ECTI Transactions on Computer and Information Technology
Journal homepage: https://ph01.tci-thaijo.org/index.php/ecticit/
Published by the ECTI Association, Thailand, ISSN: 2286-9131

A New Security Mechanism for Secured Communications Using Steganography and CBA

Abdul Aziz A B[1], Aman Gupta[2] and Sannasi Ganapathy[3]

ABSTRACT

The quick advancement of computerized information trade has caused data security to be of much significance in information transmission. As a huge measure of information is sent over the Internet, it is fundamental to protect the data from hackers. The current trend is to use AES for safeguarding the data from hackers. Even though, the AES is most frequently used encryption, but it has the disadvantage of employing several direct multi-variation conditions. Hence, it may be broken utilizing mathematical cryptanalysis. Because AES was once considered to be fairly powerful, it has been employed in a variety of encryption schemes, posing a serious threat. This paper proposed a 128-digit key cross breed algorithm (CBA-128) based on AES and DES for enhancing the security and also applies steganography-based encryption to increase the security of the data during data transmission over the network. The proposed model provides more security for the data to prevent unauthorised access. The experiments conducted to prove the efficiency and effectiveness in terms of security level and time.

Article information:

Keywords: DES, AES, Stenography, Cryptography, Cross Breed Cipher

Article history:
Received: January 30, 2022
Revised: June 17, 2022
Accepted: September 24, 2022
Published: October 29, 2022 (Online)

DOI: 10.37936/ecti-cit.2022164.247373

1. INTRODUCTION

The cryptographic is designed to decode and understand information matrix made up of 64 components that are levelled from a 64-digit key. The Advanced Encryption Standard (AES) is a cryptographic standard having a 128-cycle block size having code lengths of 128, 192 and 256 bits approximatively. Generally, the text, image, sound, and video input modalities are more secure when AES and DES are used together. The existing works identify the possible flaws in the standard AES encryption method, notably in the context of logarithmic-based cryptanalysis. Combining AES with DES is recommended for limiting the logarithmic attacks on AES. As a result, work on the Half breed AES-DES computation has been done. Inducing the beauty of stenography in the hybrid cipher algorithm (Kumar et al 2022) has brought in an additional layer of security over to the data. The newly developed enhanced AES is ensured the secured data encryption and transferred to the receiver from the sender to receiver without any interception.

The Data Encryption Standard (DES) is a matrix code computation that uses a sequence of complex methods to convert a fixed-length line of plaintext bits into another code text bit line of equal length. The matrix size is 64 bits due to DES. DES includes a key that may be used to reverse the change that allows the key to be decoded by the same client that encoded it. Even though, the key includes 64 components in which only 56 are used in the computation process. Before being removed, eight pieces are utilized to check for equality. As a result, the persuasive key length is 56 bits. The chosen key's eighth component is removed and leaving with the 56-bit key which corresponds to locations such as 8, 16, 24, 32, 40, 48, 56, 64 of the 64-cycle keys.

The Advanced Encryption Standard (AES) relies on a design rule known as a replacement stage organization. Unlike their progenitors, DES and AES don't use a Feistel structure. AES does have a set structure of 128 bits as well as a critical dimension of

[1,2] The authors are with School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India., E-mail: abdulaziz.ahamed2020@vitstudent.ac.in and aman.gupta2020@vitstudent.ac.in

[3] The author is with Centre for Cyber Physical Systems & School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India., E-mail: sganapathy@vit.ac.in

[3]Corresponding author: sganapathy@vit.ac.in, Ph: 91 9488869712

128, 192, or 256 bits, whereas Rijndael may be specified using blocks of either 32 bits or at least 128 bits. The square dimension has an upper length of 256 bits. AES works as a 4×4 section significant demand lattice containing bits. This is called a state version of the well-known Rijndael, having larger matrix dimensions, including proprietary sections within data. The majority of AES computations are performed in a single field. The AES is generated as different variations of changes that transform the original data into the final product of coded text. Each cycle includes several handling stages, one of which depends on the secret keys. A lot of reverse cycles are performed to convert figure data into the original text once again by applying a suitable private key. The block length of an AES shows the total quantity of rounds of changes that transform the original data into the encrypted data as final output is known as code text.

A cross breed cryptography combines with two cryptography systems such as asymmetrical and symmetrical. The terms "speed" and "security" are used to describe these aspects individually. The cross-breed encryption is one of the safe cryptography techniques which provides the secured secret keys. Moreover, it combines the convenience of a topsy-turvy cryptography system also with the feasibility of a block cipher method. The encryption key is used in symmetric cryptography to perform the encryption process. At a certain moment, the beneficiary uses the cryptography method to decrypt the ciphertext. After recovering the ciphertext, it is used to decode the encrypted messages.

A combination of cryptographic techniques has a variety of advantages. The first is the establishment of an affiliation connection among two client hardware configurations. Users may communicate through cross-breed encryption. Unbalanced cryptography may impede cryptography interaction. Nevertheless, two types of encryptions are performed when cryptography is used concurrently. As a result, the communication interaction is more secure and improved the performance of the applications. Picture Cryptology relates to the procedure of concealing data within a photographic file. This image selected in the design that gets referred to as a profile photo and the image which are obtained after referred image as stego image by a steganographic algorithm. Here, an image is handled in memory as an A*B as greyscale images or A*B*3 as shading images grid. Moreover, each segment of the images is addressing the energy worth of just a unit.

The text is fixed inside an image using image steganography by altering the upsides of some bits chosen via an encrypt calculation. The recipient of the image should be aware of an identical computation in order to determine what pixels must be used to split the information. Cryptography is the use of numerical concepts as well as a collection of regulation computations known as estimations to alter communications in hard-to-decipher ways. These predictable computations are used to perform encryption in key generation, enhance the branding, validate the data privacy, browse in online and maintain the confidentiality over the stored documents. There are four main objectives for cryptography such as secrecy, respectability, non-disavowal and validation.

Many security mechanisms are available for maintaining the security in different market segments, financial services, media, and government sectors. Among them, the AES is widely used to perform encryption process that protects the stored and transmitted data from unauthorised third-party access. The hybrid cryptographic algorithm is developed for providing highest security and also to execute the hardware and software implementation quickly. Moreover, any encryption technique able to incorporate as a software in hybrid cryptographic algorithm for protecting the data in transmission and storage. The Hybridized cryptographic technique is used in the various fields including financial sectors, business for sharing the sensitive data and the public networks to send emails and ATM-based transmission lines. Here, the secret keys are to be available readily after performing the encryption process. To fulfil the current needs, a new steganography-based encryption technique incorporated cross-breed algorithm is proposed in this work. The major contributions of this paper are as follows:

i. To use a 128-digit key size based crossbred computational method for enhancing the data security.
ii. To develop a 128-digit key crossbreed-based AES and DES computation method to provide the strong security to the data in data communication process.
iii. To apply a new steganography-based encryption technique to enhance the data security during the data transmission in networks.
iv. To provide more complexity to break the security in network and also prevent the malicious activities in data communication process.

Rest of this paper is organized as below: The related works have been discussed in detail in section 2. In section 3, an overall system architecture is developed and explained the workflow of the proposed model diagrammatically. Section 4 explains the proposed model with proper explanation. Section 5 demonstrated the performance of the proposed model through experimental results and comparative analysis. Section 6 concludes the work by highlighting the contributions with quantitative achievement and future directions.

2. LITERATURE SURVEY

Many cryptographic algorithms have been developed for securing the data in transmission and storage by different researchers in the past. Among them, Zeghid et al (2007) discussed the AES and also considered a key generator into AES for ensuring the enhanced performance of encryption. They proved that their model performed better than the standard AES. Kun et al (2009) developed a new encryption method that is the combination of chaos theory along with AES. The performance of AES is increased by increasing the key space and the non-linear factors. Li et al (2010) analyzes the AES algorithm and also developed a S-box structure incorporated AES for performing encryption process. The ECC algorithm is also applied along with forward and mix encryption method to improve the AES and ECC. Finally, the authors achieved high speed and security. Ali and Masrom (2010) developed a new security mechanism for protecting the data from any attacks that applies the authentication and encryption processes. Sara and Nijad (2012) proposed a Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform. They have proved that their algorithm is best when it is compared with existing works.

Ankush and Pallavi (2016) proposed a cryptographic scheme that can transform a secret image into any number of shares as per the user's needs and provide more image security. Pratiksha and Kapoor (2016) developed a new architecture to hide the data in image using steganography with the incorporation of genetic algorithm and cryptographic algorithms. They have achieved better security level than the existing system. Surinder (2017) had extensive research on the study of Multi-Level Cryptography Algorithms: Multi-Prime RSA and DES. They have calculated average values for each parameter by applying various prime numbers that are considered in their work and also demonstrated using tables and graphs. Finally, they have concluded their method as better in terms of accuracy. Milad et al (2017) developed a new integer wavelet transform aware steganography method for digital images. Their method is also incorporating a chaotic map that is enhanced as a modified logistic map that is capable of increasing the key size and security. Their method is proved as better than the existing systems in terms of PSNR rate. Jyoti et al (2019) suggested the fact that security of the scheme critically depends on a shared key and the sum of shares required for regeneration of the secret image. Milad et al (2019) developed a new 3-D sine chaotic map aware steganography method for performing the extraction and increasing the security level. They have compared with existing methods and proved that their method as better in terms of security level and robustness.

Kavin and Ganapathy (2020) developed a new secured data storage mechanism to provide the security on cloud with IoT environment. Their mechanism applies elliptic curve and Diffie-Hellman for performing encryption and decryption process effectively. They have proved their system as better than other models in terms of time and security level. Peyman et al (2020) designed a new algorithm called a digital image encryption algorithm that work based on the chaos game. The evaluation results of their algorithm are proved as an efficient and robust against the attacks. Kavin et al (2020) developed a new security framework to store the cloud user's data securely in cloud database and also access them securely. Their framework incorporates the ECC for performing encryption process, access control mechanism for ensuring the users authenticity and LDSA for effective secured access. Finally, they have proved that their framework is better when it is compared with existing systems.

Peyman et al (2021) developed a new secured video watermarking system using a new map that is a two-dimensional complex map. They have analysed their system and proved the existence of chaos. Finally, their experimental results represent a chaostic characters in this chaotic map and proved that their system is better than the existing systems in terms of visual quality and attack resistance. Jinu Mohan (2021) made research on enhancing home security through visual cryptography. Pradeep et al (2021) developed a new Matrix Translation technique and ECC aware cryptosystem to ensure the secured data communications in the sensor networks. Aesha et al (2021) brought up a new cryptographic algorithm via a two-dimensional chaotic map. Suthanthiramani et al (2021) introduced a new secured storage and retrieval model by applying the ECC in cloud environment. Their model ensures the data security in cloud database and during the data communications between the cloud users. Kavin and Ganapathy (2021) proposed a new digital signature algorithm to ensure the data integrity by applying ECC. Their algorithm achieved better accuracy and security level than the existing techniques.

3. SYSTEM ARCHITECTURE

The proposed data security model is shown in figure 1 that consists of four components such as input data, encryption phase, decryption phase and output. Here, the input data contains the regular data what the users sent to the target user in the network. The data is to be encrypted by applying the standard encryption algorithms AES and DES with 128 bit cross breed method. The encrypted data is to be decrypted by using the decryption part of the AES and DES along with cross breed method. Finally, the data is accessed by the target user in the form of plain text.

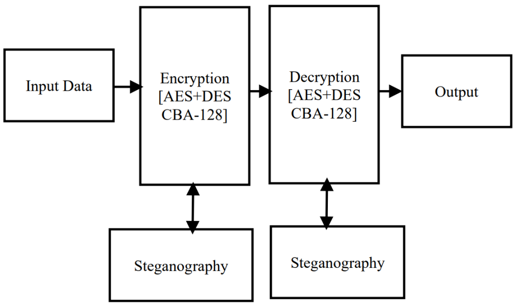

Fig.1: *System Architecture*

The steganography technique is also used in the proposed model for enhancing the security level during the data communication process in the network. Finally, the same set of methods have been applied for performing decryption process and get the original text from the input data which is in ciphertext format.

4. PROPOSED SYSTEM

This section explains the newly developed 128-digit key aware Cross Breed Algorithm (CBA-128) based Hybrid AES-DES for providing data security during communication and storage in the network. Generally, Feistel's work at IBM in the late 1960s and early 1970s gave birth to modern encryption. In 1977, the National Institute of Standards and Technology (NIST) adopted DES for encrypting unclassified data. The Advanced Encryption Standard (AES) is a new standard and it has taken the role of DES. Moreover, the DES is also linked to several difficulties including problem and solution spheres.

4.1 Problem Sphere

Even though, we discussed the various problems, DES isn't any longer safe for transmitting information throughout the business. With today's better frameworks, it is simpler to crack the code of DES computation. We can crack the DES in 8 hours using 600 million guidelines per subsequent. Additionally, if we believe that the performance of PCs will continue to get better, it will be possible to break the AES computation as well. As a result, we suggest a framework of a mixture calculation that is a combination of DES and AES. As a result, the security of both computations would be strengthened by this hybrid framework.

4.2 Solution Sphere

A computer network is a linked collection of self-governing the hubs that use unique, generally agreed-upon norms and indications identified as conventions that associate with one another and enable asset exchange ideally in a predictable and controlled manner. Correspondence has a major impact on various fields including finance related companies. This is desired for discussing sensitive information in a secure environment. Only with a fast chain of events of organizational innovation, online assaults are likewise adaptable. The traditional encryption calculations (single data encryption) aren't adequate for modern data privacy over the websites. Therefore, we offer this cross-breed Cryptography Algorithm. This is a strategy is transferring data more securely. Currently, many types of cryptographic computations provide excellent protection to data on networking, although there are a few disadvantages. The whole mixing computation is designed to improve security by combining DES and AES. The Least Significant Bit (LSB) algorithm is also applied in this work.

LSB: The Least Significant Bit (LSB) is a technique for embedding the secret messages into images. The image pixels are converted into binary form and the secret messages are to be converted as ASCII values in the form of binary values. In this technique, a least significant bit of image pixel is replaced with a binary value which is 1-bit of the secret image (Osunade and Ganiyu 2016). The LSB is used in steganography technique to hide the messages within an input image by replacing least significant bit of the image. Here, the bits of messages are hidden successfully by applying LSB. Moreover, it is possible to insert any secret message over the input image by changing the first right most bit of the image. But, the LSB is useful when the input file is bigger than the message file and it must be a grayscale image.

This framework is sound and complicated from the methods involved above, but it's actually quite viable and simple to implement. There are certain steps that are mentioned below to give an insight on implementing the framework that was planned. The proposed algorithm is capable of handling all kinds of input data including plain text. The steps of the Cross Breed Algorithm are as follows with implementation detail.

128 digits key based Cross Breed Algorithm (CBA-128)

Input: Plaintext

Output: The DES takes a contribution of 64-digit plaintext information block and 56-bit key (with 8 pieces of equality) and yields a 64-digit figure text block.

Step 1: The 8 equality pieces are eliminated from the key into its Key Permutation.
Step 2: It has 16 rounds of processes in which the raw data and the code keys are processed:
Generally, the input is given as 64-bit plain text to DES and it is converted into 64-bit cipher text with the help of 56-bit key value in a block which is also called as "64-digit figure text block".

The key is divided into two 28-bit parts.

1. Depending on the round, every half of both the code is shifted by either a slice or two.
2. The components are blended & rely on something like a Compression Permutation will reduce the code from fifty-six to forty-eight pieces. Each Compressed Code is then used to scramble the unencrypted block for the given cycle.
3. The critical essential components from stage two are used in the next one.
4. The data block is divided into 2 thirty-two-cycle halves.
5. The 50% of the data block is reliant around an Expanding Variation to grow to forty-eight pieces.
6. The stage six yield is restrictive OR-ed vague with stage three forty-eight-piece compressed code.
7. The yield for stage seven is handled by an S-box that replaces the crucial pieces thus reducing the forty-eight-piece component to 32 bits.
8. The yield for stage eight was determined by the use of a P-box to commute the pieces.
9. Every output including its P-box is carefully OR-ed only with the remainder of the block where information is procured.
10. There will be 2 information portions exchanged and the information for the next round.

Step 3: The end result of Sixteen modifications is the figure message.

Step 4: The associated code phrase would be an AES contribution.

The fifty-two 16-digit key sub-blocks that were created with the help of the 128-bit key can be delivered as follows:

i. To start with, we have a 128-cycle code, which is parcelled onto 8 16-digit sub-blocks which are used straightforwardly for the initial 8 code sub-blocks.
ii. The 128-bit code is moves consistently from one end. Furthermore, the resulting 128-bit block is further divided into 8 16-digit sub-matrices directly that are used as 8 key sub-blocks.
iii. The shifting mechanism for cycles shown is also repeated until all 52 of the 16-bit set of subs have been generated.

Step 5: To generate ciphertext, AES scores utilize the replacement or coupling of SP structure with many cycles. The number of iterations is determined by the size of the key. The key size is 128 pieces with 10 variations in cycle positions, and the key size is 192 elements with one of 12 levels and 258 levels. The key has 14 levels. However, since only one key is utilized in the computation process, all of these rounds need the usage of a rounded key that must be expanded to also include the keys for every round, starting with round 0.

The steps are as follows:

i. Replacement of the bytes: The bytes of the matrix content are substituted in the first stage based on the generated rules guided by preset S-boxes.
ii. Moving the lines: All columns in this progression are shifted by a step with the exception of the first column in the matrix.
iii. Blending the sections: The Hill figure is used in the third stage to mix-up the message by mixing the matrixes parts.
iv. Including the round key: In the last step, the text is XOR-ed only with a unique round key. These methods ensure that the final encrypted data is safe when applied many times.

Step 6: The encrypted ciphertext is passed on to the stenography process where it is embedded onto an image using the LSB algorithm of Image Steganography.

Thus, creating a triple layer security during the transmission of data has made the connection between sender and receiver more reliable and safer to transmit sensitive data during data communications. In this work, the decryption process is also done like encryption process by using the same algorithms that are used for performing encryption process.

Cryptanalysis: Cryptanalysis is used to understand the cryptosystems and also useful for enhancing the entire system by identifying the weak points and also to create a strong secret code. Moreover, this is used to ensure the data security in a system. The various scenarios such as i) write a program to hide any message in a file, ii) program to find the location of the signature in a file, iii) program to find a password of the file and the iv) program to find other hidden messages in a file. All these scenarios, the proposed model is useful for protecting the file content by applying the newly developed steganographic technique. Among them, a file content can be protected safely from attackers by safeguarding the password of the file by using the proposed steganographic technique successfully.

5. RESULTS AND DISCUSSION

The proposed model has been designed by using the C and Python programming. It requires a Laptop/Personal Computer with the configuration of i5-intel core processor and 1 GB RAM for implementing this model. Fig. 2 and 3 show the images before added the text and after add the text.

Fig.2: *Image before adding text .*

Fig.3: *Image afteradding text.*

A further developed Hybrid AES-DES calculation as a method for fortifying the current AES engineering. The half breed model outperforms the simple AES in terms of nonlinearity and all things considered, converged with DES there is better dissemination thus the probability of a mathematical assault on the half breed model is diminished. Likewise, the time shown on the examination is the standard time since the time may change based on processor accessibility and processing power. As a consequence of the same, one cannot get a different time for the same contribution for encrypting and decoding. In a framework like this, applying distinctive calculations like DES, AES, and Cross breed AES-DES for text, method of info. In this calculation, if the key isn't in a substantial organization, then a blunder report is produced. The key configuration is a mere 16-person key with 8, 4, 4 being the characters, numbers and uncommon characters respectively can be found for approval.

In this work, the input was of random paragraphs or text messages that are to be sent in a typical conversation from the sender to the receiver. The key refers to the set of agreed integers between the sender and the receiver for transcribing the messages so that the sender can send it to the receiver without the intentions of it being altered by a third party who does not have the key. The receiver, who has the key, will be able to get the message as intended by the sender.

Fig.4 demonstrates the encryption time analysis for the proposed technique by considering the various lengths of text is used as input.

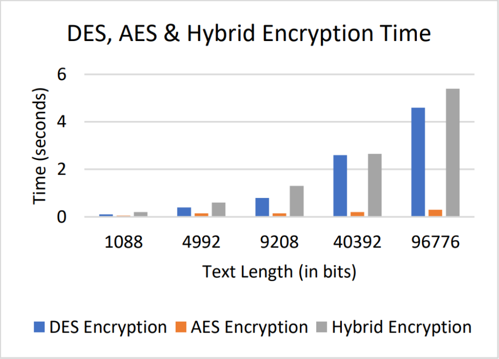

Fig.4: *Encryption Time Analysis.*

From the data, we can see that our hybrid cipher algorithm is performing not too bad with the encryption timing; considering the fact that it uses two algorithms at once. This has proven to improve the security of the transmission of data and making sure that we don't sacrifice much in terms of run time for the particular program. The reason for the better performance is the use of hybrid encryption algorithm and CBA.

Having the perks of more security and not too bad of a hit on the run time has given us a secured transmission for important and sensitive data. This is relatively quick and has a constant but gradual increase in the time taken to encrypt / decrypt the data. Which by the hair is quite minimal in differences and has quite astonishingly has improvised the rate of perpetual data transmission over the network in a secured and contemptuous manner that is looked upon the likes of the standard DES and AES where the secure nature was not observed as protensively as in the case of the newly enacted hybrid format. Which gets better with the implementation of a steganographic context-based algorithm in terms of the LSBs of the image pixels. Fig.5 demonstrates the decryption time analysis.

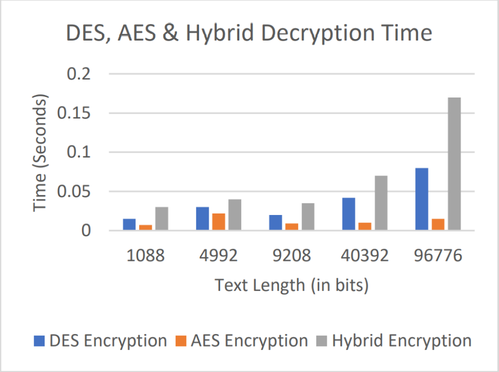

Fig.5: *Decryption Time Analysis.*

A similar scenario is viewed here, in this case, the decryption time is high; making it a proven fact that the hybrid algorithm makes a modest and secured algorithm, having increased the time of the decryption, making it harder for interpreting the data in foreign hands rather than getting it transmitted over to the receiver from the sender. Thus, proving the overall reliability of the system of transmission. Table 1 shows the time taken for performing steganography encryption and decryption on DES, AES and Hybrid.

Table 1: *Styles Summary.*

Text Length (in bits)	Stegano Encryption	Stegano Decryption
1088	24.25566983	5.303502274
4992	25.27515311	5.479101896
9208	25.45810771	5.472930431
40392	31.21945453	6.057295561
96776	39.23327327	7.199094772

Now, moving over to the steganography side, we have two sets of data, one being the senders' side and one from the receiver side. When the sender encrypts the data, it is found to take a larger amount of time for the progressively increasing order of the data transmission length. We can see that the encryption time is high whereas the decryption time increases over the course of action when the length in bits for the data meets a gradual upraise and surge in numbers.

Fig.6 shows the security level analysis between the proposed model and the standard algorithms such as AES, DES, Hybrid (AES+DES), LSB (Osunade and Ganiyu 2016) and AES+DES+LSB (Bindu et al 2021), LSB+AES (Kumar et al 2022), AES+ECC+LSB (Vandana and Kumari 2022) and RSA+Caesar Cipher+LSB (Sidi et al 2022). Five different experiments such as E1, E2, E3, E4 and E5 have been done for performing the comparative analysis by considering the various kind of same size of data are considered as input for these all five experiments.

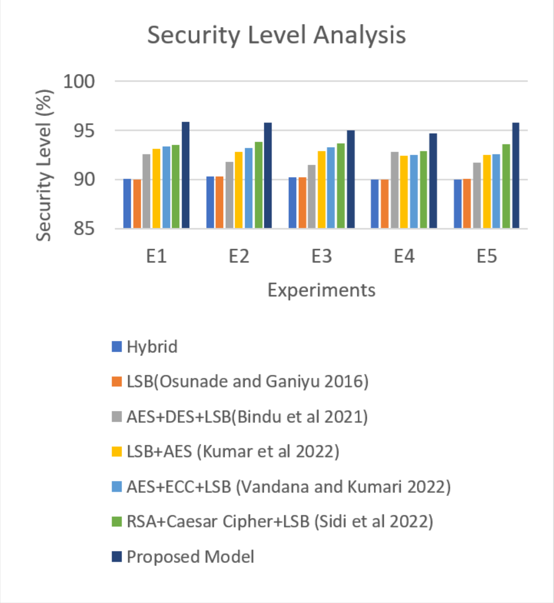

Fig.6: *SecurityLevel Analysis.*

From fig.6, it is proved that the betterment of the proposed model in terms of security level when compared with the existing works such as Hybrid (AES+DES), LSB (Osunade and Ganiyu 2016), AES+DES+LSB (Bindu et al 2021), LSB+AES (Kumar et al 2022), AES+ECC+LSB (Vandana and Kumari 2022) and RSA+Caesar Cipher+LSB (Sidi et al 2022). The reason for the enhancement is the incorporation of 128-bit CBA along with AES, DES and LSB.

6. CONCLUSION AND FUTURE WORK

As a method of enhancing the current AES architecture, a hybrid DES-AES algorithm with image steganography has been developed. The hybrid model has better nonlinearity than the standard AES. This is because it is integrated with DES and it has high distribution and also reducing the chance of an algebra form of attack. Moreover, the average time is provided in the analysis and it is depending on the availability and speed. Because, the same input is received for encryption and decryption many times. The algorithm will operate as an effective and trustworthy data encryption solution because it is a mix of two powerful encryption standards. A double key may also be used in the suggested method of strategy to protect itself from a linear form of cyber-attacks. For that particular situation, the cipher algorithm's security can be enhanced further. Moreover, an irrational number is incorporated into DES, and the AES algorithm is embedded inside the DES framework to enha1nce the security. The text input mode is used in this system to convert as binary and also feeding it into the system where encryption and decryption are applied. This hybrid algorithm is more powerful and safe by changing the number of loops in the encryption technique to match the level of security required. On the other hand, it decreases the number of iterations for obtaining lower security. In this work, we can alternatively use another algorithm to encrypt the data provided by the AES algorithm. Although, the inclusion of a third algorithm would enhance the security. As a consequence, it improves the data privacy, but it consumes more time to convert plain text to encrypted text than the hybrid method. Finally, the effectiveness or efficiency is very important for any kinds of applications. So that the security mechanism must balance the execution time and security. This work can be enhanced further with the introduction of enhanced light weight encryption method to provide security for any applications effectively with efficiency.

References

[1] P. C. Mandal, "Superiority of the Blowfish Algorithm," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no.9, pp. 196-201, 2012.

[2] B. AlBelooshi, E. Damiani, K. Salah and T. Martin, "Securing Cryptographic Keys in the Cloud: A Survey," *IEEE Cloud Computing*, vol. 3, no. 4, pp. 42-56, 2016.

[3] W. Stallings, "The advanced encryption standard," *Cryptologia*, vol. 26, No.3, pp 165–188, 2002.

[4] L. Adleman, R. L. Rivest, A. Shamir, and R. L. Rivest, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *ACM*

Communications, vol. 21, no. 2, pp.120-126, 1978.

[5] Sunil k. Makar, Sombir Singh, and Dr. Sudesh Kumar, "Enhancing the Security of DES Algorithms Using Transposition Cryptography Techniques," *International Journal of Computer Science and Software Engineering*, vol. 3, no. 6, pp. 464-470, 2013.

[6] Y. Kun, Z. Han and L. Zhaohui, "An Improved AES Algorithm Based on Chaos," *2009 International Conference on Multimedia Information Networking and Security*, pp. 326-329, 2009.

[7] X. Li, J. Chen, D. Qin and W. Wan, "Research and realization based on hybrid encryption algorithm of improved AES and ECC," *2010 International Conference on Audio, Language and Image Processing*, pp. 396-400, 2010.

[8] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A Modified AES Based Algorithm for Image Encryption," *World Academy of Science, Engineering and Technology*, vol. 27, pp. 206-211, 2007.

[9] A. H. Ali and M. Masrom, "Analysis and implementation of security algorithms for wireless communications," *2010 The 2nd International Conference on Computer and Automation Engineering (ICCAE)*, pp. 430-434, 2010.

[10] E. Biham, A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," *Journal of Cryptology*, vol.4, no. 1, pp. 3–72, 1991.

[11] O. O. Khalifa, M. R. Islam, S. Khan and M. S. Shebani, "Communications cryptography," *2004 RF and Microwave Conference, RFM 2004. Proceedings*, Selangor, Malaysia, pp. 220-223, 2004.

[12] P. Suthanthiramani, S. Muthurajkumar, G. Sannasi and K. Arputharaj, "Secured data storage and retrieval using elliptic curve cryptography in cloud," *Int. Arab J. Inf. Technol.*, vol. 18, no. 1, pp. 56-66, 2021.

[13] S. Pradeep, S. Muthurajkumar, S. Ganapathy and A. Kannan, "A Matrix Translation and Elliptic Curve Based Cryptosystem for Secured Data Communications in WSNs," *Wireless Personal Communications*, pp.1-20, 2021.

[14] B. Prabhu Kavin and S. Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications," *Computer Networks*, vol. 151, pp. 181-190, 2019.

[15] B.P. Kavin and S. Ganapathy, "A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves," *Int. Arab J. Inf. Technol.*, vol. 18, no. 2, pp. 180-190, 2021.

[16] B.P. Kavin and S. Ganapathy, "EC(DH)2: an effective secured data storage mechanism for cloud based IoT applications using elliptic curve and Diffie-Hellman," *International Journal of Internet Technology and Secured Transactions*, vol. 10, no.5, pp. 601-617, 2020.

[17] B. P Kavin, S. Ganapathy, U. Kanimozhi and A. Kannan, "An enhanced security framework for secured data storage and communications in cloud using ECC, access control and LDSA," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1107-1135, 2020.

[18] A. V. Dahat and P. V. Chavan, "Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space," *Procedia Computer Science*, vol. 78, pp. 563-570, 2016.

[19] P. Sethia and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography," *Procedia Computer Science*, vol. 87, pp. 61 – 66, 2016.

[20] S. Kaur, P. Bharadwaj and S. Mankotia, "Study of Multi-Level Cryptography Algorithm: Multi-Prime RSA and DES," *International Journal of Computer Network and Information Security*, vol.9, pp. 22-29, 2017.

[21] S. Tedmori and N. Al-Najdawi, "Lossless Image Cryptography Algorithm Based on Discrete Cosine Transform," *International Arab Journal of Information Technology*, vol. 9, no.9, pp. 471-478, 2012.

[22] J. Mohan and R. R, "Enhancing home security through visual Cryptography," *Microprocessors and Microsystems*, vol. 80, no.103355, pp. 1-13, 2021.

[23] A. Elghandour, A. Salah and A. Karawia, "A new cryptographic algorithm via a two-dimensional chaotic map," *Ain Shams Engineering Journal*, vol.12, no.2, pp.1-14, 2021.

[24] M. Y. Valandar, P. Ayubi and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *Journal of Information Security and Applications*, vol.34, no. 2, pp. 142-151, 2017.

[25] M. Y. Valandar, M. J. Barani, P. Ayubi and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimedia Tools and Applications*, vol.78, pp. 9971–9989, 2019.

[26] P. Ayubi, M. J. Barani, M. Y. Valandar, B. Y. Irani and R. S. M. Sadigh, "A new chaotic complex map for robust video watermarking," *Artificial Intelligence Review*, vol.54, pp.1237–1280, 2021.

[27] P. Ayubi, S. Setayeshi and A. M. Rahmani, "Deterministic chaos game: A new fractal based pseudo-random number generator and its cryptographic application," *Journal of Information Security and Applications*, vol.52, no. 102472, pp. 1-16, 2020.

[28] O. Osunade and I. A. Ganiyu, "Enhancing the Least Significant Bit (LSB) Algorithm for

Steganography," *International Journal of Computer Applications*, vol. 149, no. 3, pp. 1-8, 2016.

[29] K. P. B. Madavi and P. V. Karthick, "Enhanced Cloud Security using Cryptography and Steganography Techniques," *2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON)*, pp. 90-95, 2021.

[30] M. Kumar, A. Soni, A. R. S. Shekhawat and A.Rawat, "Enhanced Digital Image and Text Data Security Using Hybrid Model of LSB Steganography and AES Cryptography Technique," *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, pp. 1453-1457, 2022.

[31] K. Vandana and S. K. Kumari, "Improving Security with Efficient Key Management in Public cloud using Hybrid AES, ECC and LSB Steganography comparing with Novel hybrid Cube Base Obfuscation," *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, pp. 1-6, 2022.

[32] E. V. Sidi, I. Diop and K. Tall, "A New hybrid approach of Data Hiding Using LSB Steganography and Caesar cipher and RSA algorithm (S-ccr)," *2022 International Conference on Computer Communication and Informatics (ICCCI)*, 2022, pp. 1-4, 2022.

Abdul Aziz A.B is studying B.Tech Computer Science and Engineering with a Specialization in AI & Robotics at Vellore Institute of Technology, Chennai, India. His areas of interest include network security, cryptography, steganography and Artificial Intelligence.

Aman Gupta is studying B.Tech Computer Science and Engineering with a Specialization in AI & Robotics at Vellore Institute of Technology, Chennai, India. His areas of interest include network security, cryptography, steganography and Artificial Intelligence.

Sannasi Ganapathy is working as an Associate Professor, Centre for Cyber-Physical Systems & School of Computer Science and Engineering, at Vellore Institute of Technology, Chennai, India. He has received his M.E and Ph.D degrees in Computer Science and Engineering from Anna University, Chennai, India. He has 15 years of teaching and research experience. He has published more than 100 research papers in reputed journals and conferences. He has been shortlisted as one of the Top 2% of scientists in the world as per the Elsevier-Stanford University Survey. His areas of interest include data analysis, network security, blockchain technology, and cryptography.