Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7- Issue 1, January 2024
Paper : 99

FPGA Implementation of Combined Cryptography and Steganography to Achieve Enhanced Security

Tinu Thomas
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Amritapuri, India
tinuthomas199613@gmail.com

Anu Chalil
Department of Electronics and Communication Engineering
Amrita Vishwa Vidyapeetham
Amritapuri, India
anuchalil@am.amrita.edu

***Abstract*—In todays emerging world data transfer across internet is very frequent. Security of such data being transferred is really important.There are situations where confidential information has to be transferred and that needs extra security. The technologies and algorithms available to provide security to these data are collectively known as Cryptography. Cryptographic techniques are used for security of data. The 2 main processes of Cryptography are Encryption at sender end and Decryption at receiver end. The process of encrypting the input message to ensure secure transfer is Encryption'. Decryption is the process of getting back the original message from the encrypted message. AES is an acronym for Advanced Encryption Standard. It is the most widely used and highly secure symmetric cryptographic algorithm. The main advantage of AES algorithm is its large key size which definitely contributes to the strength of encryption and thus making the data transfer more secure. The sender as well as receiver uses the single one key for encryption and decryption respectively. Steganography is a technique that helps to provide additional layer of security by hiding one form of data in another form. A text data can be hided inside an image and transmitted with the help of this technique. Here we are implementing the well known algorithm called AES in Verilog which is used for encrypting and decrypting data and analyse the security provided and to analyse the efficiency or power consumption to see if any improvement can be done. Here we also provide one more layer of protection by combining a technique called Steganography with the AES encryption and decryption.**

I. INTRODUCTION

In the modern era, the most celebrated word is digital. Everything is getting digitalized day by day. From buying goods from grocery shops to large banking transactions, interacting with people, even consultation with doctors are relying on internet these days. Internet and online data transfer have taken a strong control on the human livelihood and so the data getting transferred over internet need to be secured. Data security stands as an important pillar as different kinds of data including personal data comes into picture. Cryptography and Steganography are two important techniques that help to provide data security. Cryptography is used to secure the data by utilising encryption at the sender end before transmission and decrypting at the receiver to collect original data after transmission. There are a wide variety of cryptographic techniques that helps in ensuring data security. The most widely used and strongest among them is the cryptographic technique using the AES algorithm for encrypting and decrypting data.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7- Issue 1, January 2024
Paper : 99

This algorithm is a symmetry based cryptographic algorithm whose strength depends on the larger key size. Steganography is also a technique which helps to protect the data while trans- ferring. It hides the data to be transferred in any multimedia element like text, image, audio etc. So, at sender side the secret message will be hided inside an image (audio or text) and transmitted. At the receiver part, the secret information is retrieved. In this method, third party will not be aware of the actual data getting transferred. This enhances the security of the data as it is much required as evident from [13]. We are using the LSB method for steganography where the LSB values of the image pixels are changed with message. So here we propose to implement AES algorithm followed by Steganography in FPGA in view of providing double layer protection to the data that is transferred across internet with reduced resource utilisation and delay.

II. Literature survey

[1] This research paper is based on a survey on a wide variety of attacks to cryptanalytics of AES. Some of the attacks discussed here are: -force attack
In this type, the hacker works hard to identify the key used by trying out all possible combinations. Due to the larger key size AES algorithm stays resistant to these attacks. only attack this type, the third party has full awareness about all the encrypted information which was encrypted by a particular key. From all the encrypted messages attacker tries to figure out the key used and thus steals the original data. Authors says that strategically analysed ciphers are less prone to these attacks and hence AES algorithm is stronger against this attack. Authors have also analysed various other attacks like side channel attack, power analysis attack, differential fault analysis attack etc. From all the analysis they have arrived at a conclusion that AES will survive against these for a longer period of time.

[2] This paper portraits a comparable study of the mostly used cryptographic algorithm like Data Encryption Standard (DES), Triple DES (3DES) also known as Triple Data Encryp- tion Algorithm (TDEA), and Advanced Encryption Standard (AES). The authors have already compared these algorithms based on their performance in terms of their how better it secures data, time for encryption and throughput. From the analysis done on the various algorithm on varying types of

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7- Issue 1, January 2024
Paper : 99

data, the authors conclude that AES algorithm is the best. AES is the strongest algorithm due to its larger key size. It is stronger, provides higher throughput and takes less time.

[3] This paper implements AES algorithm with reduced delay and improved resource utilisation. They have achieved it when earlier Sbox was replaced in AES algorithm with an S box formed by combining MUX and LUTs. This reduced the complexity and also delay was improved as values were pre computed and stored in LUTs. This paper summarizes that the complexity of S-box can be reduced by pre-computing the values and keeping it in LUTs and they can be accessed as per requirement using a MUX.

[4] This paper uses both the techniques namely, cryptography, Steganography to provide 2 layer of secureness by using an XOR operation for encryption and embedding cipher data in to image using a preselected key. The authors have managed to create a web based application that can give users the access to make use of proposed method for data transmission. The authors claim that extra security is added by combining cryptography and steganography and it becomes cumbersome for a 3rd party to interrupt the secure data transmission.

In some works [10], authors have implemented cryptography with error detection based on parity so that possible errors can be detected without extra hardware involved in it. [9] deals with the implementation of AES algorithm in detail.

III. Cryptography and Steganography

Nowadays, the field of information and communications has developed in a great way such that data security has become a major challenge. The world grows countlessly and we have internet connectivity provided at each and every corner of the world including remote areas. The dependence on internet starts from paying bills on normal grocery shops to large banking transactions, booking appointments with doctors and many more areas. The large amount of data transfer happening over internet on multiple domains cannot be left as such and a high level of security need to be ensured. The computer networks and online platforms should be secured to make sure that it maintains data authentication, privacy and integrity.

A. Cryptography

Cryptography is a learning of techniques of secure communications. It allows only the sender and correct recipient of the message to see its contents. It is an important and inevitable tool that helps in securing data of sensitive nature. Thus the major intention or functionality of cryptography techniques is to maintain the privacy and secureness of data. Basically in cryptography, the data security is ensured by converting it into cipher text before transmission and retrieving back the original data at the receiver point. It makes use of wide variety of similar algorithm for this purpose. Cipher text is nothing but the encrypted or scrambled version of the original text and none other than the intended user will be able to decode it and understand. There will be some key utilised in the algorithms to cipher the original data and that key would be available

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7- Issue 1, January 2024
Paper : 99

with the intended user to decode it. This helps in prevent- ing the unauthorized access to the information. The actual meaning of cryptography can be understood from its name itself where crypt means hidden and graphy means writing. Thus cryptography means hidden writing. Cryptography is broadly classified into three types: Symmetric key (private) cryptography, (Public key) Asymmetric cryptography, Hash functions.

1) Private key cryptography: The symmetric key cryptog- raphy is also called as private key cryptography as its key info will be available with only the sender and receiver. It uses same key at sender side for encryption as well as at the receiver end for decryption. This type of cryptographic methods are simpler and gaster. The only challenge is to transfer the key securely to the receiver. Algorithms following this type of cryptography are Data Encryption Standard (DES), Advanced Encryption Standard (AES) etc.

2) Public key cryptography: Asymmetric key cryptography usee both private and public keys for encryption and decryp- tion. It is also called public key cryptographic technique as key is public at the sender end for encryption. By the term public itself it means that the key used for encryption is visible/available to everyone. But for decryption at the receiver end, a private key is used. It is known to the receiver (the person intended to receive the message) only. Thus although the key used for encryption is known to everyone only the authorised one with the key at receiver point (private one) can decrypt data and thus making it secure for data transfer.

3) Hash functions: Hash function will be used for many operating systems for encryption of the password. It doesnt involve any key for providing security. Instead, creates a hash value of fixed length based on the text and thus makes it impossible to recover the contents of the text. The various ap- plications of cryptography involve encryption of passwords, in case of digital currencies, data security during web browsing, authentication purpose, while using electronic signatures, end to end encryption etc. The most widely utilised and strongest cryptography algorithm is AES algorithm.

B. AES Algorithm

AES stands for Advanced Encryption Standard and it is the symmetric key cryptographic algorithmwhich uses same private key at both the sender and receiver for encryption and decryption respectively. AES algorithm is mostly used nowadays as it is very stronger comparing to other algorithms like DES, triple DES etc. due to its larger key size. The key size of AES algorithm can be 128 bits or 192 bits or 256 bits. It operates on 128 bit data and outputs same bits of cipher text. The AES algorithm is depicted in figure 1. AES algorithm performs operations on bytes of data. It mainly involves 4 operations, substitution, shifting rows, mixing columns and adding round sub key. These operations are repeated multiple rounds to generate the cipher data. The no. of iterations depend on the key size used for encryption and decryption as below:

- key, 128 bit : 10 iterations.
- key, 192 bit : 12 iterations.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7- Issue 1, January 2024
Paper : 99

- key, 256 bit : 14 iterations.

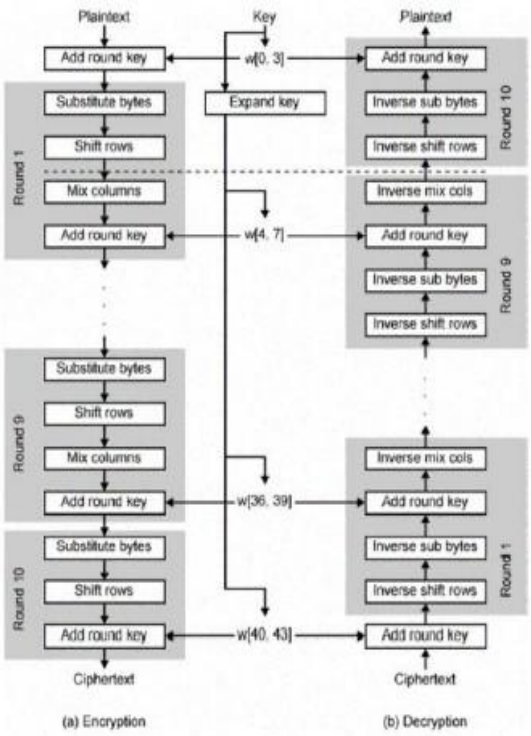

Fig. 1. AES Algorithm Flow Chart

AES considers the message data as block of 16 bytes in a column major arrangement as shown in figure2. Thus AES is also called as a block cipher algorithm.

```
[ b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]
```

Fig. 2. Column Major Arrangement of Input Data Bytes

The four main steps of AES algorithm are discussed below:

1) Substitution: This step involves substitution of each byte with a value from the S-box (substitution box). While doing substitution, the same value of incoming byte and complement of that is not used for substitution. Thus incoming 16 bytes of data are replaced with the substitution values from S-box. The S-box values are computed based on many complex calculations of multiplication and affine transformation. The complexity can be reduced by pre-computing these values store it in the LUT which can be accessed as required using a MUX.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7- Issue 1, January 2024
Paper : 99

2) Shifting rows: This is basically a permutation round where the rows are shifted. The 16 byte data is arranged in rows and columns. In this step, the 1st row only retained as such. The 2nd row cyclically shifted left by one, the 3rd shifted cyclically left by two and the 4th row shifted three. Thus it permutes bytes of data. This is then given to the mixing columns operation for further permutation. This is shown in figure 3.

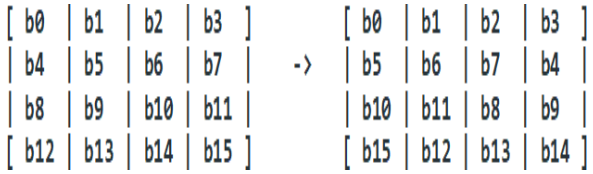

Fig. 3. Shifting of Rows

3) Mixing columns: This is yet another round of permutation where each column is performed with some mathematical calculation like matrix multiplication to form a new column that replaces the original bytes in the column. This round should not repeat in final round.

4) Round key addition: Now the matrix of bytes obtained from previous stage is considered as stream of 128 bots and XORed with the sub key. This sub key is a derived one obtained from original key 128 bit. A special key schedule algorithm is used to produce 11 different sub keys for the 10 rounds of operation and the initial addition of round key. These 4 operations are repeated for 10 rounds when 128 bit length key is used and then the cipher text is obtained. For the decryption at the receiver end, it follows the same operations by performing it in the reverse way to decode the original data from the cipher text. This is the basic working of the AES algorithm.

C. Steganography

Steganography is also a technique which is used to provide data security when it is getting transferred. This technique hides the data to be secured and transferred in some multimedia element like image, audio etc. The original data can be retrieved at the receiver end. Some authors [11] use image cryptosystems. Here we use steganography. There are many different ways by which steganography can be done. Among that the much used method is to hide the sensitive data in image and then transmit the image. Since the secret data is embedded into the pixels of the image, it will be very difficult for the attacker to detect the secret data. Watermarking is also considered as a form of steganography. It can considered as a trademark or method adopted by online publishers to recognize the source of files which are shared without permission. Addition of a steganographic layer after encryption adds onto the security of the data. The main advantage of steganography is that it helps to obscure the fact that some secret data is being transferred. Both cryptography and steganography are used for

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 7- Issue 1, January 2024
Paper : 99

ensuring security of the data being transferred. However, they differ in the way that, in cryptography, data is encrypted to a non-readable form. Everyone can sense the presence of data but cannot read it. But in steganography data I hided inside a cover object due to which only the receiver can sense the presence of original data. For all others it will be some other from which is the cover object. One of the steganographic technique used to hide the data in image is the LSB technique which is explained below.

1) LSB Method: LSB is the acronym for Least Significant Bit which is, the right mostbit with the lower index in a binary number. It is obvious from the name itself that LSB steganographic method is something to do with the LSB values. Thus in LSB steganography, the LSB values of the pixels of the image (or any other multimedia element) is replaced with the message to hide. This steganographic image is then transmitted. In conventional methods, the LSB values are replaced based on a key available and performing some calculations with the key and secret message to replace the LSB. This is complex and tiresome for a 3rd party to sense or deduce the secret message. But in proposed method, involvement of key has been eliminated in view of reducing the complexity and thus improving the resource utilisation. A simple example of LSB technique in proposed method is shown below. When applying LSB technique to every byte of 24-bit image, 3 bits can be embedded into each pixel.

Pixels:(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

A: 01000001 (secret message)

Result: (00100110 11101001 11001000) (00100110 11001000 11101000) (11001000 00100111 11101001)

IV. Implementation, Results

A. Proposed Work

The proposed work is intended to increase the security of data being transferred. Here, double layer security is provided by combining techniques called Cryptography and Steganography. Cryptography encrypts the original data to form the cipher text. The algorithm used for encryption in the proposed model is the AES algorithm which is resistant to many types of attacks as it uses a stronger key. AES is symmetry cryptographic algorithm which provides a better protection to data being transferred. The encrypted information is again protected by employing a technique called steganography where the encrypted message is hided inside the pixels of an image. The image can then be transmitted so that the attacker/hacker will not be aware of the actual data getting transferred and hence it adds to extra security layer. The LSB technique is employed here for steganography. According to the conventional LSB method, the LSB bit of the image pixels is altered to accommodate secret message based on the key used and some mathematical calculations. But in the proposed model, the LSB method is employed by just replacing the image pixels' LSB bits with the secret message data bits in view of reducing the complexity and thus improving the resource utilisation. At the receiver end the original cipher

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7- Issue 1, January 2024
Paper : 99

data(encrypted data) can be recovered from the image pixels and original message is retrieved after decryption using the same key used for encryption (by AES algorithm). Thus data can be transmitted more securely which is much more relevant in this digitalized era. Fig: 4 represents the proposed model block diagram and the expanded block diagram of steganography is shown in figure 5.

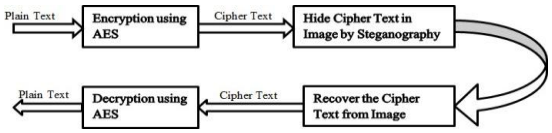

Fig. 4. Block Diagram of Proposed Work

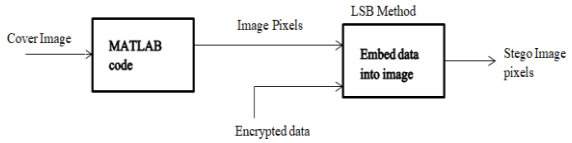

Fig. 5. Steganography

B. Results

The simulation outputs of encryption, decryption, steganog- raphy and combined cryptograpy and steganography are shown in the figures 6, 7, 8, 9, 10, 11 respectively. Encryption technique and Decryption technique is done for key size of 128, 192 and 256 bits. Simulation outputs of each as well as the combined simulation output is also shown.

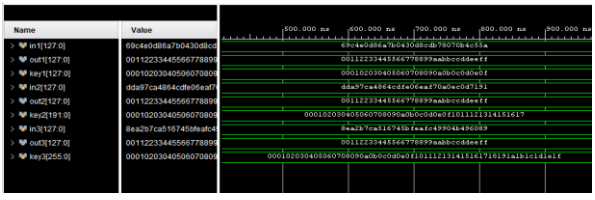

Fig. 6. Encryption

The schematic diagram is also obtained for the model which is shown in figure 12.

A 128 bit input data is provided along with keys of sizes 128, 192 and 256 bits to produce three different cipher texts of 128 bits length. This completes the encryption part. The pixels of the image generated through MATLAB is provided to the verilog code as input along with the encrypted cipher text to perform steganography and it created stego image pixels which can be reconstructed to image using MATLAB.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7- Issue 1, January 2024
Paper : 99

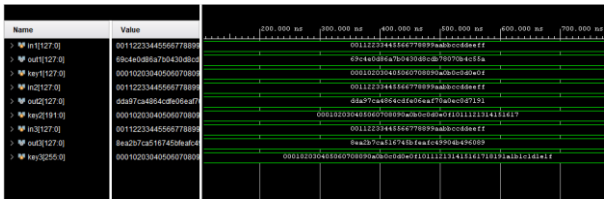

Fig. 7. Decryption

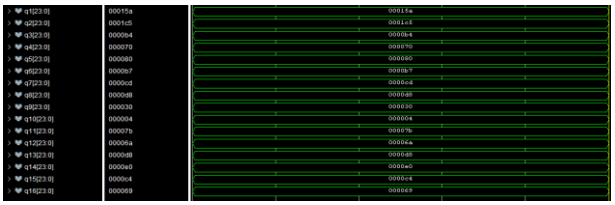

Fig. 9. Output After Steganography

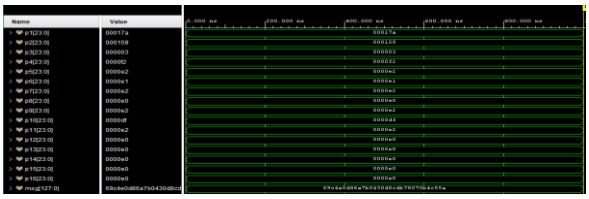

Fig. 8. Inputs to Steganography

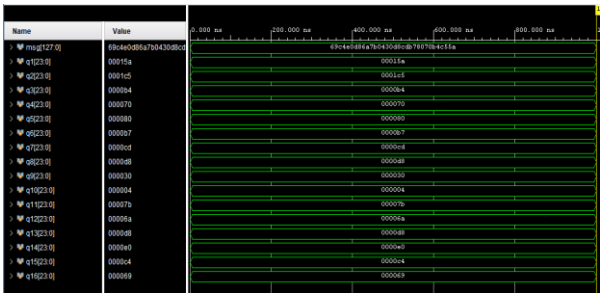

Fig. 10. Recovered Cipher Data from Stego Image

The encrypted text is recovered from steganographic image pixels at receiver end. Encrypted text is given as input to the decryption code along with the same keys as used for encryption. This outputs the original input data at the output. The comparison of resource utilisation of conventional method in [21] and proposed model is shown in Figure 13.

V. Conclusion and Scope for Further Research

This entire work is implemented in Vivado Design Suite. MATLAB was used to generate pixel values of the image which is used as the cover object for steganography. A model of combined cryptography and steganography has been proposed here in view of providing enhanced security. The complexity of LSB technique is reduced by eliminating the key thereby ensuring to improve the resource utilisation. The use of MUX and LUT based S-box reduced the delay of encryption and decryption.

Data security is an ever existing requirement and the techniques of cryptography and steganography provides a better solution for this. A double layer security is ensured here by combining cryptography and steganography. In order to obtain faster run time other algorithm like Blow fish can be used instead of AES, the implementation of which can be followed from [12]. The scope of further research lies in using making use of this model to encrypt image, audio and video data which is necessary in the digitalized world.

References

[1] Zodpe, H. and Shaikh, A., 2021. A Survey on Various Cryptanalytic Attacks on the AES Algorithm. International Journal of Next-Generation Computing, 12(2).

[2] Hamouda, B.E.H.H., 2020. Comparative study of different cryptographic algorithms. Journal of Information Security, 11(3), pp.138-148.

[3] Augustine, K.T. and Purushotham, U., 2021, October. Implementation of AES To Encrypt and Decrypt Speech Using LUT With Mux Gates. In 2021 International Conference on Advances in Computing and Communications (ICACC) (pp. 1-6). IEEE.

[4] Nunna, K.C. and Marapareddy, R., 2020, March. Secure data transfer through internet using cryptography and image steganography. In 2020 SoutheastCon (Vol. 2, pp. 1-5). IEEE.

[5] Shet, G.G., Jamuna, V., Shravani, S., Nayana, H.G. and Kumar, P., 2020. Implementation of AES Algorithm Using Verilog. JNNCE Journal of Engineering Management (JJEM), 4(1), p.17.

[6] Sunil, J., Suhas, H.S., Sumanth, B.K. and Santhameena, S., 2020, November. Implementation of AES Algorithm on FPGA and on software. In 2020 IEEE International Conference for Innovation in Technology (INOCON) (pp. 1-4). IEEE.

[7] Kumar, K., Ramkumar, K.R. and Kaur, A., 2020, June. A design implementation and comparative analysis of advanced encryption standard (AES) algorithm on FPGA. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 182-185). IEEE.

[8] Kalaichelvi, V., Meenakshi, P., Vimala Devi, P., Manikandan, H., Venkateswari, P. and Swaminathan, S., 2021. A stable image steganography: a novel approach based on modified RSA algorithm and 24 least significant bit (LSB) technique. Journal of Ambient Intelligence and Humanized Computing, 12, pp.7235-7243.

[9] Aparna, V.S., Rajan, A., Jairaj, I., Nandita, B., Madhusoodanan, P. and Remya, A.A., 2019, April. Implementation of AES algorithm on text and image using MATLAB. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1279-1283). IEEE.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7- Issue 1, January 2024
Paper : 99

[10] Dath, G.G., Chalil, A. and Joseph, J., 2018, October. An efficient fault detection scheme for advanced encryption standard. In 2018 3rd International Conference on Communication and Electronics Systems (ICCES) (pp. 99-103). IEEE.

[11] Nambiar, N.M., Rajewsari, P. and Lal, R., 2022, May. Fpga implementation of multibit lfsr as key generator for aes encryption. In 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 231-237). IEEE.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 7- Issue 1, January 2024
Paper : 99

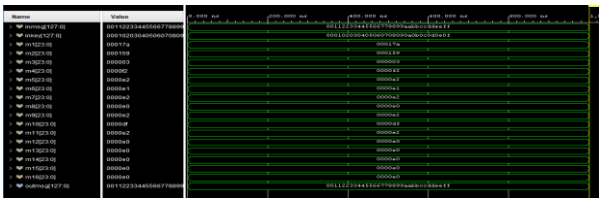

Fig. 11. Combined Cryptography and Steganography Output

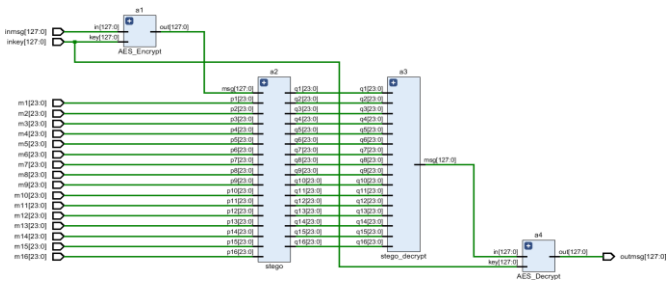

Fig. 12. Schematic Diagram

Resource Utilisation	Conventional Method (%)	Proposed Method (%)
LUT	17.44	14
IO	97.33	77

[12] Parvathy, P. and Ajai, A.R., 2020, July. VLSI implementation of blowfish algorithm for secure image data transmission. In 2020 International Conference on Communication and Signal Processing (ICCSP) (pp. 0770-0774). IEEE.

[13] Devika, K.N. and Bhakthavatchalu, R., 2022, April. VLSI implementation of crypto coprocessor using AES and LFSR. In 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 772-777). IEEE.

[14] Shashidhar, R., Mahalingaswamy, A.M., Kumar, P. and Roopa, M., 2018, December. Design of high speed AES system for efficient data encryption and decryption system using FPGA. In 2018 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT) (pp. 1279-1282). IEEE.

[15] Salim, P.T. and Vigneswaran, T., 2015. FPGA implementation of hiding information using cryptography. Indian Journal of Science and Technology, 8(19), pp.1-7.

[16] Saini, V. and Bangar, P., 2014. Design and implementation of advanced encryption standard algorithm-128 using verilog. International Journal of Engineering and Advantage Technology (IJEAT), 3(5).

[17] Mahmoud, M.M. and Elshoush, H.T., 2022. Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio SteganographyAn Innovative Approach. IEEE Access, 10, pp.29954-29971.

[18] Abood, E.W., Abdullah, A.M., Al Sibahe, M.A., Abduljabbar, Z.A., Nyangaresi, V.O., Kalafy, S.A.A. and Ghrabta, M.J.J., 2022. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics, 11(1), pp.185-194.

[19] Jan, A., Parah, S.A., Hussan, M. and Malik, B.A., 2021. Double layer security using crypto-stego techniques: a comprehensive review. Health and Technology, pp.1-23.

[20] Shifa, A., Afgan, M.S., Asghar, M.N., Fleury, M., Memon, I., Abdullah, S. and Rasheed, N., 2018. Joint crypto-stego scheme for enhanced image protection with nearest-centroid clustering. IEEE Access, 6, pp.16189-16206.

[21] Kurane, S., Harke, H. and Kulkarni, S., Text And Audio Data Hiding Using Lsband Dct Areview Approach. International Journal of Innovations in Engineering Research and Technology, pp.1-4.

[22] Elshazly, E.A., Abdelwahab, S.A., Fikry, R.M., Elaraby, S.M., Zahran, O. and El-Kordy, M., 2016. FPGA implementation of robust image steganography technique based on least significant bit (LSB) in spatial domain. International Journal of Computer Applications, 145(12), pp.43-52.

Fig. 13. Resource Utilisation Comparison

[23] Ahmed, A.M. and Nori, A.S., 2022, April. Improve Security Using Steganography and Cryptography Based on Smartphone Users Locations. In 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) (pp. 1-7). IEEE.
[24] Bansal, R. and Badal, N., 2022. A novel approach for dual layer security of message using Steganography and Cryptography. Multimedia Tools and Applications, 81(15), pp.20669-20684.
[25] Noorbasha, F., Cheruvu, J.H., Boina, P. and Battineni, S.V., 2021, February. Design of AES based Chiper and Decipher Cryptography System using Verilog HDL. In Journal of Physics: Conference Series (Vol. 1804, No. 1, p. 012170). IOP Publishing.