symmetrical key block cypher developed by Bruce Schneiier in 1996 that is used in a variety of encoding domains and cypher suites. Blowfish employs a 64-bit block cypher with key sizes ranging from 32 to 448 bits. Blowfish was created by Schneier as an alternative to DES ageing and may be optimised in hardware applications because to its compactness.

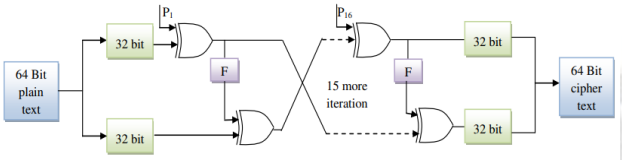


Fig. 2 Blowfish Algorithm

Triple DES

TDES, or Triple Data Encryption Algorithm, was evolved from DES in 1993. TDES is a symmetrical block cypher that applies the DES block cipher's method three times to apiece chunk's contents. It has 68-bit block sizes and 169, 110-, or 58-bit key dimensions.

The following steps are presented in Fig.3 for the encryption process:

- Encrypt the data using the DES method and the main key K1.
- Next, using the next key K2, decode the main key output created by the DES algorithm.
- Finally, encode the production of the other key with the aid of the distinct key using the DES algorithm.

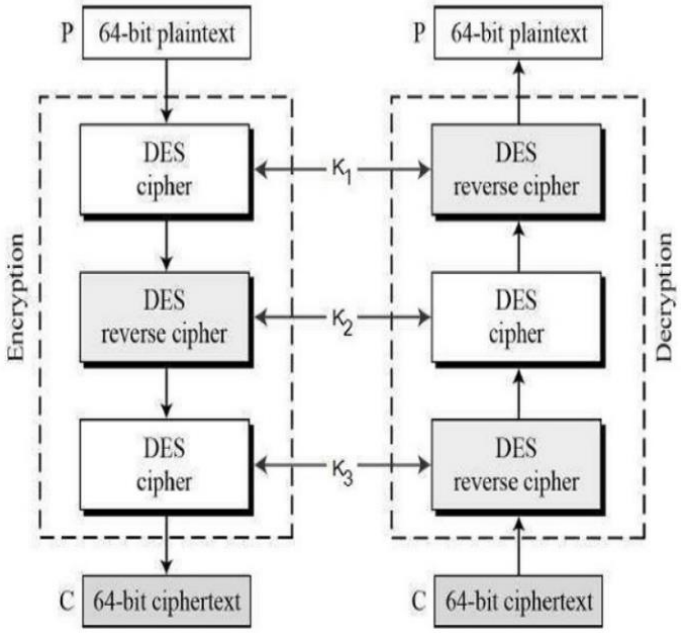


Fig. 3 Triple DES

IV. PROPOSED METHOD

The user first takeaway of the text to be concealed and then encodes it using the Blowfish encoding technique and a variable-length key. User will have the key.

This encoded data is then broken down into 'n' chunks. Now, n photographs are chosen at random from a collection of images. Individually fragmented block is randomly encoded to one picture. To achieve the right instruction in terms of data sequence, a hash table is maintained.

The proposed approach has various advantages.

- To begin with, encryption improves security. The randomization of picture transmission therefore adds to the algorithm's security. It can also be observed later in the findings that the planned technique is not noteworthy in relations of execution time.
- The goal of safely concealing information is accomplished flawlessly. The crucial thing to remember is that the photos should not be repeated, as the scheme does not become disordered.

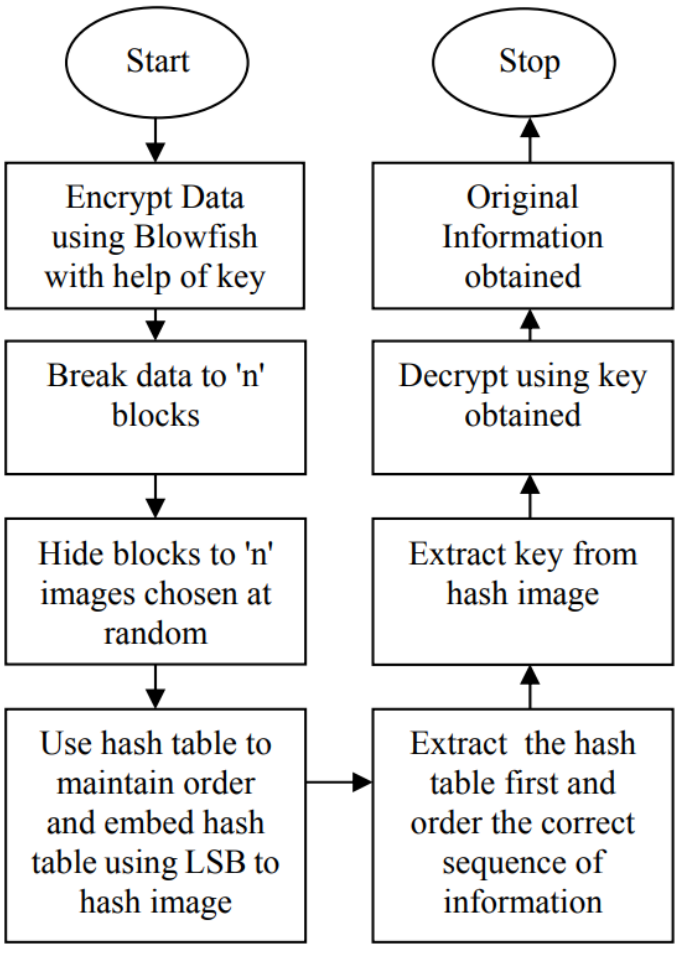


Fig. 4 Flowchart of Proposed Algorithm

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 *Revised:* 20 May 2023 *Accepted:* 03 June 2023

Because we are merging encoding with the projected algorithm, all of these add to the complication of executing the programme and will almost positively result in an amplified output in terms of execution time. Nonetheless, as can be seen, the execution time is not excessive.

IMPLEMENTATION AND OUTCOME INVESTIGATION

In the operation phase, we first look at the shaped log file in the structure with respect to time bounded on three constraints: verification of a user throughout the retrieving of the log file [14], storing of data, and the realization that our proposed scheme construction is superior to storing the statistics into the definite file in the cloud. The following is an implementation of the recommended method for safe cloud use:

a. Login to the program, which allows you to use the offered encryption method. Authentication and user identity are both protected in this way.

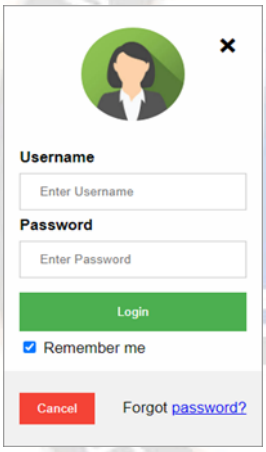


Figure 4: System login for encryption

b. The user then has the option to encrypt or decrypt the file using the preceding steps.

c. The text file is encoded using a variable-size encryption key (between 32 and 448 bits in length) and the encryption algorithm, which splits the data into fixed-length blocks of 62 bits throughout its procedure and achieves encoding for 14 times.

Figure.5. Encrypt/decrypt the text

a. Once the encryption procedure is complete, a new encryption key is created and the original key is encoded using the LSB encoding method for image steganography, which embeds the key within a cover picture for safekeeping.

b. The same text file may be decrypted using the same LSB encryption key after its encryption key has been decoded, or recovered, from the cover picture. At last, the recovered encryption key is used to decode the encrypted file.

EVALUATION OF CURRENT AND PROPOSED ALGORITHM

When compared to alternative methods of producing encryption keys, the Blowfish technique is far superior. The developed Blowfish method is superior than other symmetric algorithms as shown in table.1. Since the suggested method employs the Blowfish algorithm and the LSB algorithm for picture steganography to safeguard the encoding key, the user's data is shielded by many layers of defense.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 Revised: 20 May 2023 Accepted: 03 June 2023

Table I. Assessment of Symmetric Algorithm

S. No.	Algorithms	size	Block size	times	structure	flexible	features
1	DES	62 bits	62 bits	18	Feistel	No	Not structure
2	DCT	110 or 114 bits	64 bits	42	Feistel	Yes	Adequate
6	BLOWFISH	32-280 bits	64 bits	15	Feistel	yes	Excellent

We also have pictures, and those are 613 pixels by 632. The maximum size of a message thought to be encrypted using any of the aforementioned five algorithms is around 1Kbits. All five techniques use the same plaintext for encryption. Table I shows the initial comparison, based on how long it takes to encrypt a file, including the time needed to generate a key. Five different algorithms have been imported as Java programs and implemented in MATLAB On the same platform, [15] five different algorithms are implemented.

Fig. 1 (a) Peppers

(b) Baboon

Each algorithm's key length is taken to be the most frequently used, secure key length in practical use today. According to the numbers, the RSA cryptographic technique has the slowest encryption time overall, key generation included. Because it uses public keys, it requires two separate keys to run. Table II below displays the decryption times for various methods.

Table II. Decryption period of DES, DCT, and Blowfish

Algorithms	Length bits	Decryption time (s)
DES	52	0.000634
DCT	218	0.001024
Blowfish	118	0.000845

Since key creation is ignored during these calculations, decryption is faster than encryption. Besides (MSE), (SNR), and (PSNR) are used to measure the quality of the steganography created with the five cryptanalytic procedures and the LSB method. The image quality is quantified by the PSNR value. The greater the PSNR score, the sharper the image. The PSNR value must be more than 45 dB.

$$PSNR = 10*\log_{10}\left[\frac{R^2}{MSE}\right]$$

[15]. The Mean Squared Error (MSE) measures how unlike or similar the steganography picture is to the original. A lower MSE score indicates less variation from the original in terms of image quality and distortion. [16].

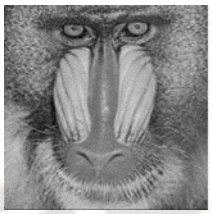
Table III. Encryption time of DES, DCT, and Blowfish

Algorithm	Key length bits	Encryption time (s)
DES	52	0.004325
DCT	158	0.000986
Blowfish	120	0.004365

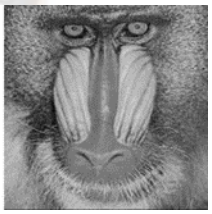
Table IV. The SNR, PSNR and MSE values

Algorithm	SNR	PSNR	MSE
DES	69.5432	71.2828	0.0054
DCT	61.4321	70.5436	0.0068
Blowfish	60.5432	72.3246	0.00876

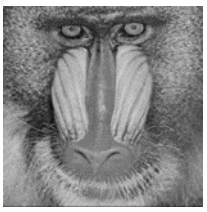
Optimal performance is attained with a high PSNR and a low MSE. The cover picture was a baboon, and the SNR, PSNR, and MSE values for the DES, DCT, and Blowfish algorithms were shown in Table IV. Perfect values are shown by the results of employing varied algorithms as cryptographic methods and the LSB process with the Peppers and Baboon pictures as cover images.



(a)



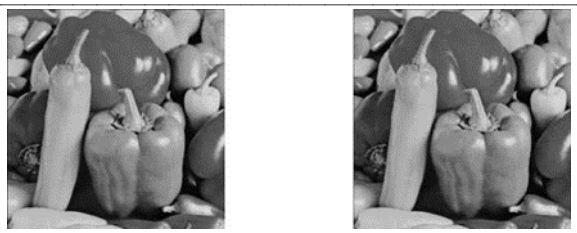
(b)



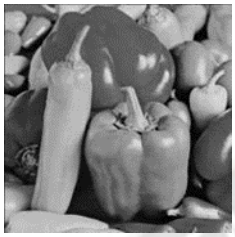
(c)

Fig. 2 cover image of baboons

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 Revised: 20 May 2023 Accepted: 03 June 2023



(a)



(c)

Fig. 3 cover images of peppers

Fig. 1 displays the 512x512 input cover pictures, whereas Figures 2 and 3 display the generated stego images using the DES, DCT, and Blowfish algorithms, respectively. Measurement of resistance to standard statistical assaults is demonstrated by comparing images. Figures 4 show a comparison amid the histograms of stego pictures and the cover image. According to the data, the histograms of the cover and stego pictures are not drastically different.

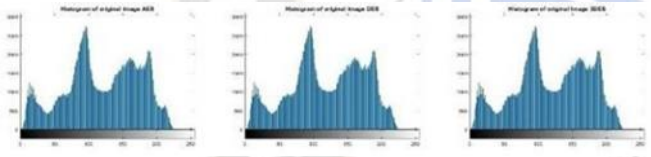


Fig. 4 Histogram retaining (a) DES (b) DCT (c) Blowfish

V. CONCLUSION

The safety and confidentiality of sensitive data in the cloud is a serious concern in cyber data security. In this study, we proposed an efficient secure-based cloud loading system that improves dispensation speed while ensuring discretion and honesty using data clustering.

The BE algorithm improves cyber security by selecting the best key using the metaheuristic method. The simulation results show that the suggested optimum blowfish method enhances cyber security accuracy for all undisclosed data while requiring less encryption, decryption, and performance time than current techniques. Though the algorithm works well for JPEG format images, its efficiency needs to be tested for other image types and HD quality images. We hope to concentrate our efforts on various types of multimedia applications, such as text, audio, and video, with appropriate algorithms. In the future, we will investigate sensitive data using different similarity techniques and an encryption-based hybrid optimisation strategy.

REFERENCES

[1] Solichin, A., & Ramadhan, E. W. (2017, October). Enhancing data security using DES-based cryptography and DCT-based steganography. In *2017 3rd International Conference on Science in Information Technology (ICSITech)* (pp. 618-621). IEEE.

[2] Prakash, V. S., Bharathiraja, N., Nayagam, R. D., Thiagarajan, R., Krishnamoorthy, R., & Omana, J. (2022, April). EB Algorithm for Effective Privacy and Security of Data Processing in MCC. In *2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC)* (pp. 241-246). IEEE.

[3] Reddy, A. ., & Waheeb , M. Q. . (2022). Enhanced Pre-Processing Based Cardiac Valve Block Detection Using Deep Learning Architectures. Research Journal of Computer Systems and Engineering, 3(1), 84–89. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/47

[4] Singhal, V., Singh, D., & Gupta, S. K. (2022). Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms. *JOURNAL OF ALGEBRAIC STATISTICS*, *13*(3), 1162-1171.

[5] Chetan, M. D., & Anitadevi, M. D. Enhanced Audio Steganography using Triple DES and DWT Transformation.

[6] Shetty, V. S., Anusha, R., MJ, D. K., & Hegde, P. (2020, February). A survey on performance analysis of block cipher algorithms. In *2020 International Conference on Inventive Computation Technologies (ICICT)* (pp. 167-174). IEEE.

[7] Kamil, S., Ayob, M., Sheikhabdullah, S. N. H., & Ahmad, Z. (2018). Challenges in multi-layer data security for video steganography. *Asia-Pacific Journal of Information Technology and Multimedia*, *7*(2–2), 53-62.

[8] Anitadevi, M. D. Enhanced Colour Image Security and Data Hiding Using ECC Encryption and DWT-SVD Transforms.

[9] Gowda, S. N. (2016, October). Using Blowfish encryption to enhance security feature of an image. In *2016 6th International Conference on Information Communication and Management (ICICM)* (pp. 126-129). IEEE.

[10] Vaidya, A., More, P. N., Fegade, R. K., Bhavsar, M. A., & Raut, P. V. (2013). Image Steganography Using DWT and Blowfish Algorithms. *IOSR Journal of Computer Engineering*, *8*(6), 15-19.

[11] Mr. Rahul Sharma. (2018). Monitoring of Drainage System in Urban Using Device Free Localization Neural Networks and Cloud computing. International Journal of New Practices in Management and Engineering, 7(04), 08 - 14. https://doi.org/10.17762/ijnpme.v7i04.69

[12] Setyaningsih, E., & Wardoyo, R. (2017). Review of image compression and encryption techniques. *International journal of advanced computer science and applications*, *8*(2).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7008
Article Received: 04 April 2023 Revised: 20 May 2023 Accepted: 03 June 2023

[13] Dhir, A. (2000). Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs. *White Paper: Spartan-II FPGAs, WP115 (v1. 0) March*, *9*.

[14] Prasad, K. L., Anusha, P., Jyothi, G., & Dileepkumar, K. (2016). Design and Analysis of Secure and Efficient Image with Embedded Sensitive Information Transferring Technique using Blowfish Algorithm. *i-Manager's Journal on Information Technology*, *5*(3), 1.

[15] ALRikabi, H. T., & Hazim, H. T. (2021). Enhanced data security of communication system using combined encryption and steganography. *International Journal of Interactive Mobile Technologies*, *15*(16), 145.

[16] Mahmood, M. A., & Tabassum, T. (2021, December). A Hybrid Cryptographic Data Security System Utilizing Fuzzy Vault Key. In *2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)* (pp. 89-93). IEEE.

[17] Kamau, J., Goldberg, R., Oliveira, A., Seo-joon, C., & Nakamura, E. Improving Recommendation Systems with Collaborative Filtering Algorithms. Kuwait Journal of Machine Learning, 1(3). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/134

[18] Asaju, B., Popoola, D. D., & Gbolagade, K. A. (2022). Enhancing Image Security Using Data Encryption Standard, Discrete Wavelet Tranfrom Watermarking, Residue Number System and Gaussian Filtering.

[19] A. Pandey, and P. Bonde, "Performance evaluation of various cryptography algorithms along with LSB substitution technique", International Journal of Engineering Research & Technology (IJERT), vol. 2, no. 6, 2013, pp. 866-871.

[20] S. Nagpal, and R. Nagpal, "Collaboration of cryptography and steganography for enhanced security: a review", International Journal of Innovative Knowledge Concepts, vol. 6, no. 8, 2018, pp. 124-128.

[21] The USC-SIPI Image Database. Available online: http://sipi.usc.edu/database/ (accessed on 6 July 2019).