Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Analysis of image security by triple DES

Subba Rao Peram [a], Giddi Harsha vardhan [a], Mandavilli Neeraj [a], B Anand Kumar [b]

[a] Department of Inforamtion Technology, VFSTR Deemed to be University, Vadlamudi, Guntur, Andhra Pradesh, India
[b] Department of Computer Science and Engineering, MLR Institute of Technology, Hyderabad, India

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Triple Des
Security
Images
Des
Encryption
Internet
Active Attack
Passive Attack

ABSTRACT

We all know that in this growing world digital services usage has become more, the digital services are like communication over the internet, medical field, military imaging systems these need will need a high level of security. To correctly store and transmit digital photographs containing sensitive information, a security level is required. This is due to the rapid advancement of multimedia technologies, the internet, and cell phones. As an outcome, image encryption resolutions are compulsory to safeguard photos from such attacks. In this system, we employ Triple DES to hide photographs (Data Encryption Standard). This sort of encryption helps to keep both active and passive threats at bay.
Copyright © 2022 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Conference on Advanced Materials for Innovation and Sustainability.

1. Introduction to cryptography

The encryption technique turns the plaintext input that is given by the user into an encrypted output i.e another format of input using a suitable algorithm and a key (i.e., cipher text). A particularly suitable algorithm will always convert the same plaintext into the same cipher text if the same key is used for both processes. Fig. 1.Fig. 2.Fig. 3.Fig. 4..

The approach is deemed steady if an attacker can't decide any attributes of the plaintext or key from the cipher text. An attacker has to now no longer be capable of deriving something approximately the important thing primarily based totally on a huge quantity of plaintext/cipher text combos that utilized it.

Many programs use cryptography, together with economic transactions, laptop passwords, and e-trade transactions.

Three types of cryptographic techniques used in general.

1. Cryptography with symmetric keys
2. Hash functions.
3. Public-key cryptography

1.1. Cryptography with symmetric keys

Cryptography with symmetric keys makes use of one key shared via way of means of each sender and consequently the receiver. The sender encrypts plaintext and sends the cipher textual content to the receiver the usage of this key. The receiver, on the other hand, decrypts the message and retrieves the apparent textual content the usage of an equal key.

2. Public-key cryptography

The maximum progressive idea in the closing 300-four hundred years is public-key cryptography. Two associated keys (public and private key) are utilised in public-key cryptography. the overall public key are regularly freely transmitted, however the personal key that is going with it should be stored secret. the overall public secret is used for encryption, while the personal secret is utilised for decryption [22,23].

2.1. Hash Functions

This set of rules would not use a key. The simple textual content is hashed with a fixed-period hash cost that prevents the obvious textual content's contents from being recovered. Many working structures additionally rent hash algorithms to stable passwords. In symmetric cryptography, the equal key's used for encryption and decryption. Both the sender and the recipient ought to have a not unusual place key that they each know.

Data encrypted with a public key can simplest be decrypted with the matching non-public key. As a result, sending a message to harsha involves the use of harsha's public key to encrypt it. Only harsha has get admission to to his non-public key, permitting him

E-mail addresses: subbarao.peram@gmail.com (S.R. Peram), harsharocking789@gmail.com (G. Harsha vardhan), mnr42000@gmail.com (M. Neeraj)

https://doi.org/10.1016/j.matpr.2022.05.321
2214-7853/Copyright © 2022 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Conference on Advanced Materials for Innovation and Sustainability.

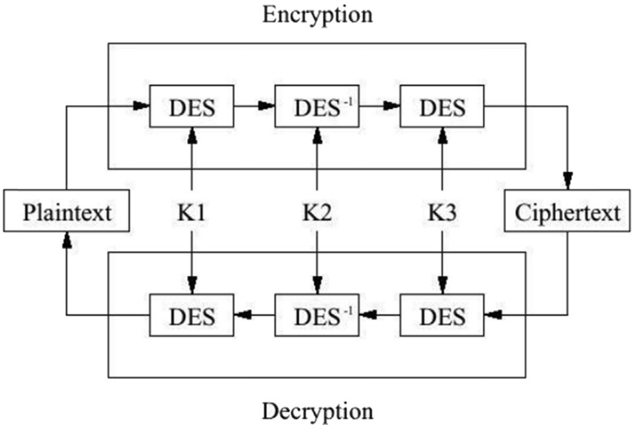

Fig. 1. Encryption scheme.

to decode the communication. Any statistics encrypted with a private key can simplest be decrypted with the overall public key that corresponds there too. Jane might also additionally moreover use her non-public key to digitally signal a message, and all of us with Jane's public key may want to decrypt the signed message and confirm that it were Jane who despatched it.

2.2. Data encryption Standard (DES)

The Data Encryption Standard (DES) can be a symmetric block cipher that turned into formerly hired with the aid of using the US authorities et al. to encrypt touchy data. When DES turned into deserted in the face of warring parties less difficult brute-pressure capability, the Advanced Encryption Standard (AES) turned into added to require its place (AES). The DES (Data Encryption Standard) set of rules became advanced inside the early Seventies as a symmetric-key block cipher. The National Institute of Standards and Technology (NIST) has followed an IBM team's work. The set of rules considers it divides the apparent textual content into 64-bit blocks and turns them to 48-bit keys are wont to encrypt the textual content.

The records is encrypted and decrypted the usage of the identical key due to the fact it is a symmetric-key approach. DES employs the Feistel structure in 16 rounds, each with its own key. Triple DES can be a symmetric key-block encryption that makes use of 3 copies of the DES cypher. It encrypts the use of key one (k1), decrypts with key two (k2), then encrypts with key 3 (k3). A two-key version exists, for the duration of which k1 and k3 are the same keys.

Because of the developing processing capability of new computers, the NIST needed to range the DES set of rules due to the fact its 56-bit key lengths had been too short. The energy of encryption is proportional to the important thing size, and DES has fallen sufferer to growing technical improvements in computing. It got here to a point in which 56-bit encryption become now no longer successful meet the brand new encryption problems and access control problems [24].

2.3. Analysis of DES

The DES contents both the asked parcels of block cipher. Cipher is particularly strong because of its features. Absoluteness-Each cipher text bit is dependent on a large number of plaintext bits.

During the ultimate many times, cryptanalysis has observed a few excrescencies in DES whilst vulnerable keys are used. DES has proved to be a assuredly nicely designed block cipher. Other than overall critical hunt, there had been no superb cryptanalytic assaults on DES.

2.4. Triple DES 3-KEY

As the safety excrescencies of DES got here decreasingly apparent, 3DES changed into provided as a way to boom the vital length while not having to supply a completely new algorithm.

Rather than using a one key as in DES,

- DES runs the DES algorithm three times, with three 56- bit keys
- Key one is used to cipher the plaintext.
- The textbook that was translated by crucial one is deciphered using crucial two.
- The text decrypted by key two is encrypted using key three. Before using 3TDES, stoner first induce and distribute a 3TDES crucial K, which consists of three different DES keys K1, K2 and K3. This means that the factual 3TDES key has length 3 multiplied by 56 equals 168 bits.

The encryption-decryption process is as follows –.

- Cipher the plaintext blocks using single DES with crucial K1.
- Now decipher the affair of step 1 using single DES with crucial K2.
- Eventually, cipher the result of step 2 with crucial K3 using single DES.
- The cipher text is the result of step 3.

Decryption of a cipher text isn't a normal process but reverse. Stoner first decrypt using K3, also cipher with K2, and eventually decipher with K1. The encryption scheme is illustrated as follows-.

Because Triple DES is designed as an encrypt – decrypt – encrypt procedure, a 3TDES (tackle) perpetration for single DES may be utilized by putting K1, K2, and K3 to the identical value. K3 is substituted through K1 withinside the change version of Triple DES (2TDES), that is equal to 3TDES. To positioned it every other way, the stoner encrypts plaintext blocks with critical K1, decrypts with critical K2, and additionally encrypts withK1.As a result, the critical period of 2TDES is 112 bits. Triadic DES encryption is particularly greater stable than unmarried DES encryption, however it is manifestly slower.

3. Literature review

New Image Encryption Technique Based On Combination of Block Displacement and Block Cipher Technique 2013. A new image encryption technique is proposed in this paper. The length of the key has already been established as a factor in the security of an algorithm. Longer keys will always provide good security measures, as a result. The suggested approach makes use of a 128- bit crucial, which provides far too important security. To benefit get entry to to the authentic key or do a cryptographic evaluation of the counseled key, a hacker will want 2128 instances to interrupt the key, which is almost insolvable [11]. All of the node movements should be aimed in the direction of the tree's root, hence the placements of the routers and the tree topology should be designed and created to achieve[21]. On the ATMEL 8051 microcontroller, the voice recognition system has been successfully constructed. The suggested system has been effectively implemented, which provides robustness and reliability due to the many factors in the research paper[14].

Because no comparable exceptional formulation were carried out to the proposed algorithm, there may be no eventuality of producing floating factor crimes. The correlation co-green in addition to their entropy values have been plant for the proposed approach.

A Survey On Different Image Encryption and Decryption Techniques This work gave a evaluation of over 25 exploration courses

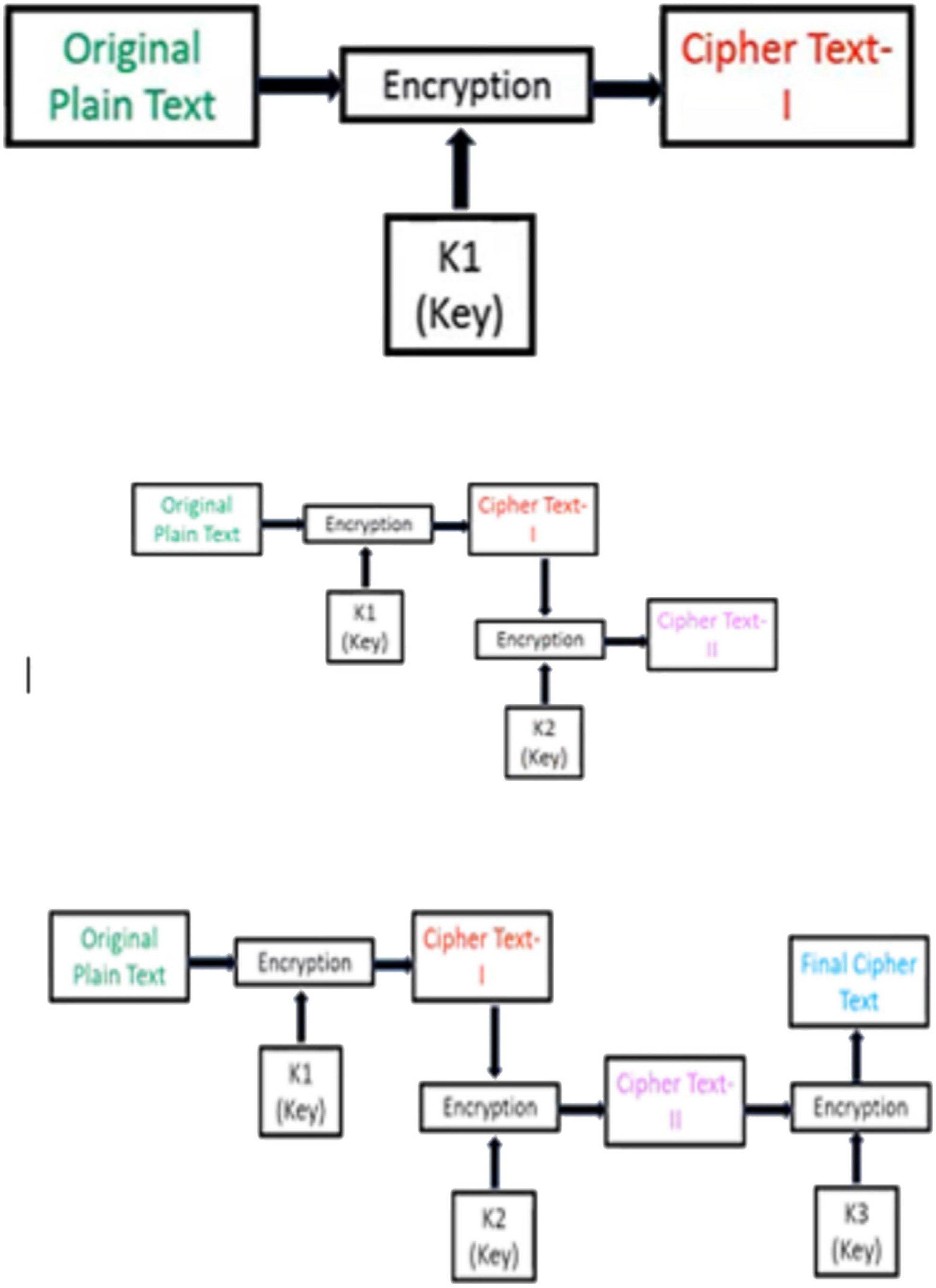

Fig. 2. Triple Key Encryption.

on photo encryption algorithms that climbed the pixel of the picture and dropped the correlation most of the pixels, appearing in an translated picture with decrease correlation most of the pixels. There was a review of the colorful image encryption and decryption algorithms that are now available. In addition, the paper looked at how Picture encryption and decryption algorithms work [112].

Text and Image Encryption/ Decryption Using Advanced Encryption Standard 2014. AES was used to encrypt and decrypt text and images in this paper. The characteristics of data are determined by its type. As a result, the same encryption method cannot be utilised for all sorts of data. If the photos are enormous in size and have real-time constraints, then a comparable strategy cannot be utilised to safeguard images and text from unwanted access. AES may be used to protect both images and text in a few different ways[213].

Performance Analysis of DES and Triple DES 2015. With the rapid advancement of digital data interchange via electronic means, data storage and transmission security is becoming increasingly crucial. Cryptography has emerged as a viable technique for protecting information security systems from hostile attacks. The most significant part of dispatches security is cryptography, which is also getting a pivotal structure block for computer security. This security medium scrambles data into undecipherable textbook that can only be decrypted or deciphered by parties who have access to the accompanying key. These algorithms need a lot

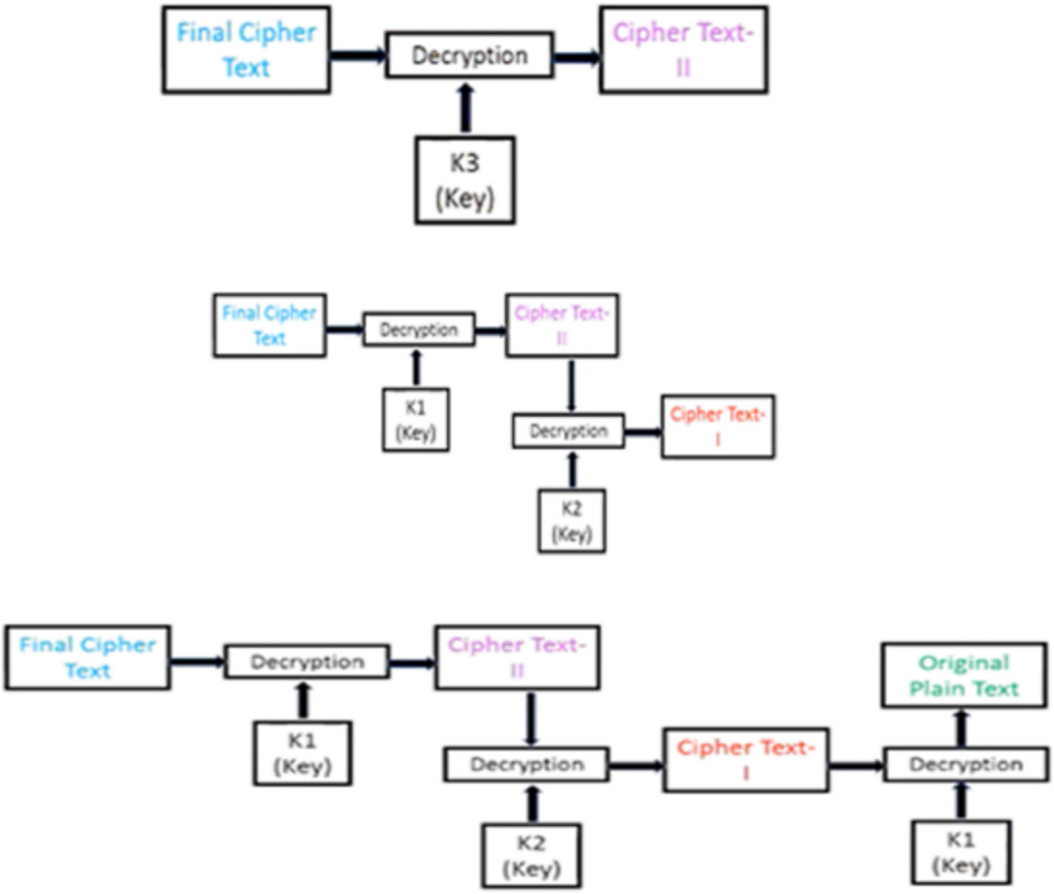

Fig. 3. TWO Key Encryption.

of computing coffers, including CPU time, memory, and calculation time. This exploration examines the performance of the extensively used symmetric encryption styles DES and 3DES [315].

Digital Watermarking Using Spatial Domain And Triple Des Due to the open atmosphere of internet use in today's period, a new set of difficulties in terms of copyright protection, security, and unauthorised sharing of private photographs have emerged. The subject of fragile and semi-fragile digital watermarking for image resilience and authentication is discussed in this study. The goal is to use a combination of digital watermarking and encryption to embed hidden information and achieve a high level of privacy and efficiency. The invader will have a hard time changing or removing the encrypted image from the cover image's spatial domain thanks to a TDES (Triple DES) encrypted watermark with a secret key bundle. MATLAB was used to implement the proposed strategies. The experimental results reveal that the proposed systems function well under a variety of noise conditions. These systems can be used for a variety of purposes, including data integrity and authentication, as well as content and copyright protection [416]. The proactive protocol and the reactive protocol are the two components that make up the zone routing protocol. The "Pro-active" protocol will deliver the packet immediately to the recipient if both the sender and the receiver are located within the same area[18].

Data Security by Using Triple DES and Performance Analysis of Crypto System This paper describes a cryptographic approach for private communication. It is a method for safeguarding sensitive information. A block cipher grounded on two cryptographic styles, the Data Encryption Standard (DES) and the Triple Data Encryption Algorithm (TDEA), is used to render the secret communication. With a block length of 128 bits and a crucial length of 256 bits, this algorithm outlines the fine way needed to change data into a cryptographic cypher and also back to the original form. This study compares the performance of the most popular encryption algorithms, including DES, 3DES, AES, and Blowfish [51719,23].

Image Encryption Built on the Altered Triple DES Cryptosystem When slate-scale prints are translated and saved in a lossless format (e.g., now no longer JPEG) with a set key for a symmetric cryptosystem, edges might also additionally seem due sections of the equal color withinside the image, revealing statistics approximately the authentic image.This is especially difficult when there are just two colours in the image, with black and white being the worst case situation. The former difficulty can be overcome with an asymmetric system, but the time it takes to run it is a significant disadvantage.

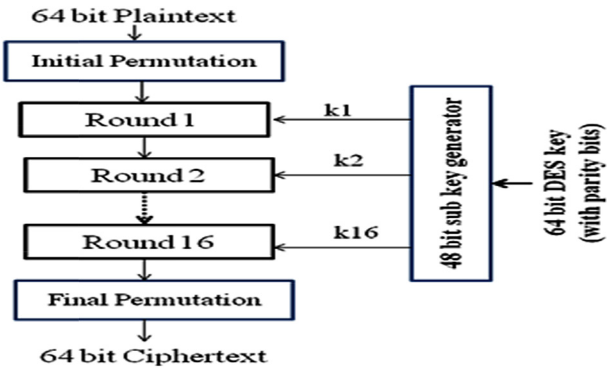

Fig. 4. Schematic Diagram.

Using the JV Theorem in conjunction with Triple DES with the addition of a variable permutation on the input string for the third round of the encryption process' first cycle. The goodness-of-fit test is a method of determining how well something fits together. The use of variable permutation is also shown to strengthen the Triple-DES cryptosystem. Still, due to the fact the images are translated with a symmetric cypher algorithm, the processing time is quicker than any given irregular algorithm. There's additionally a criterion for calculating the range of permutations [6910].

4. Existing work

Though DES has been cracked, 3DES is now appeared a stable cypher. Confusion and prolixity are requested elements of DES every little bit of cipher regular is considered necessary on numerous bits of the key, and converting a unmarried little bit of plaintext adjustments 1/2 of of the bits of cipher textual content on pars. Due to its Feistel structure and basic logic, DES is very easy to create. It does, however, need eight distinct S-Boxes, which results in a bigger footprint (AES uses a single S-Box). This is the existing work that has been going on for a long time, and you can see the benefits of the current system linked with it in the image above. However, there are drawbacks to the above-mentioned system; for example, the most severe fault with DES appears to be that it may be broken via brute-force search. Using 3DES, on the opposite hand, alleviates this problem on the fee of longer execution time. Linear cryptanalysis strategies are in addition touchy to DES. However, 247 acknowledged plaintexts are required to crack DES this manner. So to overcome this sort of issues and the attacks simultaneously the triple des has come into the field. Triple DES encryption is considerably greater steady than unmarried DES encryption, however it's miles glaringly slower. [378].

5. Proposed work

The proposed work tries to apply the same triple des algorithm technique on the image that is present on system. First an image is selected from the system that is to be encrypted, for encrypting that image using the algorithm we need to apply three different keys. And then the image will be encrypted, if any one tries to open the picture the image will be displayed as empty.to access the image again we need to decrypt the image with the three keys that are used for encrypting process.

5.1. Image decryption

Picture decryption is the polar opposite of image encryption. During the picture decryption procedure, the encrypted image is utilised as an input to the data encryption standard algorithm structure, which must be decoded. The received encrypted image is then separated into pixel blocks of the same size and length as the data encryption standard algorithm. The functionalities of various 64-bit blocks are first entered, and then the process is decrypted using the same secret key. The processes are equally accomplished with the identical secret key. There was an algorithm for picture encryption used in the image decryption process, and when the decryption process was completed, the obtained input was regarded a decrypted image with the same properties as the original image.

5.2. Significance of this project

The most important aspect of the selected projects is that they give information on different encryption and decryption methods that may be used to safeguard images that are often downloaded and shared on social media and networks.

5.3. Methodological approaches used here

Colourful journal publications, exploration papers, and papers are studied under the qualitative inquiry in order to meet the design's points, which is to give image encryption using the triadic Data Encryption Algorithm. 10. Coffers The experimental settings must be initialised in order to apply image encryption using the triadic Data Encryption standard and to estimate the performance of the proposed design. The trial is run on a 3500 AMD 64- bit CPU with 1 GB RAM to accommodate the large number of parameters necessary.

Triple des with triple number keys encryption:

- The functioning of triple DES is the same as that of double DES.
- Triple DES using three keys Kl, K2 & K3 while cracking plain textbook.
- First it performs encryption on plaintext P, which is translated using Kl and obtains thefirst cipher textbook C1.This cypher text is again encrypted with key K2, yielding the second cypher text C2.

Mathematically triple number DES (with triple keys) encryption is represented as,

C1 = E(K1, P).

C2 = E (K2, C1).

C2 = E (K2, E (K1, P.

C3 = E (K3, C2))).

C3 = E (K3, E (K2, C1)).

Which is again encrypted using K3 & generate final cipher text C3.

Where, P = Basic text,

K1 = Key − 1,

K2 = Key-2,

K3 = Key − 3,

C1 = first cipher text, C2 = second cipher text, C3 = Final cipher text,

E = Encryption Processes.

Triple des with triple number keys of decryption

- Decryption of Triple number DES is contrary of encryption.
- In triple number DES decryption. process final cipher textbook C3 decrypt using K3, result is cipher textbook C2.
- –C2 will be decipher with K2 and get C1 cipher textbook.
- Also C1 cipher textbook decipher with K1 key and get original plain textP. **Mathematically triple number DES (with 2 keys) decryption is represented as,**

C = Dec (Key1, C3).

C1 = Dec(Key2, C2).

C1 = Dec(Key2, D (Key1, C3)).

P = Dec(Key1, C1).

P = Dec (Key1, Dec(Key2, C2)).

P = D (Key1, Dec(Key2, Dec(Key1, C3))).

The original DES symmetric encryption fashion used 56- bit keys, which were inadequate to cover against practical brute force assaults. The operation of three separate DES keys for a total crucial length of 168 bits is specified by Triple DES. Although the key length of Triple DES makes it more secure against brute force attacks, it was vulnerable to meet-in-the-middle assaults since it relied on consecutive encryption processes, as discussed in a prior piece. Because of DES's quick key length, 3DES changed into created as a extra steady volition. The DES set of rules is completed

3 instances with 3 distinct keys in 3DES, nonetheless it is best taken into consideration steady if 3 distinct keys are utilized.

6. Results

The results of this work would be like after encrypting the image it displays as image encrypted successfully. If we try to open the original image after encryption the image will be displayed as empty.it means that the information in image is hidden. After the decryption process is done with the same keys which are used for encrypting process, the original image and the contents present in the image are displayed clearly.

7. Conclusion

In this paper, Image Encryption and Decryption using AES algorithm is implemented to secure the image data from an unauthorized access. A Successful implementation of symmetric key AES algorithm is one of the best encryption and decryption standard available in market. With the help of MATLAB coding implementation of an AES algorithm is synthesized and simulated for Image Encryption and Decryption. The original images can also be completely reconstructed without any distortion. It has shown that the algorithms have extremely large security key space and can withstand most common attacks such as the brute force attack, cipher attacks and plaintext attacks.

8

[20].

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] _Hardware_Implementation_of_Triple-DES_EncryptionDecryption_Algorithm.

[2] R. Pich, S. Chivapreecha, J. Prabnasak, A single, triple chaotic cryptography using chaos in digital filter and its own comparison to des and triple des, 2018 Int Work Adv Image Technol IWAIT, 2018. 2018;(4):1–4..

[3] Sujatha BR, Satyanarayana M V. I Mproved NEtwork Connectivity. October. 2009;1(3):1–8.

[4] M. Srivastava, H.M. Singh, M. Gupta, D. Raj, Digital watermarking using spatial domain and triple des, in: Proc 10th INDIACom; 2016 3rd Int Conf Comput Sustain Glob Dev INDIACom, 2016, 2016,, pp. 3031–3035.

[5] P.K. Naskar, A. Chaudhuri, A. Chaudhuri, Secure symmetric image encryption based on linear geometry, Proc - Int Conf 2014 Appl Innov Mob Comput AIMoC (2014, 2014,) 67–74.

[6] S. Gajewski, M. Sokol, M. Gajewska, Data protection and crypto algorithms' performance in RSMAD, IEEE Veh Technol Conf. (2011).

[7] W. Guo, Z. Li, Y. Chen, X. Zhao, Security design for instant messaging system based on RSA and triple DES, in: Proc 2009 Int Conf Image Anal Signal Process IASP, 2009, 2009,, pp. 415–418.

[8] M. Usama, M.K. Khan, Classical and chaotic encryption techniques for the security of satellite images, IEEE- Int Symp Biometrics Secur Technol ISBAST'08. (2008).

[9] S. Wee, J. Apostolopoulos, Secure scalable streaming and secure transcoding with JPEG-2000, IEEE Int Conf Image Process. 1 (2003) 205–208.

[10] Thushitha VR. Comparative Analysis to Improve the Image Accuracy In Face Recognition System Using Hybrid LDA Compared With PCA. 2022;

[11] F. Antonios, N.S. Petrakis, P. Margaronis, E. Antonidakis, Hardware Implementation of Triple-DES Encryption /, Decryption Algorithm. (2006; (January).).

[12] 64_2017_3620_MOESM21_ESM.

[13] D. Suster, M. Michal, H. Huang, S. Ronen, S. Springborn, M. Debiec-Rychter, S.D. Billings, J.R. Goldblum, B.P. Rubin, M. Michal, S. Suster, A.C. Mackinnon, Myxoinflammatory fibroblastic sarcoma: an immunohistochemical and molecular genetic study of 73 cases, Mod Pathol 33 (12) (2020) 2520–2533.

[14] A. Vijayaraj, N. Velmurugan, Limited Speech Recognition For Controlling Movement Of Mobile Robot, International Journal of Engineering Science and Technology 2 (10) (2010) 5275–5279.

[15] Pathology. 2020. p. 2520–33.

[16] https://www.ibn.com/doces/en/zos/5.1.0?topic=operation-triple-des-encryption.

[17] https://pycryptodome.readthedocs.io/en/latest/src/cipher/des3.html.

[18] S. Avudai Selvi & A. Vijayaraj " Increasing quality of service in video traffic using zone routing protocol in wireless networks" , 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) , DOI: 10.1109/STARTUP.2016.7583929.

[19] https://github.com/Vatshayan/Image-Security-by-Triple-DES-Final-YearProject/blob/main/README.md.

[20] https://www.geeksforgeeks.org/encrypt-and-decrypt-image-using-python/.

[21] A. Vijayaraj, U., Sudharshana " Construction of routing tree and node discovery in wireless networks", in: IEEE International Conference on Communication and Signal Processing, 2014, https://doi.org/10.1109/ICCSP.2014.6950103.

[22] , Improved Key Generation Scheme of RSA (IKGSR) Algorithm Based on Offline Storage for Cloud vol 645 (2018), https://doi.org/10.1007/978-981-10-7200-0_31.

[23] P. Chinnasamy, P. Deepalakshmi, HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud, J Ambient Intell Human Comput 13 (2) (2022) 1001–1019, https://doi.org/10.1007/s12652-021-02942-2.

[24] P. Chinnasamy, P. Deepalakshmi, "A scalable multilabel-based access control as a service for the cloud (SMBACaaS)".Transactions on, Emerging Telecommunications Technologies 29 (8) (2018) e3458, https://doi.org/10.1002/ett.3458.