

DOI: 10.32604/csse.2023.041061

ARTICLE





Hybrid Dynamic Optimization for Multilevel Security System in Disseminating Confidential Information

Shahina Anwarul¹, Sunil Kumar², Ashok Bhansali³, Hammam Alshazly^{4,*} and Hany S. Hussein^{5,6}

¹School of Computer Science, University of Petroleum and Energy Studies, Dehradun, 248007, India

²Department of Computer Science, Graphic Era Hill University, Dehradun, Uttarakhand, 248001, India

³Department of Computer Engineering and Applications, GLA University, Mathura, India

⁴Faculty of Computers and Information, South Valley University, Qena, 83523, Egypt

⁵Electrical Engineering Department, College of Engineering, King Khalid University, Abha, 62529, Saudi Arabia

⁶Electrical Engineering Department, Faculty of Engineering, Aswan University, Aswan, 81528, Egypt

*Corresponding Author: Hammam Alshazly. Email: ha.alshazly@svu.edu.eg

Received: 09 April 2023 Accepted: 12 June 2023 Published: 09 November 2023

ABSTRACT

Security systems are the need of the hour to protect data from unauthorized access. The dissemination of confidential information over the public network requires a high level of security. The security approach such as steganography ensures confidentiality, authentication, integrity, and non-repudiation. Steganography helps in hiding the secret data inside the cover media so that the attacker can be confused during the transmission process of secret data between sender and receiver. Therefore, we present an efficient hybrid security model that provides multifold security assurance. To this end, a rectified Advanced Encryption Standard (AES) algorithm is proposed to overcome the problems existing in AES such as pattern appearance and high computations. The modified AES is used for the encryption of the stego image that contains the digitally signed encrypted secret data. The enciphering and deciphering of the secret data are done using the Rivest–Shamir–Adleman (RSA) algorithm. The experiments are conducted on the images of the USC-SIPI standard image database. The experimental results prove that the proposed hybrid system outperforms other SOTA (state-of-the-art) approaches.

KEYWORDS

Cryptography; steganography; digital signature; rectified AES; encryption

1 Introduction

Information security plays a substantial role in data communication through a transmission channel (i.e., physical communication or through a network channel). In order to ensure secret communication between the sender and receiver, a secure information dissemination system is the need of the hour as illustrated in Fig. 1. Impregnable communication is indispensable for transmitting data in a public channel. Gradually, the increase in communication infrastructure concerns the high altitude of information security in communication networks [1]. Due to the advancements in information



technology, it is easy, fast, and economical to send and receive data over the Internet [2,3]. The most common techniques to safeguard sensitive information are cryptography and steganography [4–6]. The concepts of steganography and cryptography are utilized to ensure confidentiality and authentication but the addition of a digital signature ensures integrity and non-repudiation also. Cryptography is the process of converting plaintext to unintelligible form so that the attacker could not read the transmitted message between sender and receiver [7]. It can be classified into two categories: Symmetric-key cryptography and Asymmetric-key cryptography. In symmetric-key cryptography, only one shared secret key is utilized for both the encryption and decryption process while asymmetric key cryptography employs the public key and private key for enciphering and deciphering secret data.



Figure 1: The process flow of the information dissemination system

The term steganography came from the Greek word stegano+graphy means covered writing [8]. It helps to hide secret messages inside any cover media such as images, video, audio, etc. A digital signature encrypts the hash value of the secret message using the private key of the sender which ensures the message is sent by the sender only [9]. The concept of digital signature with cryptography ensures non-repudiation (i.e., the sender cannot deny that the message was sent by him/her), and maintains the integrity of data. Eavesdropping and Man-in-the-middle attacks are the major challenges present in an information dissemination system. It is the biggest myth that only the encryption process is able to secure our data on the network. The required security is achieved through proper access control, ensuring integrity, and data availability [10,11]. Therefore, we propose a hybrid system that grabs the usefulness of the discussed individual security techniques to make an efficacious security system. The proposed research aims to ensure all the security primitives commonly known as the CIA triad (i.e., confidentiality, integrity, and availability), authentication, and non-repudiation [12].

The major contributions of this work are:

- The problem of pattern appearance and high execution time exists in standard AES, therefore, we propose a modified AES that helps to mitigate the existing problems in AES.
- The problem of eavesdropping by the intruder leads to the breach of confidential information, therefore, a novel hybrid system for multilevel security in disseminating secret information is proposed.
- The proposed system ensures all the security requirements such as confidentiality, integrity, availability and non-repudiation.
- Comparative analysis of the performance of standard AES and Rectified AES is done in terms of entropy, correlation coefficient, and execution time.
- The proposed rectified AES achieved a 1.05% improvement in entropy and a 1.25% improvement in execution time in comparison to standard AES.

The structure of the paper is systematized as follows. The first section covers a brief overview of the need for multilevel security and hybrid systems. Section 2 confers the contemporary literature on the tools and techniques used for multilevel security. Section 3 elaborates on the materials and the proposed method to ensure confidentiality, integrity, availability, and non-repudiation. The experimental setup such as system configuration, the programming language for the implementation, the dataset used, the conducted experiments, and the discussion related to the achieved results are discussed in Section 4. Finally, Section 5 concludes the research article and proposes the prospects of the research.

2 Related Works

Earlier, individual techniques [13–17] have been utilized to provide data security but now the interest of researchers has been shifted towards hybrid systems. In the contemporary scenario, a greater amount of research work has been done for hybrid security systems to deliver an elevated level of information security [18–23]. Curvelets-based ECG steganography technique was proposed by Jero et al. [24] that embeds the confidential data of patients into their ECG signals. The proposed approach only provides the confidentiality of data but the attacker can replace the embedded data that may lead to an integrity breach. Abbas et al. [25] proposed a hybrid approach to enhance the data security for the cloud. They used the amalgamation of steganography and cryptography to provide high-level cloud security. AES, RSA, Least Significant Bit (LSB), and Lempel-Ziv-Welch (LZW) algorithms are used to achieve all the security primitives. The key feature of their work is that it also provides compression of data that leads to the requirement of less bandwidth at the time of transmission and makes the algorithm faster.

The hybrid system proposed by Jassim et al. [26] utilized steganography and cryptography techniques to embed secret data inside an image. The message is encrypted through the RSA algorithm and occluded inside an image using the LSB steganography technique. The method achieved confidentiality and authentication primitives but the modification in the hidden data can be done by the attacker. Anwarul et al. [27] suggested some modifications in the AES algorithm to overcome the existing problems such as pattern appearance and high computations. The authors used modified AES for the encryption of an image. Further, steganography is employed for hiding the shared secret key of AES in the encrypted image to enhance security. The study projected by Belkaid et al. [28] targeted the protection of medical information available in the form of images. They suggested a hybrid encryption technique to provide security to medical images from illegitimate access to the patient's data.

The amalgamation of steganography, encryption, and watermarking in a hybrid system was presented by Razzaq et al. [29]. The encryption in the proposed method was done by the secret key generated by shifting the pixel bits using the XOR operator. The steganography and watermarking techniques were used for data hiding and copyright protection, respectively. Alarood et al. [30] suggested an image steganography technique for Internet of Things (IoT) networks. The approach utilized the characteristics of the pixels of the cover image for the embedding process. They classified the highly smooth and less smooth domains to identify the eligible pixels that could include in the embedding phase.

Liao et al. [31] presented a new approach for the steganography of medical images that utilized the dependencies of the inter-block coefficients. The experimental results in the presented paper proved that the steganographic algorithm in [31] is better than other existing steganographic approaches. Denis et al. [32] proposed a hybrid system for the cloud-based healthcare systems consisting of AES and RSA algorithms for the encryption process. They utilized the concept of a genetic algorithm for the pixel adjustment process to enhance the hiding capability of the algorithm. In [32], the authors developed three modules in the presented paper. The encryption process was done using AES and RSA, whereas the hiding of patient's data in the medical cover image was done using Discrete Wavelet Transform. In addition, they utilized Adaptive Genetic Algorithm in the embedding phase for the pixel adjustment process.

The aspects of security, privacy, trust, and anonymity in DNA computing were discussed in [33]. In order to protect user data, each of them has a specific function. The authors described how DNA computing is used to address these issues. Data encryption and masking are two methods used to achieve data security, where the objectives of data security can vary depending on the type of information being protected. The use of these techniques can help protect sensitive information and control access to it. Kumari et al. [34] discussed community detection algorithms (CDAs) and the issue of community deception in complex industrial networks for privacy reasons. They introduced two methods to conceal nodes from CDAs, using persistence and safeness scores to optimize the problems. The objective functions aim to minimize the persistence score and maximize the safeness score of the nodes, and the simulation results showed the efficacy of the proposed strategies in concealing community information in complex industrial systems.

Niu et al. [35] proposed a solid-state circuits-based communication system that provides highspeed transmission of data. The secure transmission is missing in their research. In the presence of passive and active eavesdropping attacks, Cao et al. [36] examined the security of semi-grant-free Non-orthogonal multiple access transmission. They utilized IoT to reduce access delay and provide massive connectivity in the network. The research proposed by Cao et al. [37] examined the physical layer security of the wireless-powered information dissemination systems by considering the presence of a passive eavesdropper. The results of their research illustrate that low transmission power is required in the proposed system. Gao et al. [38] presented an asynchronous updating Boolean network encryption algorithm based on chaos (ABNEA) to ensure the safe transmission of the network. The algorithm uses a novel 2D chaotic system to generate key streams for encryption and a synchronous updating Boolean network is converted to a Boolean matrix and propagated on the network as an image. Simulation experiments and security analysis demonstrated the effectiveness of ABNEA in encrypting asynchronously updating Boolean networks and have good security characteristics. Even though the discussed methods in the literature covered different aspects, they are limited to ensuring confidentiality, integrity, and authentication. Therefore, we proposed a multi-level information dissemination system that ensures all the security primitives such as confidentiality, integrity, availability, authentication, and non-repudiation.

3 Materials and Methods

3.1 The RSA Algorithm

In the proposed system, the encryption and decryption of the secret text are done using the RSA algorithm [39]. The algorithm follows an asymmetric key cryptography approach and works on the fact that the factorization of large integers is difficult. First, two prime numbers are selected, i.e., α and β , where public key and private keys are derived from the selected prime numbers. The second step is to calculate block size (n) and Euler's totient function ($\Phi(n)$). After getting the values of n and $\Phi(n)$, select public key (e) in such a way that the Greatest Common Divisor (GCD) of e and $\Phi(n)$ should be equal to 1. The private key (d) is calculated using the public key. The enciphering process is done using the public key (e) to get the ciphertext (Ci) and the deciphering is done using the generated private key (d) to acquire the plaintext (P). The diagrammatic flow of the RSA algorithm is illustrated in Fig. 2.



Figure 2: The overall working of the RSA algorithm

3.2 The Proposed Rectified AES Algorithm

The earlier version of AES consists of 10, 12, or 14 rounds which consist of a 128-bit key in 10 rounds, a 192-bit key in 12 rounds, and a 256-bit key in 14 rounds. Each round consists of four operations such as substitute bytes, mix columns, shift rows, and add round keys [40]. The complete structure of the algorithm is illustrated in Fig. 3. It receives 128-bit plaintext to convert into 128-bit ciphertext. The maximum number of calculations are performed in the mix columns step. The value of each byte of a column is replaced by a new value which is a function of all four bytes in that column. The columns are considered as polynomials over GF(2⁸) and multiplied by a fixed polynomial a(x) modulo $x^4 + 1$ given by Eq. (1).

$$(x) = \{03\}^3 + \{01\} x^2 + \{01\} x + \{02\}$$
(1)



Figure 3: The structure of the AES algorithm

Therefore, we rectified the mix columns step to minimize the number of computations that make the algorithm faster. Mix column step plays a significant role in providing confusion and diffusion to the cipher text, thereby enhancing the security of the encryption process. In the MixColumns step, each column of the 4×4 state matrix is transformed using a mathematical function that mixes the bytes of the column. The scrambling step is also added to alleviate the problem of pattern appearance. The scrambling step is done before passing the input to the modified AES by XOR ing the actual image with the randomly generated matrix. The dimensions of the randomly generated matrix are the same as the dimensions of the input image.

In the substitute bytes step, the substitution of the value of each byte is done using 16×16 bytes S-box table which is prepared using the transformation of values in Galois Field (GF(2⁸)). The permutation of the bytes between the columns is done in the second step of each round known as the shift rows step. The mix columns step requires a lot of computations that make the algorithm slow. The modification in this step is done in the same way as the computations are performed in the shift rows step as shown in Fig. 4. The values in the first column remain the same while the bytes of the second column take a one-step cyclic downward shift and so on. At the time of deciphering, the operation is done by shifting upwards cyclically from the second column onwards. This modified step simply permutes the bytes between the rows. The proposed modification reduces the computations but makes the algorithm prone to attacks. To compensate for the generated issue, multilevel security is provided using various security methods. The last step of the algorithm (i.e., add round keys) is utilized by XORing the state array with 128-bit of the expanded key.



Figure 4: The rectified mix columns step

3.3 The Proposed System

The purpose of the intended research is to secure text and image data from intruders. The proposed methodology is divided into five modules on the sender side: generation of keys, confidential text encryption/decryption, generation/verification of the digital signature, embedding/fetching of the digitally signed encrypted secret text in the carrier file, and encryption/decryption of the stego image. Similarly, these five modules are repeated in reverse at the receiver side for acquiring the secret data. The complete flow of the suggested system at the sender and recipient sides is illustrated in Figs. 5 and 6, respectively. Algorithm 1 demonstrates the functionality of the proposed system at the sender's end while the working at the recipient side is discussed in Algorithm 2.



Figure 5: The schematic process flow at the sender side



Figure 6: The schematic process flow at the receiver side

Algorithm 1: Secret information dissemination algorithm for multilevel security on the sender side

Input: Carrier image {C}, secret text {S}, sender's private key { \check{S}_{pri} }, receiver's public key { \check{R}_{pub} }, shared secret key { \mathscr{K}_{sec} }, randomly generated matrix of size same as carrier image {C} **Output:** Digitally signed encrypted stego image {2}

```
function sender_process (S, C, \check{R}_{pub}, \check{S}_{pri}, \mathscr{K}_{sec})

\check{E} \leftarrow \operatorname{Enc}(\operatorname{RSA}(S, \check{R}_{pub}))

\mathfrak{H}_1 \leftarrow \operatorname{Hash}_{\operatorname{SHA512}}(S)

\hat{H} \leftarrow \operatorname{Enc}(\mathfrak{H}_1, \check{S}_{pri}))

\mathfrak{D} \leftarrow \check{E} + \hat{H}

\hat{I} \leftarrow \operatorname{Hide}(\operatorname{LSB}(\mathfrak{D}, \operatorname{C})))

\mathfrak{b} \leftarrow \hat{I} \oplus \mathbb{C}

\mathfrak{c} \leftarrow \operatorname{Enc}(\operatorname{Mod}_{\operatorname{AES}}(\mathfrak{b}, \mathscr{K}_{sec})))

return \mathfrak{Z}
```

Algorithm 2: Secret information dissemination algorithm for multilevel security on the receiver side

Input: Digitally signed encrypted stego image {8}, public key of sender $\{\check{S}_{pub}\}$, a private key of receiver $\{\check{R}_{pri}\}$, shared secret key $\{\mathscr{K}_{sec}\}$, randomly generated matrix of size same as carrier image {C} **Output:** Carrier image {C}, secret text {S}

function receiver_process (2, $\check{R}_{pri}, \check{S}_{pub}, \mathscr{K}_{sec}$) $b \leftarrow \text{Dec}(\text{Mod}_A\text{ES}(2, \mathscr{K}_{sec}))$ $\hat{l} \leftarrow b \oplus \mathbb{C}$ $C, D \leftarrow \text{Fetch}(\text{LSB}(\hat{l}))$ $\check{E}, \hat{H} \leftarrow D$ $\mathfrak{H}_1 \leftarrow \text{Dec}(\hat{H}, \check{S}_{pub})$ $S \leftarrow \text{Dec}(\text{RSA}(\check{E}, \check{R}_{pri}))$ $\mathfrak{H}_2 \leftarrow \text{Hash}_{\text{SHA512}}$ (S) *if* ($\mathfrak{H}_1 == \mathfrak{H}_2$) *print* ("Signature verified") *return* C, S

3.3.1 Generation of Keys

This module consists of the generation of the sender's private key $\{\check{X}_{pri}\}$, the receiver's private key $\{\check{X}_{pri}\}$, the sender's public key $\{\check{X}_{pub}\}$, and the receiver's public key $\{\check{X}_{pub}\}$ for the enciphering and deciphering process using the RSA algorithm. A shared secret key $\{\mathscr{K}_{sec}\}$ is also generated for the encryption of the stego image using a modified AES algorithm. A secret key $\{\mathscr{K}_{sec}\}$ is shared with the receiver by embedding it inside the digitally signed encrypted image. The approach of hiding the shared key inside an image for sharing is better than the key sharing using the Diffie-Hellman [41] approach because of the possibility of a Man-in-the-middle-attack [42] in Diffie-Hellman.

3.3.2 Encryption/Decryption of the Confidential Text

The confidential text {S} is encrypted by RSA algorithm {Enc(RSA(S, $\check{R}_{pub})$ } using a public key of the receiver { \check{R}_{pub} } and utilizing Optimal Asymmetric Encryption Padding (OAEP) [43,44] to accomplish computational security. The decryption of the encrypted secret data { \check{E} } is done at the receipent side using the receiver's private key {Dec(RSA($\check{E}, \check{R}_{pri})$)}.

3.3.3 Generation/Verification of Digital Signature

The digital signature of the sender is generated by encrypting the hash value of the secret text { H_1 } using SHA512 hashing algorithm {Enc(H_1 , \check{S}_{pri})} stored in { \hat{H} }. The digital signature is done by utilizing the private key of the sender { \check{S}_{pri} } that is only known to the sender. The digitally signed encrypted secret text is generated and stored in {D}. The verification of the digital signature is done at the receiver side using the public key of the sender { \check{S}_{pub} } which ensures non-repudiation. The verification step is done by decrypting the hash value of the received encrypted secret text { $Dec(\hat{H}, \check{S}_{pub})$ } stored in { H_1 } and comparing it with the calculated hash value of the secret text { H_2 }.

3.3.4 Embedding/Fetching of Encrypted Secret Text in the Carrier File

In this module, the digitally signed encrypted secret data $\{D\}$ is embedded inside the cover image $\{C\}$ using Least Significant Bit (LSB) steganography technique $\{Hide(LSB(D, C))\}$ to generate stego image $\{\hat{I}\}$. This step ensures confidential communication between the sender and the recipient. The

receiver retrieves the hidden digitally signed encrypted secret message {Fetch(LSB(\hat{I}))} from the stego image.

3.3.5 Encryption/Decryption of the Stego Image

After embedding the digitally signed encrypted secret text, the encryption of stego image {2} is also done to fool the intruder {Enc(Mod_AES($\mathcal{B}, \mathcal{K}_{sec}$)} using a shared secret key { \mathcal{K}_{sec} } between the sender and receiver. The attacker will think that the image is encrypted so it would be confidential data but the secret data is hidden behind the image. This module is done to provide multi-level security by encrypting the stego image using a modified AES algorithm. The addition of scrambling of an image using XOR operation with the random matrix of the same size of image is done before employing modified AES to overcome the pattern appearance problem existing in AES { $\hat{I} \oplus \mathbb{C}$ } and generates scrambled image { \mathcal{B} }. At the receiver side, first, the descrambling process { $\mathcal{B} \oplus \mathbb{C}$ } is done to get the encrypted stego image. Then, the decryption of the stego image is done using modified AES {Dec(Mod_AES(2, $\mathcal{K}_{sec})$)}. After decrypting the stego image, the fetching of digitally signed secret data is made.

4 Experimental Evaluation

This section covers the details of the system configuration, the dataset utilized, the evaluation metrics employed to measure the effectiveness of the proposed research, and the analysis of the results.

4.1 Experimental Environment

All the experiments are conducted to scrutinize the efficacy of the intended system. The configuration of the system comprises Windows10 with AMD Ryzen 5 4600H, Radeon Graphics, and 8 GB RAM. The implementation of the proposed method is accomplished using Python3.

4.2 Dataset Used

All the experiments are conducted on the images of the USC-SIPI standard image database [45] (https://sipi.usc.edu/database/) and some synthetic images that are publicly available. The dataset consists of 44 images having different sizes such as 256×256 , 512×512 , and 1024×1024 . All the images are in TIFF format. The dataset consists of both grayscale and color images as shown in Fig. 7. The experiments on color images are conducted by converting them into the gray scale image to reduce computational requirements.

4.3 Evaluation Metrics

The proposed research is evaluated based on execution time, entropy, pattern appearance, and correlation coefficient. The term entropy E(I) defines the degree of randomness of the information in an image, which can be calculated using Eq. (2). The ideal value of entropy is 8. The value of entropy less than 8 shows some degree of predictability of information in an image. The correlation between the original image and the encrypted image $C(I_1, I_2)$ defines the degree of similarity between the two images that are being calculated using Eq. (3). The low value of the correlation coefficient between the original image and the encrypted image represents a good encryption process. The execution time of the algorithm considers both the encryption and decryption time.

$$E(I) = \sum_{j=1}^{n} P(I_j) \log_2 P(I_j)$$
(2)

Here, $P(I_j)$ is the probability of the jth pixel of the image I and n is the number of pixels in an image.

$$C(I_1, I_2) = \frac{\sum_p \sum_q \left(I_{1(pq)-} \overline{I_1} \right) \left(I_{2(pq)-} \overline{I_2} \right)}{\sqrt{\left(\sum_p \sum_q \left(I_{1(pq)-} \overline{I_1} \right)^2 \right) \left(\sum_p \sum_q \left(I_{2(pq)-} \overline{I_2} \right)^2 \right)}}$$
(3)

Here, I_1 and $\overline{I_1}$ are the input image and mean of the gray values of the pixels of an input image, respectively. Similarly, I_2 and $\overline{I_2}$ are the encrypted image and mean of the gray values of the pixels of an input image, respectively. The location of the pixels in an image is represented by p^{th} row and q^{th} column of an image.



Figure 7: The sample images of the USC-SIPI dataset

4.4 Results and Discussion

The experimental results are conducted in two stages. First, the rectified AES algorithm is evaluated, and second, the implementation of the proposed system is done. The evaluation of the rectified AES is done based on execution time, entropy, pattern appearance, and correlation coefficient in contrast to the standard AES algorithm shown in Table 1. Then, the comparative discussion of the outcomes of the proposed system with other existing literature is given in Table 2. Fig. 8a illustrates the pattern appearance problem in existing AES and Fig. 8b demonstrates the encryption using modified AES with no pattern appearance. The results in Figs. 8a and 8b are generated by applying standard AES and rectified AES algorithms, respectively for the encryption process.

Table 1 illustrates the superiority of the rectified AES over the standard AES in terms of entropy, correlation coefficient, and execution time. The last row of Table 1 indicates the average of the results obtained on all the images of the dataset whereas the first four rows show the result on some images of the dataset. The improvement in entropy value of the proposed rectified AES is 1.1%, as well as

execution, is approximately two times faster. The correlation value indicates that there is a negligible correlation between original images and encrypted images.

Input image	Size		Entropy	,	Correlation co between the in the encrypted	Defficient aput image and image	Execution time (in ms)		
		Original image	Encrypted image using AES	Encrypted image using rectified AES	Encrypted image using AES	Encrypted image using rectified AES	Encryption using AES	Encryption using rectified AES	
House	256 * 256	2.6797	6.5719	7.9993	-0.2048	0.0014188	10141	9432	
Female	256 * 256	5.9484	7.8325	7.9994	-0.015924	-0.000366	10521	9941	
Peppers	512 * 512	7.2226	7.9992	7.9994	0.0017145	0.0017545	99008	78019	
Mandrill	512 * 512	7.8362	7.9988	7.9994	-0.0004202	-0.0030691	101008	79118	
Average	_	5.8645	7.2419	7.9991	-0.3194297	-0.0002618	3218 (s)	1543 (s)	

Table 1: Comparison of the rectified AES with the standard AES algorithm

Table 2: Comparison of the intended system with SOTA approaches

Author, year	Confidentiality	Integrity	Authentication	Non-repudiation
Guclu [46], 2022	Yes	Yes	Yes	No
Bharathi et al. [47], 2021	Yes	No	Yes	No
Abbas et al. [25], 2020	Yes	Yes	Yes	No
Jassim et al. [26], 2019	Yes	No	Yes	No
Hambouz et al. [48], 2019	Yes	Yes	Yes	No
Biswas et al. [49], 2019	Yes	Yes	Yes	No
Anwarul et al. [27], 2017	Yes	No	Yes	No
Jain et al. [50], 2017	Yes	Yes	Yes	No
Kumar et al. [51], 2011	Yes	No	Yes	No
Proposed system	Yes	Yes	Yes	Yes

(a)

Figure 8: (Continued)

Figure 8: Encryption and decryption (a) using AES (b) using modified AES

In this section, the experiments are conducted to show the implementation of the proposed system. The private and public keys are generated for the encryption using the RSA algorithm. The encrypted text of the given secret text "My ATM pin is 1234. Keep it secret else it will be misused" is also given in Fig. 9. The hash of the secret message using the SHA512 hashing algorithm and the encrypted hash using the sender's private key are displayed in Figs. 10 and 11, respectively.

Requirement already satisfied: pycryptodome in c:\users\shahi\anaconda3\lib\site-packages (3.11.0) Public key: (n=0xea93a6064d95ada4e02b7fcd47f461a931f63a77bf437ca3f8c08c02834ab5170d9ad2545f10a43130393b882ad63a0a2e64fb3a910f8 72b41d9445d12e3f41df6e4ba391f8b69cce4ac29a3a46d4d173dd9ed327cb6e67636390ac71e5cb9cb2e88;9d6a45eabf00b5ec5594223bd1cfc757cacbf 61bb2c84972f8b5d8d51, e=0x10001) ---BEGIN PUBLIC KEY--MIGFMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDqk6YGTZWtpOArf81H9GGpMfY6 d79DfKP4wIwCg0q1Fw2a0lRfEK0xMDk7iCrW0gouZPs6k0+PK0HZ2URdEuP0Hfbk ujkfi2nM5Kwpo6RtTRc92e0yfLbmdjY5CsceXLnLLujJ1qReq/ALXsVZQi09HPx1 fKy/YbsshJcvi12NUQIDAQAB -- END PUBLIC KEY--Private key: (n=0xea93a6064d95ada4e02b7fcd47f461a931f63a77bf437ca3f8c08c02834ab5170d9ad2545f10a43130393b882ad63a0a2e64fb3a910f8 f2b41d9d9445d12e3f41df6e4ba391f8b69cce4ac29a3a46d4d173dd9ed327cb6e67636390ac71e5cb9cb2ee8c9d6a45eabf00b5ec5594223bd1cfc757cacbf 61bb2c84972f8b5d8d51, d=0x194ce078c8906ec09c2f04e342b200808bb3777de7e2a3045a758604555dcee7541fd134a96635975a90a9b3978f30865d97a f92aeae89e1602c898c092978bcb) ----BEGIN RSA PRIVATE KEY--MIICXAIBAAKBgQDqk6YGTZWtpOArf81H9GGpMfY6d79DfKP4wIwCg0q1Fw2a0lRf EKQxMDk7iCrWOgouZPs6kQ+PK0HZ2URdEuP0Hfbkujkfi2nM5Kwpo6RtTRc92e0y fLbmdjY5CsceXLnLLujJ1qReq/ALXsVZQiO9HPx1fKy/YbsshJcvi12NUQIDAQAB AoGAGÚzgeMiQbsCcLwTjQrIAgIuzd33n4qMEWnWGBFVdzudUH9E0qWY1l1qQqbOX jzCGXZeloxz3NSVgvlrZLUK21C4zmecMeTwalIBAbHGZ8znU3x7OTfmdgIbrSm8c MPR3d7qSL1fD2yj967WKnLKmlCMa+Srq6J4WAsiYwJKXi8sCQQDyD4wSbgUtC7gV 7lGwz/Dojbau+1Qf9l6ORcjXde+GuTEFwkxCkGIMajl8gyUuVa8UjxtfTYtd1jFF M5naHw5DAkEA+BXF04MFV4LWd1EBG7kOyjHickJCnSo0/XDL9bm9N6oSmVqcJcWd quj5ivbF12KIv2Q7yXRMXxDvfcWCaZWe2wJAP0BKxMIU/ilSyABHPmGHv0zS8LRh zhxNpvWbPpnlphmcMroLvVUHGeFj9iI6w/nFzyR57ZRQt4txwnhyWmnFCwJAdEL3 38TCJx3I1kffBhf2x2kTX0qQH0ldZfyLiQ/Pjhuk9btR/B2dYzAlait10hd6UH9v yVw4QkEUi10ZZ1PYCwJBALarmIEKZpCEiOL0KAw4C6NVAjFqFo4IwnAJLgjdga8W gDdVq2ccUQ2mhcfwqQLZfSYljUMgHTml1uSCzrqZ83o= --- END RSA PRIVATE KEY--Encrypted: b'd9e8544fa0c529e0812d954594740e7ea59e9437cf5f8054bb68ed79a9a64558d5d772a4894c437861a070369d6fae03d712d6e696a6f412c0 2ac9bfa52b60b3ee6b6c9141961f4ea45f5e2bd856daa5013ae37a9f69deed4a9bd8f28fdc497803d057a2e94b72529dbeec2bd3e59915238ebf630a0d653a5 36339c1624f9d8e

Figure 9: Generation of keys and encrypted secret text

879f3bfa24f029f0c3fd4779b1374f79f1e4941af4ce24ff13b27818dc87c870dfbcab787b7fb3082a6c8af0cc0d6aa4b9b5c29149baecb82e5e045825f5230

Figure 10: The hash value of secret text

b'126f899bf65a063dfa109aec6347824a028e8f91daec1e009fb9e6d69fbcce154331155c0658a801f480e56299f810ede663f86b5a3e3d248e96a9bd80e71 a917f8148fda6bf81e8a2d83451f0ba27af9f95fa939889811097d2af33d61c026adeb9ef10bc6c100c136630152a048cb56666a43c19ff0ab00ce02cc01f27 ee3d'

Figure 11: Encrypted hash value

The combination of encrypted secret data and encrypted hash value generates the digitally signed encrypted secret data to be hidden inside the carrier file. This amalgamation guarantees the integrity of data and non-repudiation. The security of the secret text is improved by the use of steganography. The intruder is not able to identify the hidden data inside the cover media as displayed in Figs. 12a and 12b. The size of the resultant image after embedding the secret text is changed as displayed in Fig. 13. Statistical steganalysis is not possible because there is no significant change in the visibility of the histogram of the original image (cover image) and stego image as illustrated in Fig. 14. In Fig. 14, the x-axis represents the different color values, which lie between 0 and 255, and the y-axis represents the number of times a particular intensity value occurs in the image.

Figure 12: Steganography (a) cover image (b) stego image

baboon			baboon1	
TIFF File (.tiff)		Type of file:	TIFF File (.tiff)	
Photos	Change	Opens with:	Photos	Change
C:\Users\shahi\Desktop		Location:	C:\Users\shahi\Desktop	
768 KB (7.86.572 bytes)		Size:	768 KB (7.87.090 bytes)	
772 KB (7.90.528 bytes)		Size on disk:	772 KB (7.90.528 bytes)	
27 October 2021, 00:33:27		Created:	27 October 2021, 00:33:56	
26 September 1997, 21:03:19		Modified:	27 October 2021, 01:11:36	
27 October 2021, 00:35:47		Accessed:	27 October 2021, 01:11:36	
Read-only Hidden	Advanced	Attributes:	Read-only Hidden	Advanced.
	baboon TIFF File (:tiff) Photos C:\Users\shahi\Desktop 768 KB (7.86.572 bytes) 772 KB (7.90.528 bytes) 27 October 2021, 00:33:27 26 September 1997, 21:03:19 27 October 2021, 00:35:47 Read-only Hidden	baboon TIFF File (.tiff) Photos C:\Users\shahi\Desktop 768 KB (7.86.572 bytes) 772 KB (7.90.528 bytes) 27 October 2021, 00:33:27 26 September 1997, 21:03:19 27 October 2021, 00:35:47 Read-only Hidden	baboon TIFF File (tiff) Photos Change C:\Users\shahi\Desktop 768 KB (7.86.572 bytes) 772 KB (7.90.528 bytes) 27 October 2021, 00:33:27 26 September 1997, 21:03:19 27 October 2021, 00:35:47 Read-only Hidden Advanced	baboon image:/image

Figure 13: Size of the cover image and stego image

Figure 14: Histogram analysis of cover image and stego image

The fetching of digitally signed encrypted secret text from stego image is done in experiments using the HxD editor. The encrypted secret text and the encrypted hash value start from the character 'b' as shown in Fig. 15. The decrypted text from the embedded data is displayed in Fig. 16. The hash value of the received message is decrypted by the sender's public key and the secret text is decrypted using the recipient's private key. Then, the hash value of the decrypted secret text is calculated again. If the calculated hash value and the received hash value match, that means the signature is verified and integrity is maintained. The signature verification that ensures non-repudiation is shown in Fig. 17.

If if ie Edit Search View Analysis Tools Windows (ANS) Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Nex Nex Image: Search View Analysis Tools Windows (ANS) Nex Nex Nex Nex Nex Image: Search View Analysis Tools Windows Milling Windows (ANS) Nex Nex Nex Nex Nex Image: Search View Analysis Tools Windows Milling Windows Milli	Hx Hx	D - [C:\Use	ers\sh	ahi\	Desk	top/	babo	oon1.	tiff]										
Image: Control of the second	15 F	ile Edit	Searc	h V	iew	Ana	lysis	Too	ols	Wind	low	Hel	р						
		👌 🕶 🔛	10	<u>OP</u>		-	+ +	16	-	~ \	Wind	lows	(ANS	51)		~	hex		>
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 08 0C 0D 0E Decoded text 0000C0020 00 01 01 00 03 00 00 01 02 00 00 01 02 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 01 00 00 01 00 00 01 00 00 01 00 00 01 00 00 01 00 00 01 00 00 01 00	Ш ь	aboon1.tif	f																
000C0020 00 00 01 02 00 00 01 02	OFI	fset (h)	00	01	02	03	04	05	06	07	08	09	OA	OB	oc	OD	OE	OF	Decoded text
000C0030 00 03 00 <	000	00020	00	00	01	01	00	03	00	00	00	01	02	00	00	00	01	02	
000C0040 00 01 00 01 00 <	000	00030	00	03	00	00	00	03	00	oc	00	86	01	03	00	03	00	00	
000CC0050 00	000	000040	00	01	00	01	00	00	01	06	00	03	00	00	00	01	00	02	
000CC0060 00 01 00 01 00 01 00 01 00 00 01 00	000	00050	00	00	01	11	00	04	00	00	00	01	00	00	00	08	01	15	
000CC0070 00 01 00	000	000060	00	03	00	00	00	01	00	03	00	00	01	17	00	04	00	00	
000CC0080 00 00 00 00 00 00 08 00 8 2 27 64 35 000CC0080 53 33 34 35 34 35 34 35 34 35 34 37 66 33 35 34 65 37 65 61 35 000C00000 36 65 35 34 37 36 66 35 35 35 36 64 35 65 35 64 35 35 36 64 35 65 36 64 34 35 35 36 64 35 65 36 37 38 36 31 32 <td>000</td> <td>00070</td> <td>00</td> <td>01</td> <td>00</td> <td>oc</td> <td>00</td> <td>00</td> <td>01</td> <td>10</td> <td>00</td> <td>03</td> <td>00</td> <td>00</td> <td>00</td> <td>01</td> <td>00</td> <td>01</td> <td></td>	000	00070	00	01	00	oc	00	00	01	10	00	03	00	00	00	01	00	01	
000CC0090 65 38 35 34 46 61 30 65 30 38 31 e8544faoc529e083 000CC00B0 39 65 39 34 33 763 66 35 35 34 62 62 9e9437cf5f8054b 000CC00D0 64 37 37 36 63 34 33 73 86 43 433 37 38 64 35 38 64 35 35 38 64 35 35 38 64 35 35 38 64 35 35 38 64 35 36 34 33 37 38 36 34 33 37 38 36 34 33 37 38 36 34 34 33 37 38 36 34 34 33 37 38 33 36 34 39 37 38 30 33	000	000080	00	00	00	00	00	00	00	08	00	08	00	08	62	27	64	39	b'd9
000CC00A0 32 64 39 35 34 35 34 37 34 30 65 37 65 61 35 2d954544740e7eas 000CC00C0 36 38 65 64 37 39 61 39 61 36 34 35 38 64 35 000CC00C0 64 37 37 2 61 34 38 37 38 63 1 4772a4394c43786 000CC00F0 31 32 64 36 39 36 31 32 65 36 39 36 31 32 65 36 39 36 31 66 34 65 61 35 66 34 65 66 34 65 61 35 55 36 39 31 35 32 36 61 35 63 36 36 36 36 31 36 36	000	000090	65	38	35	34	34	66	61	30	63	35	32	39	65	30	38	31	e8544fa0c529e081
000CC00B0 39 65 39 34 33 77 61 36 61 35 34 62 62 99437cf5f805tb 000C00D0 64 37 37 32 61 34 35 35 36 64 35 36 64 36 64 37 38 36 31 64 37 38 36 31 64 36 34 33 37 38 36 31 66 36 31 36 36 39 36 66 66 66 34 31 36 31 12d6656a6f112c0 000C0100 32 61 65 37 31 31 31 31 31 31 31 31 33 31 31 33 31 35 34 43 37 33 30 33 55 32 32 36 64 51 31 30 35 3	000	OCOOAO	32	64	39	35	34	35	39	34	37	34	30	65	37	65	61	35	2d954594740e7ea5
000C00C0 36 38 65 64 37 39 61 39 61 33 35 36 44 35 35 36 44 35 35 36 45 35 36 45 35 36 46 36 36 33 37 37 37 30 33 36 36 35 35 36 45 36 66 31 32 64 36 66 61 35 30 31 36 36 66 31 32 65 55 32 62 66 31 32 65 65 31 36 31 66 34 31 33 <	000	OCOOBO	39	65	39	34	33	37	63	66	35	66	38	30	35	34	62	62	9e9437cf5f8054bb
000CC00D0 64 37 37 32 61 34 39 34 63 34 33 37 38 63 1 d77244994c437865 000CC00F0 31 32 64 36 53 39 36 61 55 30 36 43 1 32 63 30 12d6e696a6f412cd 000C0100 32 61 63 39 13 13 31 31 32 63 30 12d6e696a6f412cd 000C0100 32 66 39 31 31 31 33 64 65 64 66 64 56 54 46 56 54 46 36 57 52be2bd556daa50 000C0140 39 62 64 38 65 55 39 31 35 32 33 53 33 53 33 53 33 53 33 55 56 56 56	000	000000	36	38	65	64	37	39	61	39	61	36	34	35	35	38	64	35	68ed79a9a64558d5
000C00E0 61 30 37 30 33 36 39 64 36 66 61 30 33 64 37 a070369d6fae03d 000C00F0 31 32 64 36 53 39 31 34 31 32 63 30 12d6e696af12cd 000C0100 36 62 36 53 32 62 36 30 62 36 55 22de9bfa52b60b3ed 000C0100 36 62 36 35 36 64 65 64 64 53 34 65 54 44 65 64 64 64 65 64 64 65 64 65 64 65 64 65 64 65 66 65 66 65 65 63 37 66 36 36 37 37 36 33 37 80 95 96 65 65 65	000	OCOODO	64	37	37	32	61	34	38	39	34	63	34	33	37	38	36	31	d772a4894c437861
000C00F0 31 32 64 36 36 39 36 61 35 32 62 30 31 32 63 30 12d6669666f412cd 000C0100 36 62 36 39 31 34 31 39 36 31 64 56 61 35 66 35 65 32 62 64 36 31 64 65 61 35 63 31 34 31 39 36 31 65 61 35 33 31 34 31 39 36 31 65 61 35 33 31 32 63 34 65 65 32 37 38 33	000	OCOOEO	61	30	37	30	33	36	39	64	36	66	61	65	30	33	64	37	a070369d6fae03d7
000C0100 32 61 33 96 2 66 135 32 22 36 30 23 34 31 34 31 33 31 34 31 33 31 33 31 33 31 33 31 33 33 31 33 33 31 33 33 31 33 33 31 33 33 33 31 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 34 33 33 33 33 33 33 33 33 33 33 33 34 33 33 34 33 33 34 33 33 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 34 <	000	OCOOFO	31	32	64	36	65	36	39	36	61	36	66	34	31	32	63	30	12d6e696a6f412c0
000C0110 36 62 36 39 31 34 31 36 31 65 34 65 134 000C0120 35 66 35 66 35 36 64 61 13 31 35 36 64 65 65 64 34 61 33 31 36 33 37 61 39 66 64 65 65 64 34 61 33 37 35 30 33 36 37 61 39 66 64 63 34 39 33 33 31 35 32 39 40 573 23 53 39 31 35 33 40 35 33 31 35 33 31 35 33 31 35 35 39 31 35 35 33 31 35 35 33 31 35 35 33	000	0C0100	32	61	63	39	62	66	61	35	32	62	36	30	62	33	65	65	2ac9bfa52b60b3ee
000C0120 35 66 35 65 32 62 64 38 35 36 64 61 35 03 31 95522bd956daa50 000C0130 33 61 65 33 7 61 39 66 64 63 34 9 37 38 30 31 94622dfc49780 000C0140 64 30 35 37 61 32 65 39 34 53 32 39 64 30 33 944 35 32 39 61 35 32 39 31 35 32 39 64 36 35 33 66 33 39 31 64 63 65 76 33 39 63 64 36 35 61 30 36 33 64 33 39 64 64 36 35 61 30 36 33 65 33 </td <td>000</td> <td>0C0110</td> <td>36</td> <td>62</td> <td>36</td> <td>63</td> <td>39</td> <td>31</td> <td>34</td> <td>31</td> <td>39</td> <td>36</td> <td>31</td> <td>66</td> <td>34</td> <td>65</td> <td>61</td> <td>34</td> <td>6b6c9141961f4ea4</td>	000	0C0110	36	62	36	63	39	31	34	31	39	36	31	66	34	65	61	34	6b6c9141961f4ea4
000C0130 33 61 53 37 61 39 66 65 65 64 46 15 000C0140 39 62 64 33 66 64 63 34 39 37 38 30 33 000C0150 64 30 35 37 61 32 65 39 34 62 37 23 35 32 39 64 d057a2e94b72529 000C0160 62 65 63 32 66 31 36 53 39 31 35 32 39 bec2b3e5991522 000C0180 36 33 39 63 31 36 32 34 66 39 61 36 33 34 37 38 234 dfa109aec637622 000C0180 61 30 32 38 65 36 31 65 36 31 65 36 36	000	0C0120	35	66	35	65	32	62	64	38	35	36	64	61	61	35	30	31	5f5e2bd856daa501
000C0140 35 62 64 36 62 32 38 66 64 33 37 38 33 34 35 36 35 35 35 35 35 35 35 35 35 35 35 <	000	0C0130	33	61	65	33	37	61	39	66	36	39	64	65	65	64	34	61	3ae37a9f69deed4a
000C0150 64 30 35 37 61 32 65 39 34 62 37 32 35 32 39 64 d057a2e94b7252e 000C0160 62 65 63 32 64 33 63 31 35 32 33 bec2bd3e59152 000C0170 36 65 62 66 33 30 61 30 64 35 33 61 35 33 bec2bd3e59152 000C0180 36 33 39 63 31 66 32 34 66 35 31 36 32 34 66 36 31 37 32 34 dfa109acc634702 000C0180 61 30 32 38 65 36 31 66 63 36 31 66 62 63 65 36 31 66 62 63 65 66 36 36	000	0C0140	39	62	64	38	66	32	38	66	64	63	34	39	37	38	30	33	9bd8f28fdc497803
000C0160 62 65 63 32 62 64 33 65 35 39 31 35 32 33 becc2bd3e5991522 000C0170 38 65 62 66 36 33 01 64 36 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 33 61 35 34 37 35 32 4 61 65 63 31 65 30 61 30 63 33 43 33 33 33 33 33 33 33 33 33 33 33 33 33 33 <td< td=""><td>000</td><td>0C0150</td><td>64</td><td>30</td><td>35</td><td>37</td><td>61</td><td>32</td><td>65</td><td>39</td><td>34</td><td>62</td><td>37</td><td>32</td><td>35</td><td>32</td><td>39</td><td>64</td><td>d057a2e94b72529d</td></td<>	000	0C0150	64	30	35	37	61	32	65	39	34	62	37	32	35	32	39	64	d057a2e94b72529d
000C0170 38 65 62 66 33 30 61 30 64 36 33 33 16 130 64 36 33 33 16 130 64 36 33 33 16 130 36 33 33 39 63 31 36 32 34 66 39 64 38 65 27 62 339 62 66 38 65 37 61 30 36 33 39 62 66 36 35 61 30 36 33 31 65 36 33 31 65 36 33 16 65 33 16 65 33 16 65 33 16 33 33 13 35 35 36 33 31 35 35 33 16 35 33 16 33 33 135 35 36 33	000	000160	62	65	65	63	32	62	64	33	65	35	39	39	31	35	32	33	beec2bd3e5991523
00000180 36 33 39 63 31 36 32 34 66 39 64 38 65 27 62 6339c1624f9d8e1 00000190 27 31 32 36 63 39 39 62 66 36 35 12 34 4fa109acc634782 00000100 61 30 32 38 65 38 64 61 65 31 64 66 63 53 44 37 38 23 4 dfa109acc634782 00000100 30 36 62 36 31 64 61 66 36 31 65 30 028e8f91dacc1e0 000000100 35 34 33 31 35 35 63 30 65 36 33 64 36 64 36 65 36 36 36 36 31 65 36 30 65 37 <td>000</td> <td>0C0170</td> <td>38</td> <td>65</td> <td>62</td> <td>66</td> <td>36</td> <td>33</td> <td>30</td> <td>61</td> <td>30</td> <td>64</td> <td>36</td> <td>35</td> <td>33</td> <td>61</td> <td>35</td> <td>33</td> <td>8ebf630a0d653a53</td>	000	0C0170	38	65	62	66	36	33	30	61	30	64	36	35	33	61	35	33	8ebf630a0d653a53
000C0190 27 31 32 36 63 39 39 62 66 36 35 61 30 36 33 126f89bf65a06 000C01B0 61 30 32 38 65 31 30 31 37 36 32 34 000C01B0 61 30 32 86 53 66 39 31 64 65 31 65 31 65 31 65 33 31 31 35 55 30 65 33 65 33 31 31 35 55 30 65 33 65 33 65 33 65 33 65 33 65 33 66 33 65 33 65 33 65 33 65 33 65 33 65 33 65 33 65 33 65 33 65 33 63 33	000	0C0180	36	33	33	39	63	31	36	32	34	66	39	64	38	65	27	62	6339c1624f9d8e'b
000C01A0 64 66 61 31 30 39 61 65 63 36 33 34 37 38 32 34 dfal09acc634782 000C01B0 61 30 32 38 65 38 64 61 65 31 65 30 234 dfal09acc634782 000C01D0 30 66 23 65 36 64 61 65 36 65 10 95bec4657bbcc2 000C01D0 35 34 33 31 35 35 63 30 36 35 38 61 38 30 65 36 31 155 56 30 36 38 31 30 55 36 32 39 36 63 36 33 64 32 36 53 36 33 64 32 46 38 30 65 37 31 61 39 36	000	000190	27	31	32	36	66	38	39	39	62	66	36	35	61	30	36	33	126f899bf65a063
000C01B0 61 30 32 38 65 30 66 39 31 64 61 65 63 31 65 30 a028eBf9ldaecle 000C01C0 30 39 66 62 39 65 36 64 36 39 66 63 31 65 30 09fb9edd69fbcce 000C01D0 35 34 33 31 31 55 56 30 65 38 31 30 65 53 66 38 66 36 63 64 36 63 64 36 63 64 36 53 64 33 65 37 31 61 36 64 36 64 64 36 66 37 31 61 33 65 37 31 61 33 65 37 31 61 35 36 63 36 33 64 64 6	000	0001A0	64	66	61	31	30	39	61	65	63	36	33	34	37	38	32	34	dfa109aec6347824
000C01C0 30 39 66 62 39 65 36 64 36 39 66 62 63 65 31 09fb9e6d69fbcce 000C01D0 35 34 33 31 31 35 35 63 30 36 35 38 61 38 30 000C01D0 35 34 33 31 31 35 35 63 30 36 35 86 13 30 15431155c0658a0 000C01F0 64 65 36 36 63 36 62 35 61 33 65 33 64 32 486 36 33 64 32 36 63 31 64 30 65 31 64 33 66 64 61 36 31 31 486 63 13 1718187da 56 31 34 33 34 33 34 31	000	0C01B0	61	30	32	38	65	38	66	39	31	64	61	65	63	31	65	30	a028e8f91daecle0
000C01D0 35 34 33 31 35 35 63 30 36 35 38 61 38 30 54331155c0658a8 000C01E0 31 66 34 38 30 65 35 36 32 39 96 63 83 31 65 35 36 32 39 96 38 31 30 65 35 36 32 36 61 38 31 65 36 36 62 56 13 35 54 31 64 38 36 62 66 38 31 65 46 66 66 31 66 64 61 36 62 66 38 31 65 177814874046781 60 62 61 32 37 61 8243451704674 60 63 31 31 35 66 61 39 35 66 61 33	000	0C01C0	30	39	66	62	39	65	36	64	36	39	66	62	63	63	65	31	09fb9e6d69fbcce1
000C01E0 31 66 34 38 30 65 35 36 32 39 39 66 38 31 30 65 1f480e5629f810 000C01F0 64 65 36 33 66 38 31 65 33 64 32 66 33 64 32 4663f86b5a3e3d 000C0200 34 38 65 39 36 61 39 62 43 30 65 37 31 61 35 48696a5b45ba3e3d 000C0200 31 37 66 38 31 48 66 64 61 36 31 65 66 66 33 31 65 66 32 37 61 82 334 65 66 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33 33<	000	OCOLDO	35	34	33	33	31	31	35	35	63	30	36	35	38	61	38	30	54331155c0658a80
000C01F0 64 65 36 36 63 36 62 35 61 33 65 33 64 32 000C0200 34 38 65 39 36 61 39 62 64 38 30 65 37 31 61 39 48e96a9bd80e71ad 000C0220 34 37 66 38 33 43 36 64 62 66 31 63 17f818faa6bf81e 000C0220 38 61 32 64 38 33 34 35 31 66 30 62 61 32 37 61 8a2d83451f0ba27 000C0220 66 39 35 66 13 33 34 63 16 30 32 83 33 13 19f9f5fas93988981 000C0220 61 64 65 23 66 31 30 62 33 30 <	000	OCOLEO	31	66	34	38	30	65	35	36	32	39	39	66	38	31	30	65	1f480e56299f810e
000C0200 34 38 65 39 36 61 39 62 64 38 30 65 37 31 61 35 48e96a9bd80e71a 000C0210 31 37 66 38 31 34 38 66 64 61 36 66 38 31 57 51 66 53 31 65 64 61 36 66 53 31 65 66 36 31 65 66 53 31 65 66 36 36 66 52 37 51 65 66 52 37 61 82d33451f0ba27 000C02200 66 39 35 66 61 39 33 39 38 39 38 31 31 f9f95fa93988981 097d2af33d61c022 adeb9f10bc6c100 000c02260 61 64 65 66 31 30 31 30 adeb9f10bc6c100 0	000	OCOLFO	64	65	36	36	33	66	38	36	62	35	61	33	65	33	64	32	de663f86b5a3e3d2
000C0210 31 37 66 38 31 34 38 66 64 61 36 62 66 38 31 65 17f81487da6bf816 000C0220 38 61 32 64 38 33 34 35 31 66 30 62 61 32 37 61 8a2d83451f0ba27 000C0220 66 39 63 66 61 39 33 93 83 39 31 31 f9f95fa93989811 000C0220 30 39 37 64 32 61 66 33 39 38 39 38 31 31 097d2af33d61c02 000C0250 61 64 65 23 96 66 31 30 30 adeb9ef10bc6c100 000C0270 35 36 36 31 33 36 31 36 31 36 31 36 32 37 <td>000</td> <td>00200</td> <td>34</td> <td>38</td> <td>65</td> <td>39</td> <td>36</td> <td>61</td> <td>39</td> <td>62</td> <td>64</td> <td>38</td> <td>30</td> <td>65</td> <td>37</td> <td>31</td> <td>61</td> <td>39</td> <td>48e96a9bd80e71a9</td>	000	00200	34	38	65	39	36	61	39	62	64	38	30	65	37	31	61	39	48e96a9bd80e71a9
000C0220 38 61 32 64 38 33 34 35 31 66 30 62 61 32 37 61 Ba2d83451f0ba276 000C0230 66 39 35 66 13 33 39 38 39 38 31 1 ff9f95fa53988981 000C0240 30 37 64 26 66 31 33 34 63 163 31 31 ff9f95fa53988981 097daf33d61c024 000C0250 61 64 65 62 39 65 66 31 30 62 33 33 34 62 36 63 31 30 0 adeb9ef10bc6c100 adeb9ef10bc6c100 adeb9ef10bc6c100 adeb9ef10bc6c100 66 30 61 62 56663435152a04864 63 66 63 61 66 30 61 65 56664335152a04864 66 66 63 66 63 66	0.00	000210	31	37	66	38	31	34	38	66	64	61	36	62	66	38	31	65	1778148fda6bf81e
000C0230 66 39 35 66 61 39 33 39 38 31 1 <th1< th=""> <th1< th=""> 1</th1<></th1<>	0.00	000220	38	61	32	64	38	33	34	35	31	66	30	62	61	32	37	61	8a2d83451f0ba27a
000C0240 30 39 37 64 32 61 66 33 33 64 34 63 30 32 33 64 33 33 64 36 31 33 33 64 34 63 30 32 33 64 33 34 34 31 33 36 33 34 34 31 33 33 36 31 33 33 34 36 31 33 30 30 adeb9ef10bc6c100 c136630152a048c1 000C0270 35 36 36 36 31 33 34 38 63 62 31 33 36 34 38 63 62 36 36 36 36 36 31 33 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 36 </td <td>0.00</td> <td>000230</td> <td>66</td> <td>30</td> <td>66</td> <td>30</td> <td>35</td> <td>66</td> <td>61</td> <td>30</td> <td>33</td> <td>30</td> <td>38</td> <td>38</td> <td>30</td> <td>38</td> <td>31</td> <td>31</td> <td>f9f95fa939889911</td>	0.00	000230	66	30	66	30	35	66	61	30	33	30	38	38	30	38	31	31	f9f95fa939889911
000C0250 61 64 65 62 31 30 62 31 30 adeb9ef10bc6c100 000C0260 63 31 33 36 36 33 30 31 35 36 36 31 30 adeb9ef10bc6c100 000C0260 63 31 33 36 36 33 30 31 35 32 61 30 33 63 62 c136630152a048ct 000C0280 30 30 63 63 30 31 66 63 66 63 66 64 5666643219f0at 000C0280 30 30 63 63 30 31 66 32 37 65 65 33 000C0280 64 30 32 63 63 30 31 66 32 37 65 65 33	000	000240	30	39	37	64	32	61	66	33	33	64	36	31	63	30	32	36	097d2af33d61c026
000C0260 63 31 36 36 31 35 32 61 30 34 863 62 cl36630152a048cb 000C0270 35 36 36 36 31 33 63 31 39 66 66 30 61 62 56666a43c152a048cb 000C0270 35 36 36 31 33 63 31 39 66 66 30 61 62 56666a43c19ff0ab 000C0280 30 30 63 63 30 31 66 32 37 65 53 000C0280 63 30 32 63 63 30 31 66 32 37 65 65 33	0.00	000250	51	64	65	62	30	65	66	31	30	62	63	36	63	31	30	30	adeb9ef10bc6c100
000C0270 35 36 36 36 36 61 34 33 63 31 39 66 66 30 61 62 000C0280 30 30 63 65 30 32 63 63 30 31 66 32 37 65 65 33 000C0220 64 37	000	000260	63	31	33	36	36	33	30	31	35	32	61	30	34	38	63	62	c136630152a048cb
000C0280 30 30 63 65 30 32 63 63 30 31 66 32 37 65 65 33 00C002C01f27ee3	000	000270	35	36	36	36	36	61	34	33	63	31	30	66	66	30	61	62	56666a43c19ff0ab
	00	000280	30	30	63	65	30	32	63	63	30	31	66	32	37	65	65	33	00ce02cc01f27ee3
	0.0	000290	50	27	00	00	30	0.00	00	00	30	91	00	1.0 45	91	00	00	99	4.

Figure 15: Fetching of embedded digitally signed encrypted secret text

Decrypted: b'My ATM pin is 1234. Keep it secret else it will be misused.'

Figure 16: Decryption of embedded digitally signed secret text

Received hash is same as the hash of the decrypted text

----signature verified-----

Figure 17: Decryption of embedded digitally signed secret text

5 Conclusion and Future Direction

The present work amalgamates cryptography, steganography, and digital signature to ensure confidentiality, integrity, availability, and non-repudiation. We presented an efficient hybrid security model using the RSA and rectified AES algorithms for the encryption of secret text and cover images, respectively. The proposed rectifications in the AES algorithm are successfully verified in terms of achieved entropy values approximately equal to the ideal value (i.e., 8), the low correlation coefficient between the original and encrypted image, and less processing time. The experimental results concluded that the proposed system achieved all the security primitives in comparison to the other existing hybrid systems. The present research can be further extended to providing multilevel security to other mediums also such as audio, video, etc. The compression of the images could also be done as a preprocessing step for the efficient use of bandwidth of the network during the transfer of encrypted images.

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Large Group Research Project under Grant Number RGP2/162/44.

Author Contributions: The authors confirm contribution to the paper as follows: study conception and implementation: Shahina Anwarul, Sunil Kumar; analysis and interpretation of results: Shahina Anwarul, Ashok Bhansali, Hammam Alshazly, Hany S. Hussein; draft manuscript preparation: Shahina Anwarul, Sunil Kumar, Hammam Alshazly. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data that support the findings of this study are openly available at https://sipi.usc.edu/database.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

- [1] W. Stallings, *Cryptography and Network Security*. Pearson Education India, 2016. [Online]. Available: https://www.amazon.in/Cryptography-Network-Security-Principles-Practice/dp/0134444280
- [2] L. Yang, Z. Xiong, G. Liu, Y. Hu, X. Zhang *et al.*, "An analytical model of page dissemination for efficient big data transmission of C-ITS," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 9, pp. 16524–16533, 2021.

- [3] Z. G. Xiong, M. Y. Zeng, X. M. Zhang, S. Y. Zhu, F. Xu *et al.*, "Social similarity routing algorithm based on socially aware networks in the big data environment," *Journal of Signal Processing Systems*, vol. 94, no. 11, pp. 1253–1267, 2022.
- [4] U. Ogiela, "Cognitive cryptography for data security in cloud computing," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 18, pp. e5557, 2020.
- [5] A. M. Qadir and N. Varol, "A review paper on cryptography," in *Proc. of 7th Int. Symp. on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, pp. 1–6, 2019.
- [6] S. Dhawan and R. Gupta, "Analysis of various data security techniques of steganography: A survey," *Information Security Journal: A Global Perspective*, vol. 30, no. 2, pp. 63–87, 2021.
- B. A. Forouzan and D. Mukhopadhyay, *Cryptography and Network Security*. Tata McGraw-Hill Education, 2015. [Online]. Available: https://www.amazon.in/Crypt-Network-Security-Forouzan/dp/9339220943
- [8] M. H. Abood, "An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms," in *Proc. of Annual Conf. on New Trends in Information & Communications Technology Applications (NTICT)*, Baghdad, Iraq, pp. 86–90, 2017.
- [9] K. Fenrich, "Securing your control system: The "CIA triad" is a widely used benchmark for evaluating information system security effectiveness," *Power Engineering*, vol. 112, no. 2, pp. 44–49, 2008.
- [10] G. Liu, "Data collection in MI-assisted wireless powered underground sensor networks: Directions, recent advances, and challenges," *IEEE Communications Magazine*, vol. 59, no. 4, pp. 132–138, 2021.
- [11] J. Yu, L. Lu, Y. Chen, Y. Zhu and L. Kong, "An indirect eavesdropping attack of keystrokes on touch screen through acoustic sensing," *IEEE Transactions on Mobile Computing*, vol. 20, no. 2, pp. 337–351, 2021.
- [12] I. Bhardwaj, A. Kumar and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in IoTs," in *Proc. of 4th IEEE Int. Conf. on Signal Processing, Computing and Control* (*ISPCC*), Solan, India, pp. 504–509, 2017.
- [13] A. Bhardwaj, G. V. B. Subrahmanyam, V. Avasthi and H. Sastry, "Security algorithms for cloud computing," *Procedia Computer Science*, vol. 85, pp. 535–542, 2016.
- [14] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," in *Proc. of 3rd IEEE Int. Conf. on Advances in Computing, Communication & Automation (ICACCA)*, Dehradun, India, pp. 1–7, 2017.
- [15] S. Namasudra, P. Roy, B. Balusamy and P. Vijayakumar, "Data accessing based on the popularity value for cloud computing," in *Proc. of Int. Conf. on Innovations in Information, Embedded and Communication Systems (ICHECS)*, Coimbatore, India, pp. 1–6, 2017.
- [16] Z. Chen, "Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm," *Journal of Computational and Cognitive Engineering*, vol. 1, no. 3, pp. 103–108, 2022.
- [17] R. Verma, A. Kumari, A. Anand and V. S. S. Yadavalli, "Revisiting shift cipher technique for amplified data security," *Journal of Computational and Cognitive Engineering*, 2022. https://doi.org/10.47852/ bonviewJCCE2202261
- [18] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li et al., "A 3D model encryption scheme based on a cascaded chaotic system," Signal Processing, vol. 202, pp. 108745, 2023.
- [19] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li et al., "EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory," *Information Sciences*, vol. 621, pp. 766–781, 2023.
- [20] A. Wani and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," CAAI Transactions on Intelligence Technology, vol. 6, no. 3, pp. 281–290, 2021.
- [21] S. Namasudra, "A secure cryptosystem using DNA cryptography and DNA steganography for the cloudbased IoT infrastructure," *Computers and Electrical Engineering*, vol. 104, pp. 108426, 2022.
- [22] A. Gutub, "Boosting image watermarking authenticity spreading secrecy from counting-based secretsharing," CAAI Transactions on Intelligence Technology, vol. 8, no. 2, pp. 440–452, 2022. https://doi. org/10.1049/cit2.12093
- [23] R. Wu, S. Gao, X. Wang, S. Liu, Q. Li et al., "AEA-NCS: An audio encryption algorithm based on a nested chaotic system," Chaos, Solitons & Fractals, vol. 165, pp. 112770, 2022.

- [24] S. E. Jero and P. Ramu, "Curvelets-based ECG steganography for data security," *Electronics Letters*, vol. 52, no. 4, pp. 283–285, 2016.
- [25] M. S. Abbas, S. S. Mahdi and S. A. Hussien, "Security improvement of cloud data using hybrid cryptography and steganography," in *Proc. of IEEE Int. Conf. on Computer Science and Software Engineering* (CSASE), Duhok, Iraq, pp. 123–127, 2020.
- [26] K. N. Jassim, A. K. Nsaif, A. K. Nseaf, B. Priambodo, E. Naf'an *et al.*, "Hybrid cryptography and steganography method to embed encrypted text message within image," *Journal of Physics: Conference Series*, vol. 1339, no. 1, pp. 012061, 2019.
- [27] S. Anwarul and S. Agarwal, "Image enciphering using modified AES with secure key transmission," in *Proc.* of the Int. Conf. on Communication and Computing Systems (ICCCS), Gurgaon, India, pp. 137, 2017.
- [28] B. M. Belkaid, L. Mourad, C. Mehdi and A. Soltane, "Secure transfer of medical images using hybrid encryption: Authentication, confidentiality, integrity," in *Proc. of IEEE Int. Conf. on Computer Vision and Image Analysis Applications*, Sousse, Tunisia, pp. 1–6, 2015.
- [29] M. A. Razzaq, R. A. Shaikh, M. A. Baig and A. A. Memon, "Digital image security: Fusion of encryption, steganography and watermarking," *International Journal of Advanced Computer Science and Applications* (IJACSA), vol. 8, no. 5, pp. 224–228, 2017.
- [30] A. Alarood, N. Ababneh, M. Al-Khasawneh, M. Rawashdeh and M. Al-Omari, "IoTSteg: Ensuring privacy and authenticity in internet of things networks using weighted pixels classification based image steganography," *Cluster Computing*, vol. 25, no. 3, pp. 1–12, 2022.
- [31] X. Liao, J. Yin, S. Guo, X. Li and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," *Computers & Electrical Engineering*, vol. 67, pp. 320–329, 2018.
- [32] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools* and Applications, vol. 80, no. 14, pp. 21165–21202, 2021.
- [33] S. Namasudra, D. Devi, S. Choudhary, R. Patan and S. Kallam, "Security, privacy, trust, and anonymity," in *Advances of DNA Computing in Cryptography*. Florida, USA: Chapman and Hall/CRC, pp. 138–150, 2018.
- [34] S. Kumari, R. J. Yadav, S. Namasudra and C. H. Hsu, "Intelligent deception techniques against adversarial attack on the industrial system," *International Journal of Intelligent Systems*, vol. 36, no. 5, pp. 2412–2437, 2021.
- [35] Z. Niu, B. Zhang, B. Dai, J. Zhang, F. Shen *et al.*, "220 GHz multi circuit integrated front end based on solid-state circuits for high speed communication system," *Chinese Journal of Electronics*, vol. 31, no. 3, pp. 569–580, 2022.
- [36] K. Cao, H. Ding, B. Wang, L. Lv, J. Tian *et al.*, "Enhancing physical layer security for IoT with nonorthogonal multiple access assisted semi-grant-free transmission," *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 24669–24681, 2022.
- [37] K. Cao, H. Ding, W. Li, L. Lv, M. Gao et al., "On the ergodic secrecy capacity of intelligent reflecting surface aided wireless powered communication systems," *IEEE Wireless Communications Letters*, vol. 11, no. 11, pp. 2275–2279, 2022.
- [38] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li et al., "Asynchronous updating Boolean network encryption algorithm," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 8, pp. 4388–4400, 2023. https://doi.org/10.1109/TCSVT.2023.3237136
- [39] E. Milanov, "The RSA algorithm," RSA Laboratories, 2009. [Online]. Available: https://sites.math. washington.edu/~morrow/336_09/papers/Yevgeny.pdf (accessed on 15/09/2023).
- [40] A. Kak, AES: The Advanced Encryption Standard [Lecture Notes on Computer and Network Security]. Purdue University, 2023. [Online]. Available: https://engineering.purdue.edu/kak/compsec/NewLectures/ Lecture8.pdf
- [41] E. Bresson, O. Chevassut and D. Pointcheval, "Dynamic group diffie-hellman key exchange under standard assumptions," in *Proc. of Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Amsterdam, The Netherlands, pp. 321–336, 2022.

- [42] S. Gangan, "A review of man-in-the-middle attacks," *Computing Research Repository*, arXiv preprint 1504.02115, 2015.
- [43] A. M. Ahmadian and M. Amirmazlaghani, "A novel secret image sharing with steganography scheme utilizing optimal asymmetric encryption padding and information dispersal algorithms," *Signal Processing: Image Communication*, vol. 74, pp. 78–88, 2019.
- [44] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques*, Perugia, Italy, pp. 92–111, 1994.
- [45] A. G. Weber, "The USC-SIPI image database version 5," USC-SIPI Report, vol. 315, no. 1, pp. 1–24, 1997.
 [46] M. Guclu, "Multi-level security model developed to provide data privacy in distributed database systems,"
- *Tehnički Vjesnik*, vol. 29, no. 2, pp. 369–378, 2022.
- [47] P. Bharathi, G. Annam, J. B. Kandi, V. K. Duggana and T. Anjali, "Secure file storage using hybrid cryptography," in *Proc. of 6th Int. Conf. on Communication and Electronics Systems (ICCES)*, Coimbatre, India, pp. 1–6, 2021.
- [48] A. Hambouz, Y. Shaheen, A. Manna, M. Al-Fayoumi and S. Tedmori, "Achieving data integrity and confidentiality using image steganography and hashing techniques," in *Proc. of 2nd Int. Conf. on New Trends* in Computing Sciences (ICTCS), Amman, Jordan, pp. 1–6, 2019.
- [49] C. Biswas, U. D. Gupta and M. M. Haque, "An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography," in *Proc. of IEEE Int. Conf. on Electrical, Computer and Communication Engineering (ECCE)*, Cox's Bazar, Bangladesh, pp. 1–5, 2019.
- [50] A. Jain and V. Kapoor, "Novel hybrid cryptography for confidentiality, integrity, authentication international," *Journal of Computer Applications*, vol. 171, pp. 35–40, 2017.
- [51] R. Kumar and P. R. Murti, "Data security and authentication using steganography," *International Journal of Computer Science and Information Technologies*, vol. 2, no. 4, pp. 1453–1456, 2011.