Multi-Layered Hybrid Security Framework for Online Banking Transactions

O. Sarjiyus and I. Manga
Department of Computer Science, Adamawa State University, Mubi, Nigeria.
sarjiyus@gmail.com

DOI: 10.56201/ijcsmt.v10.no6. 2024.pg32.58

Abstract

The concept of information security in the financial industry is not merely an organizational priority, it is a cornerstone of trust, ensuring stability and resilience of the entire economic infrastructure. The financial sector of Nigeria as a crucial pillar of the country's economy is undergoing a transformative digital revolution. As financial institutions navigate the complex terrains of evolving cyber threats, regulatory frameworks and customer expectations, a holistic and proactive approach in information security becomes paramount. This research explores the landscape of information security in Nigeria financial sector addressing key challenges, current practices with a clear focus on emerging trends by strengthening major parameters for safety of online data transmission by seeking to examine common security challenges bedeviling transactions of bank customers with a view to protecting them from all forms of malicious tendencies and threats posed by hackers and attackers and mitigating these attacks using a multi-layered hybrid security framework. For the methodology, data elicitation is primarily done using the Key Informant Interview Method (KIIM) using seven banks namely UBA, GTB, Polaris bank, Union bank, Stanbic IBTC, First bank, Fidelity bank. The secondary method was used draw data from journal articles, lecture notes, conference papers and proceedings while the design of the new system was based on a multi-layered approach, incorporating up to five (5) security parameters in a bid to drastically reduce the challenges and threats to Internet banking.

The system's model design is systematically structured to effectively capture and display key functionalities and expected attributes for optimal output. Various modeling tools, including class diagrams, activity diagrams, DFDs, and use case diagrams, are used, while the database is designed with an entity-relationship (E-R) diagram to ensure a robust framework. MATLAB R2021a processes images imported from the Java platform, with analysis performed on seven standard USC-SIPI gray-scale images in 512x512 TIFF format. These datasets are used to secure customer data post-encryption using a modified RSA technique, achieving high Peak Signal-to-Noise Ratio (PSNR) values and very low Mean Square Error (MSE) values, essential for secure credential transmission.

Keyword: *Cryptography, Cyberthreats, Information Security, Smartcard, Steganography, Transactions*

Introduction

In this modern era, technology has reached its zenith to the point where majority of financial institutions, including banks and their customers, routinely conduct business with the click of a mouse. This is made conceivable utilizing the web.

Web banking is an innovation in the financial server which permits clients to do banking transactions anytime and from anywhere. The use of the Internet by financial institutions to conduct businesses and interact with the market has begun. One of the most important Internet services offered by financial institutions is Internet banking (Al-thobhani & Al-malweri, 2021).

Laukkanan (2016) asserts that the Internet is one of the most widely used business and communication channels ever. This is on the grounds that progressions in ICT has brought about the reduction of the entire globe to a solitary town where it is feasible for one to arrive at the universe of people, places and things in the sparkle of an eye, yet contrasted with the developed world is the fact that the emerging nations are yet to completely have the right stuff and harness the profitable possibilities implanted in electronic banking.

Despite the huge potential outcomes and benefits given by the web and electronic banking, which incorporate transfer of funds with such a lot of ease and convenience, checking of accounts records, payment of bills, accessing account statement over a period and so on. These operations are conceivable whenever and wherever with the global platform Internet inside the comfort zone of the clients without the need to truly show up in the bank premises. However, it has been discovered that numerous factors hinder the effectiveness of Internet banking in virtually every developing economy worldwide. These factors include distrust, fear, manipulation of web content and privacy threats frequently posed by hackers and other intruders.

In addition, Sarjiyus et al. (2019) identify additional factors such as phishing and reputational damage within the context of valuable infrastructure deployment.

In another review, Sarjiyus et al (2019) thought that monetary institutions will end up putting a huge proportion of their clients on the verge of losing sensitive banking credentials and funds. Customers will lose faith in the online banking system if banks do not improve on their security. However, it should be noted that cyber-attacks are possible because e-banking transactions take place on public networks that are susceptible to a variety of security compromise (Sarjiyus et al., 2021).

It is against this background that this research on e-banking security seeks to examine the security challenges bedeviling transactions of bank clients with the end goal of shielding them from malignant assaults by hackers using a Multi-layered Hybrid system that consolidates improved cryptography with steganography algorithms.

Review of Related Works

Steganography and cryptography whenever utilized independently have been known to be exclusively deficient for complete data security; in this manner, a more dependable and viable instrument can be accomplished by consolidating the two strategies (Rahman *et al.*,2023). Consolidating these methodologies can guarantee improvement in secret data security and will meet the prerequisites for security and strength for communicating significant data over open channels. Data security is acquiring quick consideration because of the increment in size and kind of information being communicated over the Internet (Hassija *et al*., 2021). One of the proposed arrangements is the misuse of the upsides of cryptographic and steganographic procedures and their blend into a half breed strategy (Pritilata & Mahmood, 2022). The strategy for this blend has been proposed in many investigates albeit past audits have neglected to appropriately address them. The blend of numerous steganographic strategies with various schemes like cryptography, AES techniques, alteration component, random key generation and key-based security calculations has been audited (Shankar *et al.*, 2020). The quantity of detailed attacks to information security is consistently increasing and is turning into a genuine security challenge. These dangers can be best defeated utilizing cryptographic and steganographic procedures. Current studies explore the blend of the two methods to accomplish a heartier, more grounded and viable structure with better security abilities in contrast with the individual segments when utilized independently (Verma, 2021). An encryption method dependent on joining cryptographic and steganographic procedures for installing and embedding information (Adee & Mouratidis, 2022). For the cryptographic angle, they proposed the utilization of SCMACS which is a compelling information encryption procedure that utilizes the one's (1's) complement technique. It utilizes a symmetric key methodology wherein both the sender and the receiver offer a similar encryption and decoding keys. For steganography, they proposed the utilization of the generally favored LSB strategy. With this, there emerges the issue of key handling/management since a solitary key is utilized for both encryption and decoding which can be compromised (Adee & Mouratidis, 2022). A profoundly gotten steganography method involved a mix of DNA arrangement with Hyper elliptic Curve Cryptography was proposed (ettiyan & Geetha, 2023). This methodology enjoys the benefits of the part strategies to guarantee a more elevated level of correspondence security. To conceal a secret message utilizing this scheme, the image is first changed over into DNA arrangements utilizing the nucleotide to a binary table. There are three essential strides from the side of the sender in this scheme; the first is the pixel values of both the secret message and the cover image should be changed over to their particular DNA trio values by the use of characters to the DNA trio transformation; and subsequently, the trio esteems changed over to the parallel qualities structure (Ettiyan & Geetha, 2023). The last stage includes the use of XOR application on the secret and cover images' binary qualities to produce the stego image. The obstacle of utilizing the hyperelliptic bend cryptography (HECC) in such manner is that in light of the short operand lengths, HECC is usually appropriate for processors which are computationally obliged. Another investigation introduced a staggered restricted information implanting method contained incorporated visual cryptography and steganography (Jadhav *et al.*, 2021). In this investigation, a strategy known as halftoning was utilized to lessen image pixels to make the handling step simple get-togethers a visual cryptographic method is applied to create the offers prior to applying a LSB-based steganographic procedure to hide the offers in all the diverse cover images. The downside of coordinating the framework with visual cryptography is that the differentiation of the transformed and remade image gives off an impression of being tempered with; basically, the contrast of the image is diminished. The mix of a solid encryption plan and steganography was proposed to guarantee the security of classified message during transmission (Sarjiyus *et al*, 2021). This strategy proposed the utilization of AES-128 key encryption method to initially scramble the secret message prior to encoding it into a QR code. Then, at that point, the scrambled message in the UTF-8 configuration is changed into a base 64-bit to guarantee it is viable for additional handling. Then, at that point, another degree of safety is added to the interaction by scrambling the encoded image. At long last, the mixed QR code is stowed away in an appropriate transporter/carrier which is safely sent to convey the secret data. The strategy embraced the Least Significant Bit technique to accomplish the advanced image steganography. At the point when the message is gotten by the beneficiary, the privileged information is removed from the transporter through an interpreting cycle, implying that a four-level security can be accomplished with this strategy during the transmission of a mysterious message (Sarjiyus *et al.,* 2021). The utilization of fast reaction code (QR) in consolidating with AES-128 cannot ensure high level of safety. This is on the grounds that there is an actual assault on the QR code which tries to alter the QR code, changing its tone from dark to white or the other way around, thus supplanting a real QR code with a phony one. An image steganography strategy which used the DES technique for instant message encryption was introduced (Rathor *et al.,* 2022). The strategy utilizes a 16 round and block size 64-bit. Afterward, the K-implies pixel bunching strategy was utilized to group the image into a few fragments and insert the information in each portion. A few bunching techniques were utilized for image division. Division included a huge arrangement of data introduced as pixels with every pixel further having three segments which are Red, Green, and Blue (RGB). Having shaped the groups, a LSB technique is utilized to parcel the scrambled message into K number of portions which are to be disguised in each bunch. In spite of every one of these, the utilization of DES and the way that it utilizes 56-bit key for encryption make it unacceptable and uncertain for use by this application. Cryptography and Steganography if utilized independently have been accounted for to be lacking for the transmission of information because of their inborn shortcomings (Kannadhasan & Nagarajan, 2021). Consequently, a framework dependent on joining the two advancements was proposed in which it will be near impossible for an outsider to penetrate the security of the framework and tamper with secret data. In the proposed framework, a newly created Two Fish strategy was applied for the encryption cycle while an Adaptive B45 steganography procedure was utilized for the steganography.

Methodology

This study employs the object-oriented analysis and design (OOAD) approach, as the system's interconnected components lend themselves well to this method. The use of UML as a visual language allows for clear modeling of processes, applications, and systems, effectively illustrating the system’s architecture.

To conduct this research, a detailed analysis of the existing internet banking security systems used by banks such as First Bank Plc, Fidelity Bank, Stanbic IBTC, and UBA—alongside Polaris Bank's FINACLE 10.8 and intellect TM PRIVACY—was carried out. This provided an in-depth evaluation of current security measures, and a review of recent internet banking security models helped identify specific gaps this research aims to address. Primary data were collected through Key Informant Interviews (KIIM) with critical stakeholders and senior ICT officers from these banks, who shared insights into various operational levels of the system. Additionally, in-person visits to bank branches facilitated direct observation of internal operations and technical processes. For secondary data, lecture notes, newsletters, and journal articles were reviewed to gather relevant information for the study.

The Current Framework

The existing e-banking framework as used in Nigeria is such that the bank gives a token to the client where by the token uses a key alongside an additional entropy source (like the current time, t that is recorded from a clock synchronized on same token or a brief, short time arbitrary CHALLENGE from the server and generated through little control console connected to the token) in a bid to item create fleeting passwords, OTPs which may last as long as a minute and are shipped off the enrollment cell phone of the client. As the OTP is created, the client manually duplicates it from the display and enters it straightforwardly into the browser for transaction to be enabled.

It is obvious that most banks in Nigeria are currently using the Finacle system for online banking transactions. First bank, UBA, Stanbic IBTC and quite recently, GTB are on Finacle while Polaris is on intellect (TN) privacy and Union bank, is on Flex tube. All these systems are based on the One Time Password (OTP) security.

A significant weakness of the current framework is that a Trojan might exploit it to take client delicate information and simply send into the browser. Trojan horses hiding under the windows environment might drop the Dynamic Link Library (DLL) in a bid is register its Class id (CLSID) as a browser helper object in the registry of the windows environment and subsequently, tend to steal (cart away all information entered into the browser). In addition, there is a tendency for the Trojan to install a self-signed root certificate, allowing the intruder to generate SSL connections using official outlook connections on the infected system having web servers, which can be used for malicious purposes against Internet banking systems. Thus, this enables the interloper to host counterfeit financial sites. Such spoofed sites can be utilized to trap a client into utilizing it to go through with transactions, then, at that point, making the intruder to depict himself as a Man- in-the- Middle (MitM) to relay transactions between the client and the bank server.

Furthermore, a seasoned hacker who has the propensity to guess the key used in the encryption process through trial and error is another potential flaw in the current system that allows customer details and credentials to be easily hacked.

Analyzing the Proposed Methods

The new framework depends on forestalling noxious assaults and hacking activities by utilizing a modified and improved scheme for the RSA cryptography (with a second level security added) for the encoding of client card subtleties and server generated CHALLENGE (for which a corresponding RESPONSE string is produced at the gateway). The scrambled subtleties are from that point implanted in an image for onward transmission to the server.

In essence, the banking information is not entered directly into the browser. This is to keep away from pre-uncovering client banking subtleties which makes it defenseless to assaults due to Trojans, Man-in-the-Browsers assaults. Client subtleties are accordingly first encoded in the Card

Reader; as the PKI smartcard is entered into the smartcard reader, its contents are encrypted by the modified RSA algorithm and thereafter obtaining a RESPONSE string before manually entering it into the browser and where a Cover image consequently shows up (from the server) to embed the already encoded subtleties. The so formed Stego image moves to the server via the communications channel.

In the proposed framework since banking credentials are pre-scrambled prior to entering into the browser, the Trojan horse, Man- in- the- browser assaults would have no effect on the encoded credentials. Likewise consolidating the RSA encryption mechanism with LSB steganography (by implanting the scrambled subtleties into the cover image to create a stego image) makes it very hard for attackers to hack client credentials transiting through the network.

The current, conventional RSA cryptography which is susceptible to attacks is changed to get more robust key pairs (Public key *e*, Secret key *d*) which are a function of a newly derived functionality, f created instead of the modulus, n thus making it apparently difficult to precisely figure out the Private (secret) key, d and even factorize the modulus, *n* or *q* (*n*). The additional security layer, t created is feasible since as opposed to utilizing the modulus, n to tie any one of the keys as (*e*,*n*) and (*d*,*n*) a number is gotten and defined by t, lying between *n*-*p* and *n* and specified on the interval, $n\text{-}p<t<n$ and tied to a new key pair (*e*,*t*) and (*d*,*t*) to be used to provide vigorous encryption and decryption process; consequently conquering factorization and brute force assaults to an extremely large extent. Basically, t now serves as the new security layer within the original modulus, *n*. With this, a formidable hybrid security is being formed by integrating the modified RSA with LSB steganography.

Therefore, the new model for the enhanced security in Internet banking can be quantified as:

Client and Server Authentication + Data Encryption + Data Steganography + Certificate Authority (CA) = Security and Reliability.

$$\text{PN packet} = \sum_{i=5}^{layers} \text{.data} + \sum_{i=5} \text{.PDU} \qquad (1)$$

From the perspective of the sender (the user), a PN packet consists of the sum of the protocol with the network parameters and the sum of the data that has been systematically passed through all five layers of security (ALS-layers, 2SSL layers, 1IPsec layer).

At the recipients end

$$\text{Data}=\sum_{i=5}^{layer} + PDU + \sum_{i=1}^{5}, \quad PN\ Packet \quad \text{PDU} + \sum_{i=5}^{layers}.\ PDU + \sum_{i=5}, PN\ Packet \qquad (2)$$

Organization of the Multi-layered Security System.

Level-1 IPsec-this level is a protocol which enables host to host security and protection and information privacy. Principally, the IPsec empowers host to have security and consequently, neutralizing such dangers as man-in- the- middle, Secret key assaults, IP spoofing and so on. The IPV6 is typically integrated into the host operating system. This configuration enables the Service Provider to manage the numerous left IP address providers (for customers and network components) for the host OS. So, for every transaction by the customer using an alternate special IP address, hence making it very hard for the aggressor to launch online attacks. Moreover, the IPsec is an enabler for virtual advanced network which like the end-to-end tunnels by applying Symmetric and asymmetric key cryptography.

Level - 2 SSL and TLS-these are key enablers in the protection of transaction entities. While SSL is a protocol in the network layer saddled with encrypting information as it transits through the channel, /network utilizing encryption system given by RSA when a transaction is carried out between the clients PC and the bank server. While TLS is saddled with creating end-to-end tunnel between host computer Pc and the Bank web server. Whenever a transaction session is established between the customer Pc and the web server, SSL encrypts the data using the During information encryption, a public key is instantly created to encode the information with a relating elevate key age to decode information just for a given meeting of exchange.

Level - 3ALS-these are techniques that are followed to guarantee that deceptions or infection Mali ashy server units end client program don't get to client banking certification went into the program. This is finished utilizing of PKI brilliant card where client qualifications went into the card this card peruser considers. The entered certification, for example, client PIN, challenge and so on. are implemented in the card by employing the RSA cryptographic strategy to generate an encrypted response string. This response string has already been manually typed into the browser, thereby preventing content manipulation issues caused by man in the middle attacks.

Under the ALS alleviation meeting capturing is disposed of since the PKI smartcard embedded card per user is first verified by approved by the bank server while the server is thusly additionally confirmed by the smartcard. a costly method of mutual authentication that could be called handshaking.

Extra boundaries.

Level- 4: This involves making the RSA used in the PKI card tighter and strengthening the ALS further by adding additional, second security layers to the standard RSA.

Level-5 the steganography methodology added further extends the proposed system security thereby enabling the cover image to embed the encoded information and resulting to a stego image whose contents are not detectable to an expected hacker. Consequently, security of the proposed system has likewise gotten a significant lift.

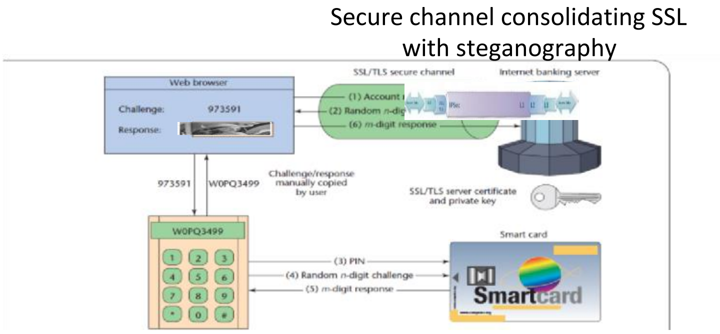

Figure: 3.1 Model of the Multi-layered security system.

In building the system, the design and modelling were carried out using tools which includes the Class Diagram, Activity Diagram and Data Flow Diagram (DFD)

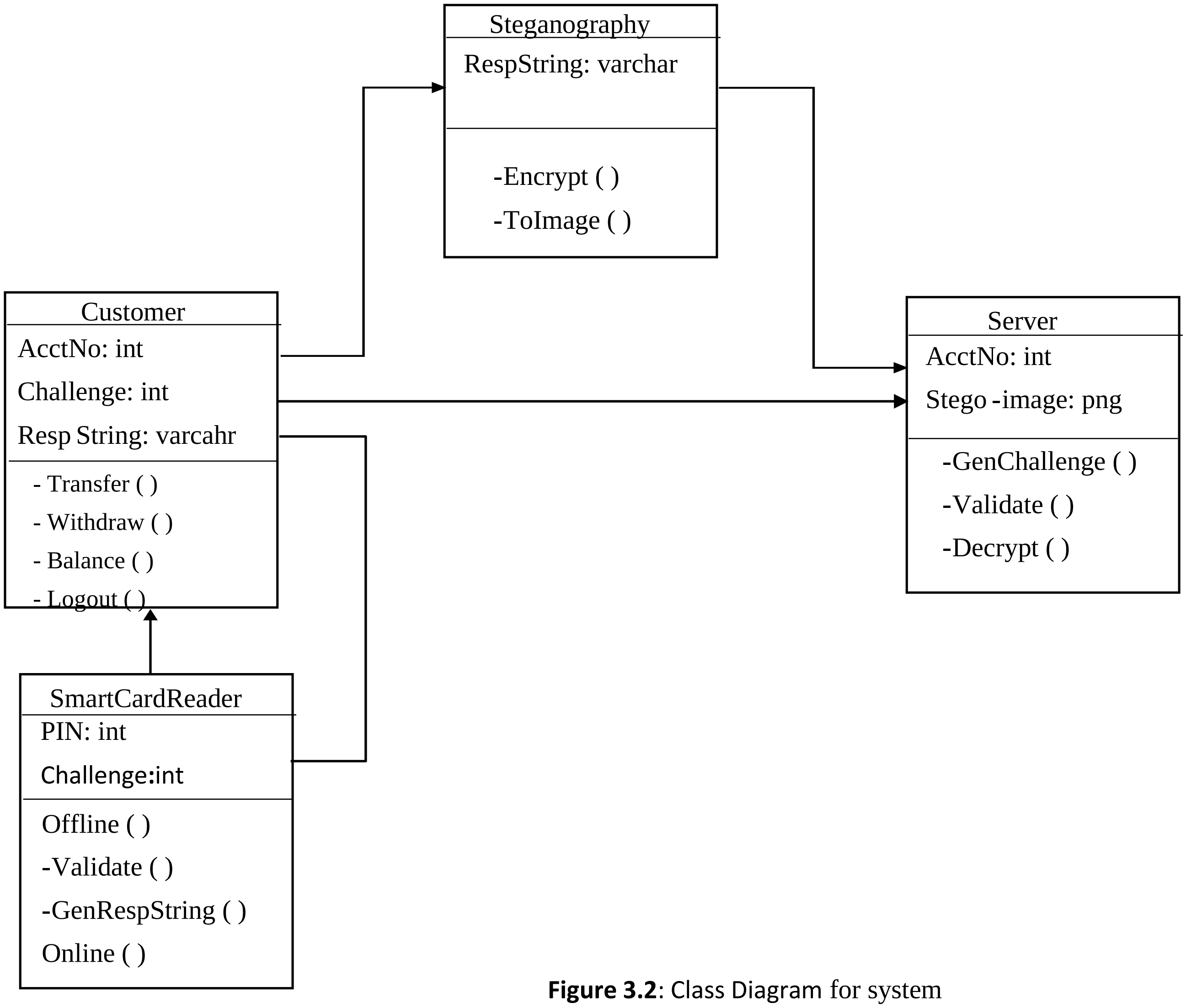

Figure 3.2: Class Diagram for system

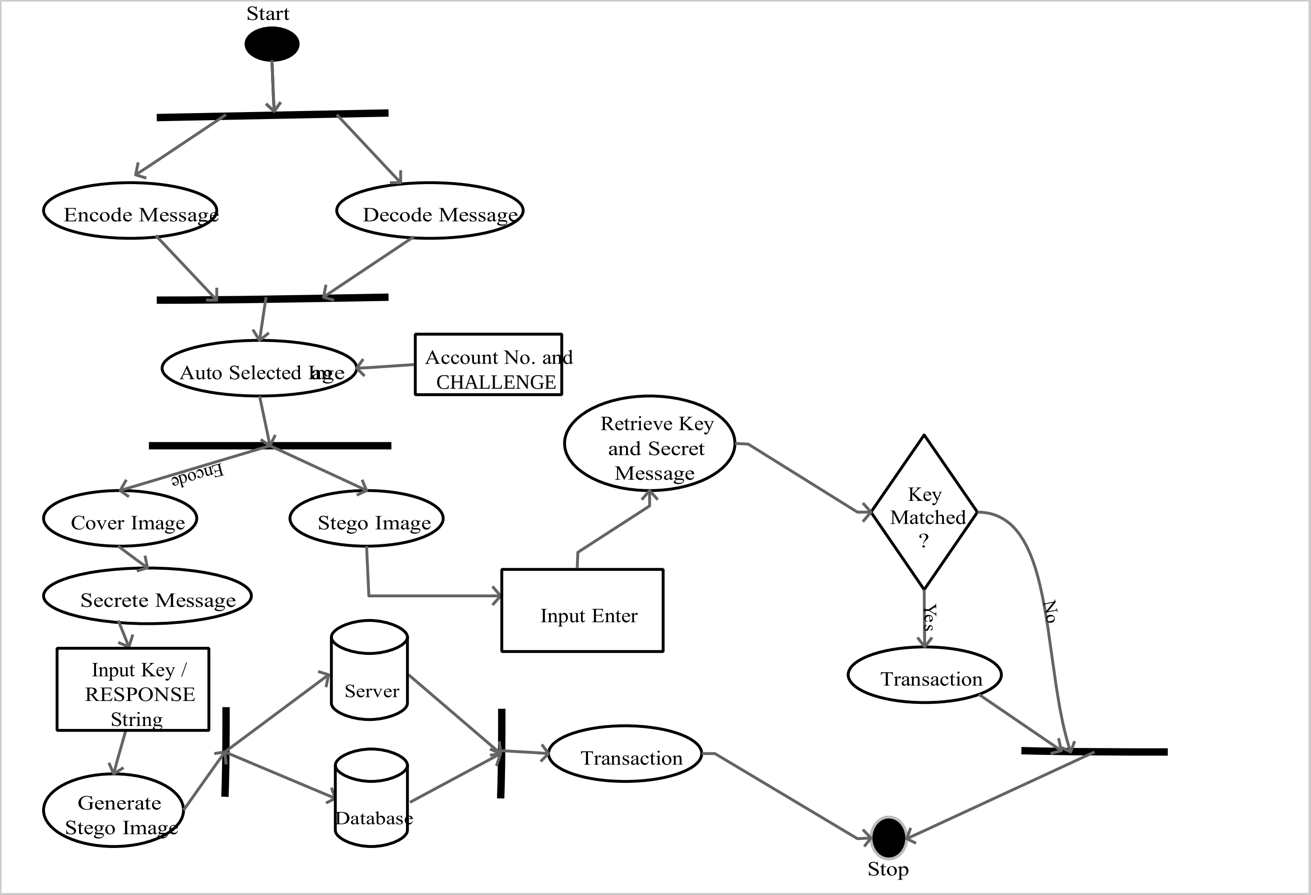

Figure 3.3: Activity Diagram for the system

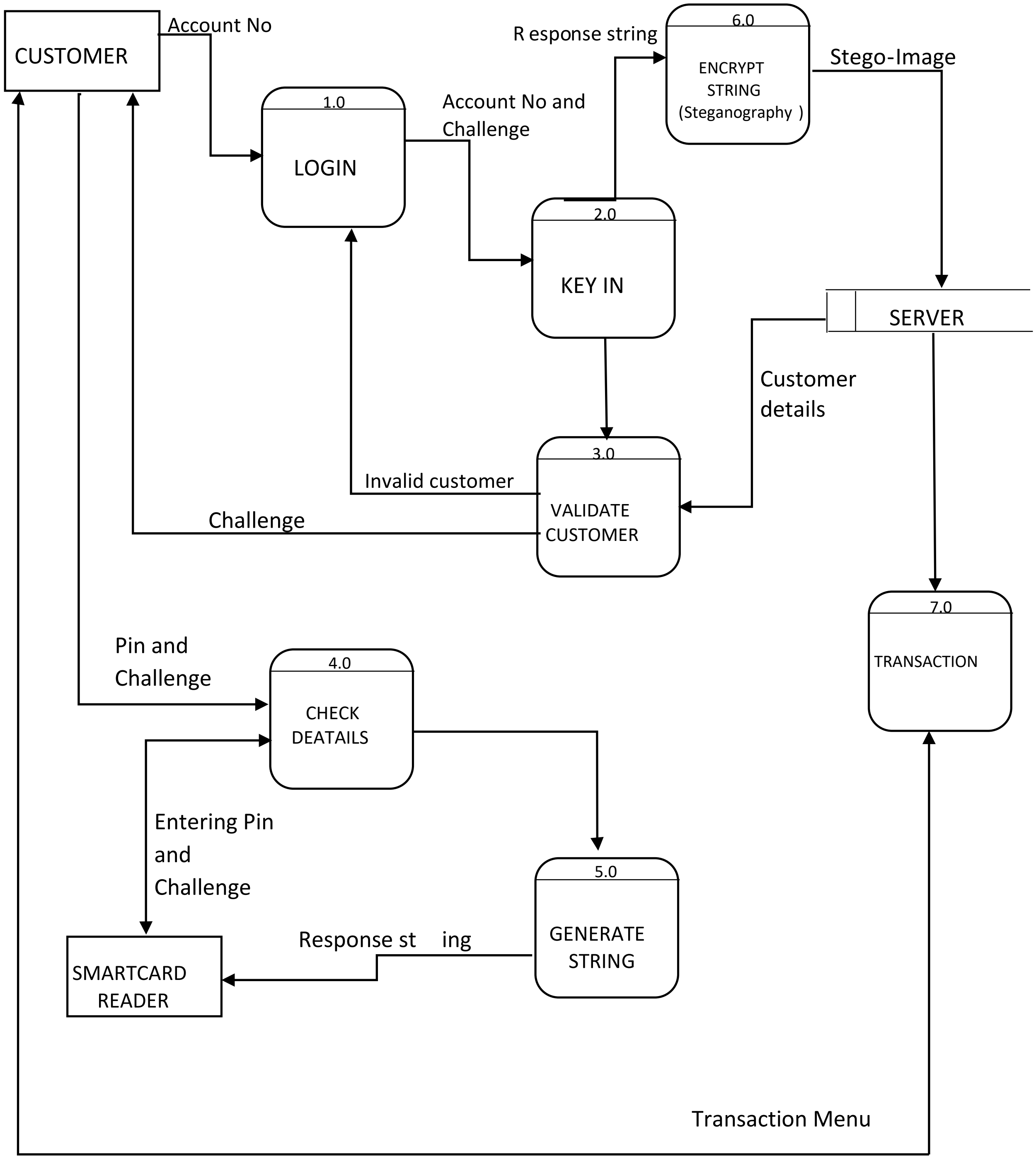

FIGURE 3.4: Data Flow Diagram for System

Existing RSA calculation.

A. Key age
1. Select two enormous indivisible numbers p and q.
2. Figure n = p*q
3. Figure the totient capability ø(n) = (p-1)*(q-1)
4. Gather e with the accompanying condition gcd (e, ø(n) = 1 where: 1<e< ø(n))
5. Select arbitrary 'e' from the rundown
6. Process d from the relation (de mod ø(n) = 1)
7. Send public key (e, n)
8. Send private key (d, n)

B. Encryption

C. Scrambling a plaintext, M utilizing the public key usefulness e,

C=M^e Mod (n)

D. Decryption

The scrambled text is unscrambled using the secret key d as,

D=C^d Mod (n)

Modified RSA Scheme

1. Select two indivisible numbers p and q
2. Complete the modulus n to such an extent that n = p×q
3. Enter for ø(n), ø(n) = (p-1)×(q-1)
4. Plan public key, e structure.

a. Gcd (k, n) = 1 indicates that k and n are coprime.
b. Get t to supplant n

5. Given q<p then put t to such an extent that

(n-p) <t<n where t is the number fulfilling the connection q<p

a. gcd (k, ø(n)) = 1
b. figure d from the connection;

6. Phase 2: Since d*e mod (t) equals 1, the public key becomes (e, t) and the private key becomes (d, t). ECRYPTION

Source scrambles message with public key (e, t) as

c=m^e Mod (t)

Phase3: Decryption

Recipient unscrambles (decrypt) the message with private key (d, t)

M=√ ((c^.d) Mod (t))

Table 4.1: Encryption time for Existing vs Modified RSA Encryption

	Time in Seconds	
Size (KB)	Existing	Modified
51.33	8.08	13.02
483.64	8.76	13.50
512.85	10.54	14.00
4835.44	11.86	14.74
5036.65	13.92	15.86
48335.60	14.45	17.26
50327.40	16.50	19.22
581528.76	20.88	25.01

Table 4.2: Decryption time for Existing VS Modified RSA Decryption

	Time in Seconds	
Size (KB)	Existing	Modified
51.33	8.08	8.08
483.64	8.76	8.76
512.85	9.22	9.22
4835.44	11.86	11.86
5036.65	12.01	13.01
48335.60	13.33	15.53
50327.40	16.00	16.92
581528.76	17.05	18.21

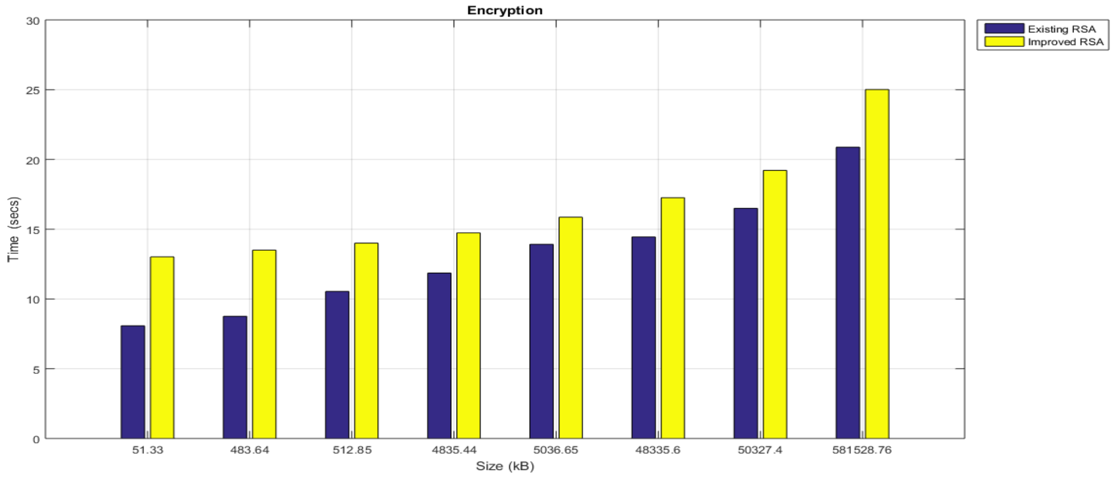

Figure 4.1: Graph showing the Encryption Times for Existing and Hybrid RSA

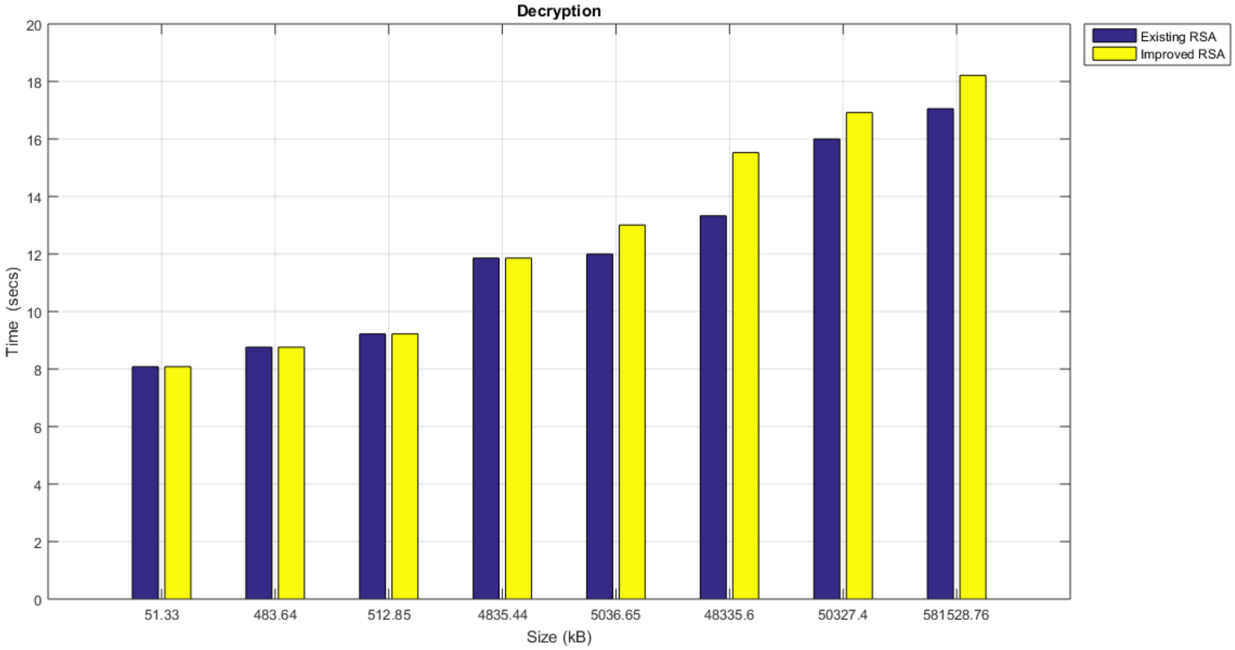

Figure 4.2: Graph Showing the Decryption Times for Existing and Hybrid RSA.

Encryption

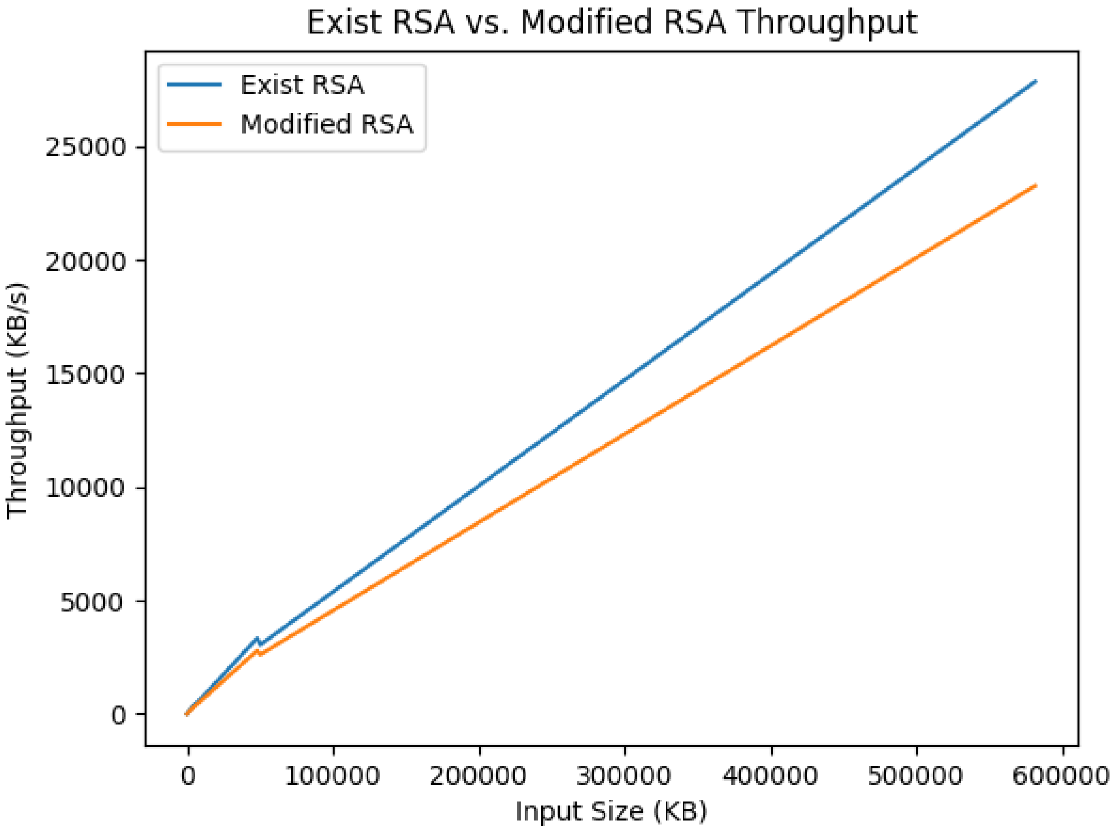

Figure 4.3: Throughput for the Existing RSA vs Hybrid RSA Encryption

Decryption

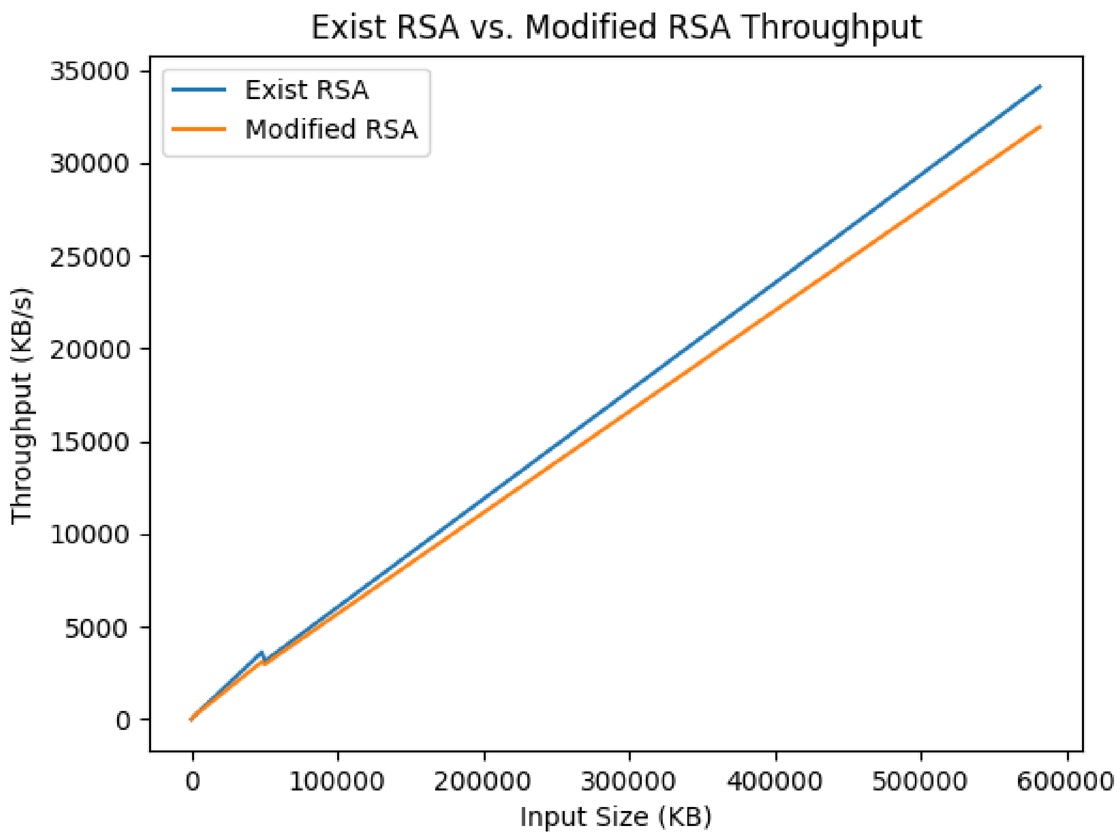

Figure 4.4: Throughput for the Existing RSA vs Hybrid RSA Decryption

Table 4.3: Encryption Throughput for the Existing RSA vs Hybrid(modified) RSA

Encryption Throughput for the Encryption

Size (KB)	Existing RSA Time (Secs)	Hybrid (Modified) RSA Time (Secs)	Throughput for Existing RSA	Throughput for (Modified) RSA
51.33	8.08	13.02	6.353	3.942
483.64	8.76	13.50	55.210	35.825
512.85	10.54	14.00	48.657	36.632
4835.44	11.86	14.74	407.710	328.049
5036.65	13.92	15.86	361.828	317.569
48335.60	14.45	17.26	3345.024	2800.440
50327.40	16.50	19.22	3050.145	2618.491
581528.76	20.88	25.01	27850.994	23261.150

Table 4.4: Decryption Throughput for the Existing RSA vs Hybrid(modified) RSA

Throughput for the Decryption

Size (KB)	Existing RSA Time (Secs)	Hybrid (Modified) RSA Time (Secs)	Throughput for Existing RSA	Throughput for Modified RSA
51.33	8.08	8.08	6.600	6.600
483.64	8.76	8.76	55.210	35.825
512.85	9.22	9.22	55.624	55.624
4835.44	11.86	11.86	407.710	407.710
5036.65	12.01	13.01	419.371	387.137
48335.60	13.33	15.53	3626.077	3112.402
50327.40	16.50	16.92	3145.463	2974.433
581528.76	17.05	18.21	34107.259	31934.5

Table 4.5: Experimental values for Entropy of Cover Image(s) and Stego image

Entropy		
Nature of Image	**Cover Image**	**Stego Image**
Baboon	7.343351	7.343355
Pepper	7.593654	7.593673
Jet plane	6.713514	6.713518
Livingroom	7.295174	7.295349
Pirate	7.236708	7.236714
House	5.752872	5.754073
Walk bridge	7.683081	7.683023

Table 4.6: showing results obtain using LSB with hybrid RSA comparing with the one obtained using LSB with RSA.

Name of image file	Results obtained using LSB with hybrid RSA		Results obtain using LSB with RSA (shetti *et al.,2015)*	
	PSNR	**MSE**	**PSNR**	**MSE**
Baboon	83.231353	0.000309	51.149000	0.499100
Pepper	82.822303	0.000395	51.072800	0.509700
Jet plane	82.631373	0.000355	51.345300	0.477000
Livingroom	82.678325	0.000351	51.166500	0.497200
Pirate	82.921010	0.000332	51.149200	0.499300
House	83.451296	0.000294	51.147199	0.499298
Walk bridge	83.022014	0.000324	51.140189	0.498300

Figures 4.5– 4.13 giving the results for various cover images and corresponding stegoimages with their histograms

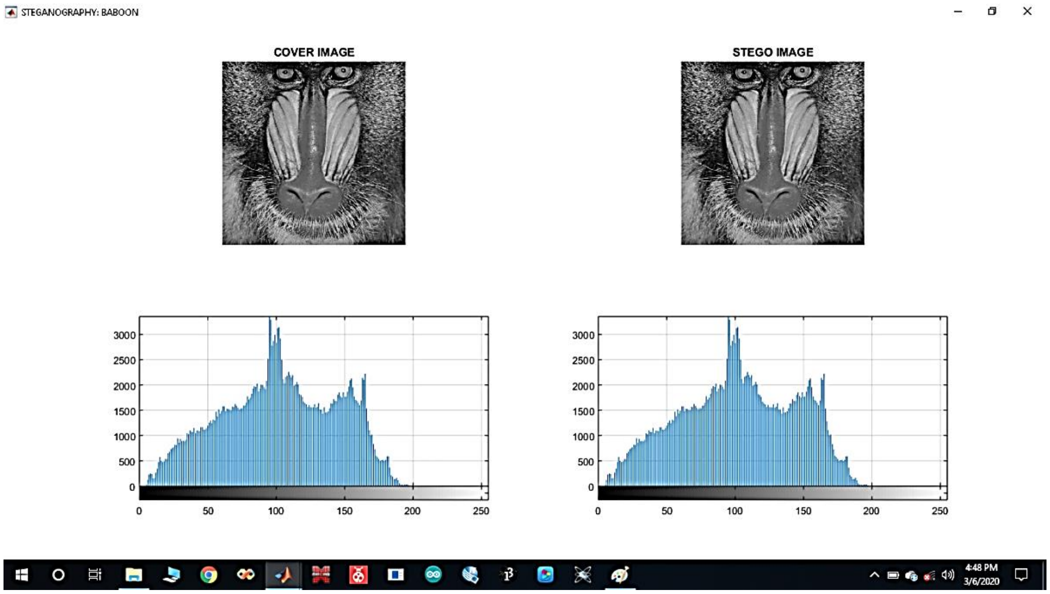

Figure 4.5: Result for Cover image Baboon, its Stego image and corresponding Histograms

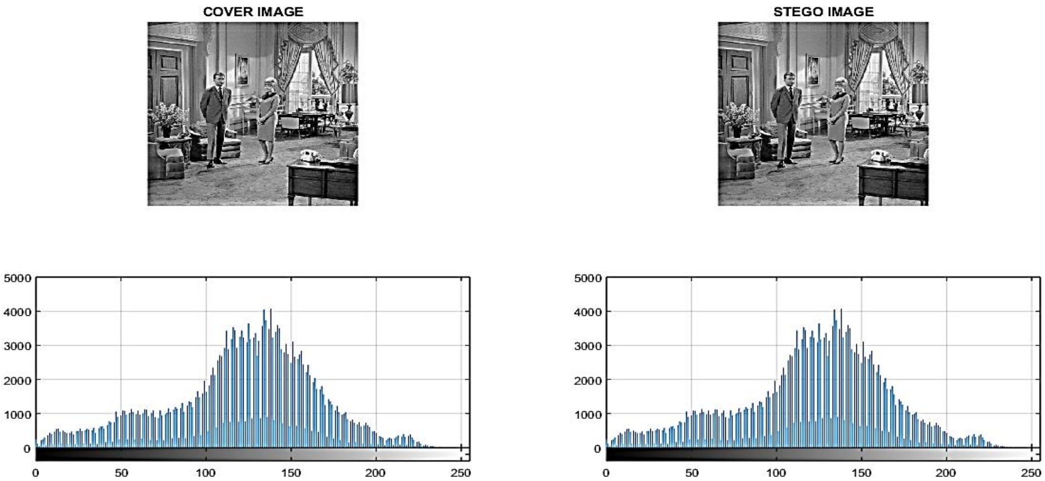

Figure 4.6: Result for Cover image Livingroom, its Stego image and corresponding Histograms.

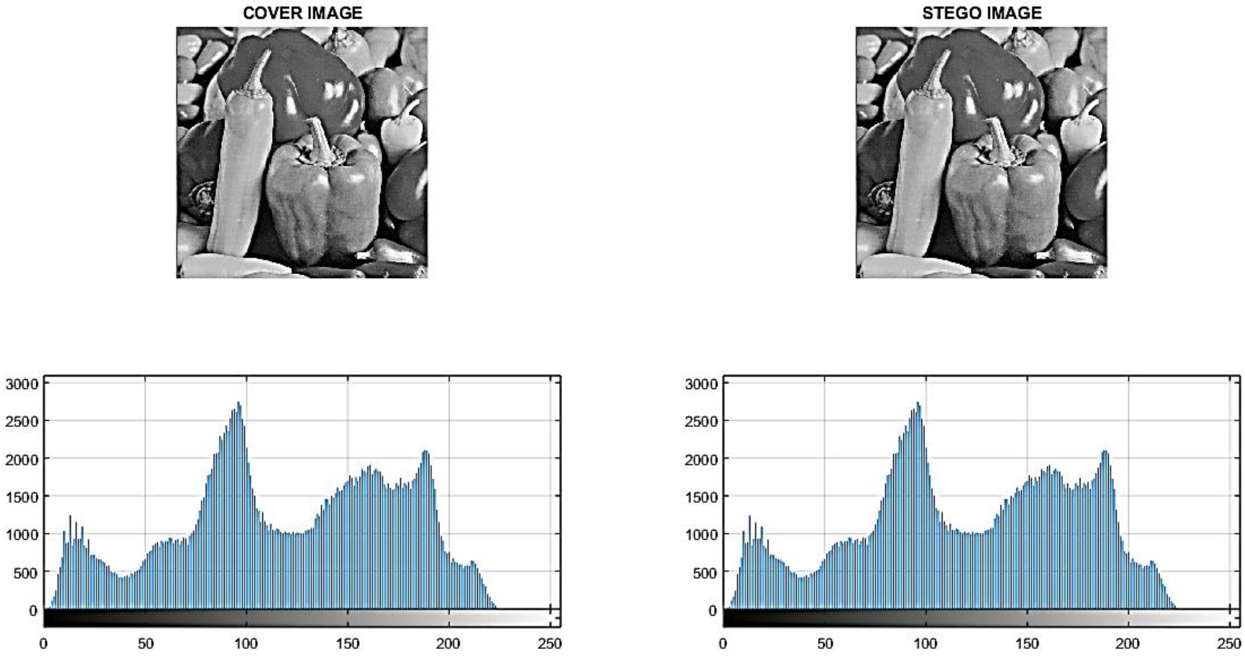

Figure 4.7: Result for Cover image Pepper, its Stego image and corresponding Histograms.

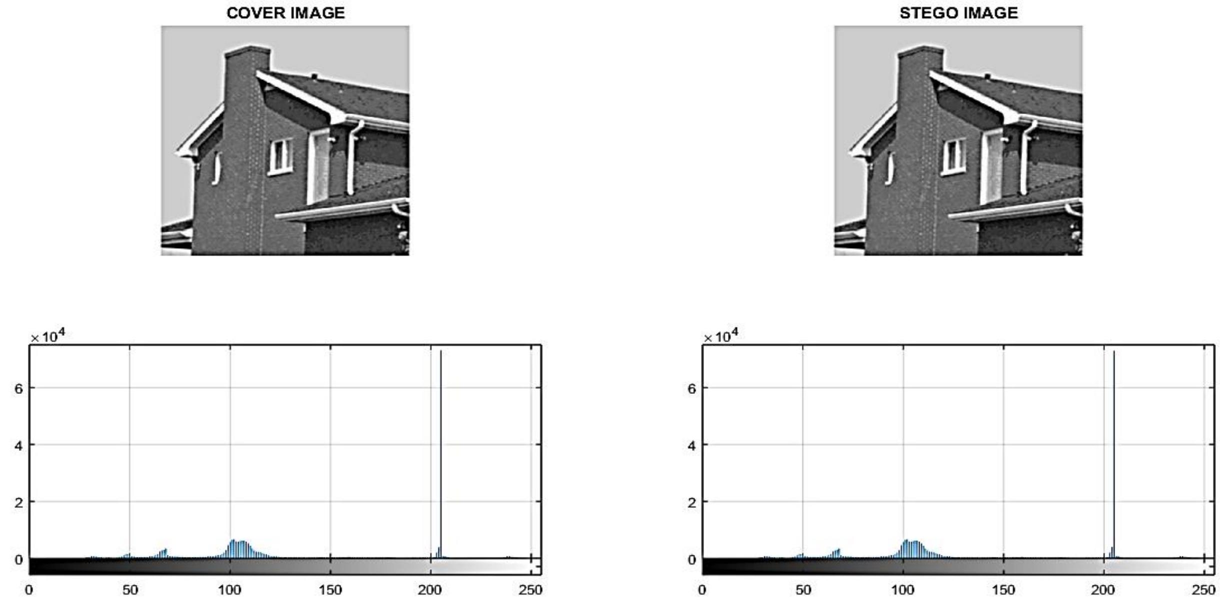

Figure 4.8: Result for Cover image House, its Stego image and corresponding Histograms

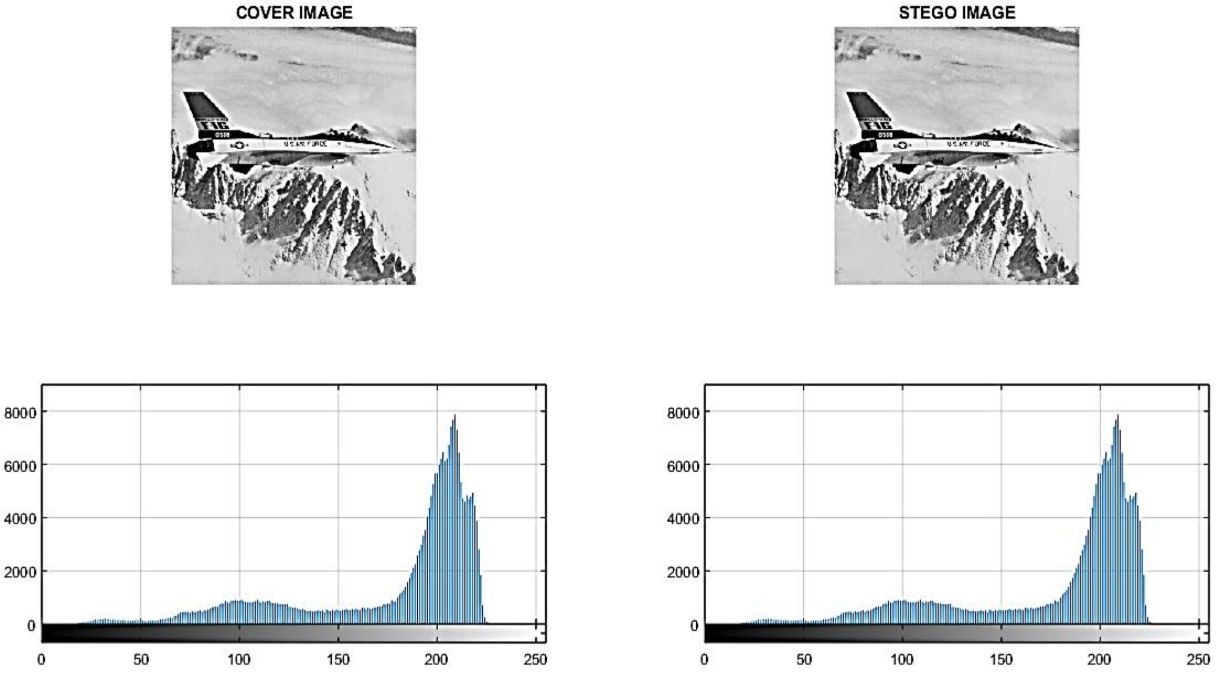

Figure 4.9: Result for Cover image Jet plane, its Stego image and corresponding Histograms

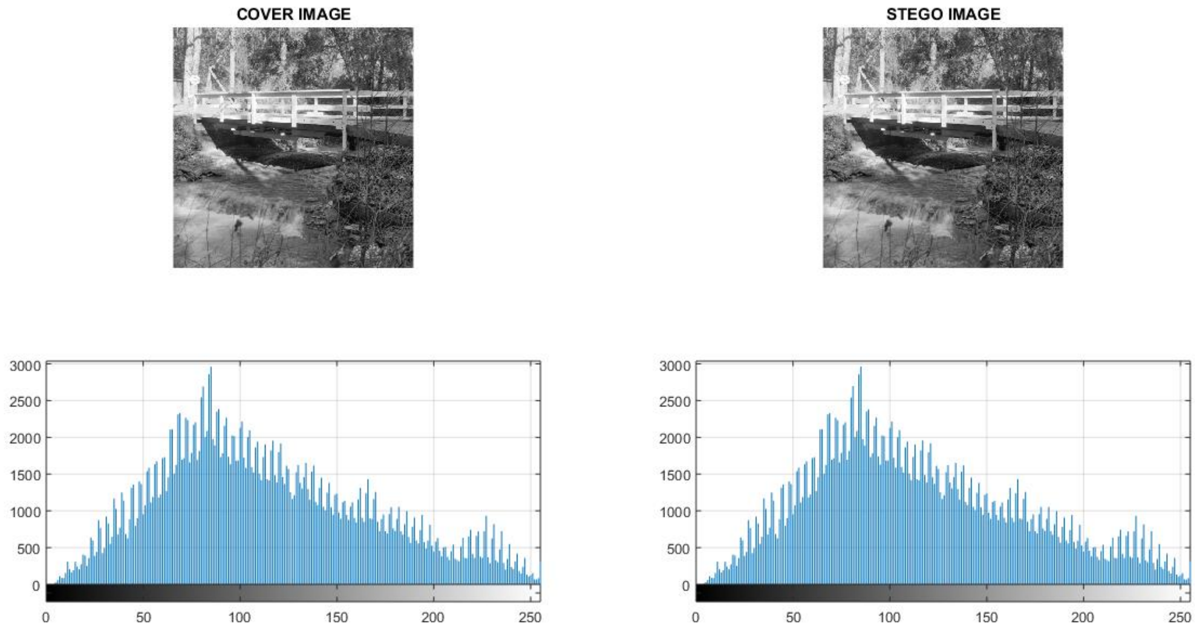

Figure 4.10: Result for Cover image Walk bridge, its Stego image and corresponding Histograms

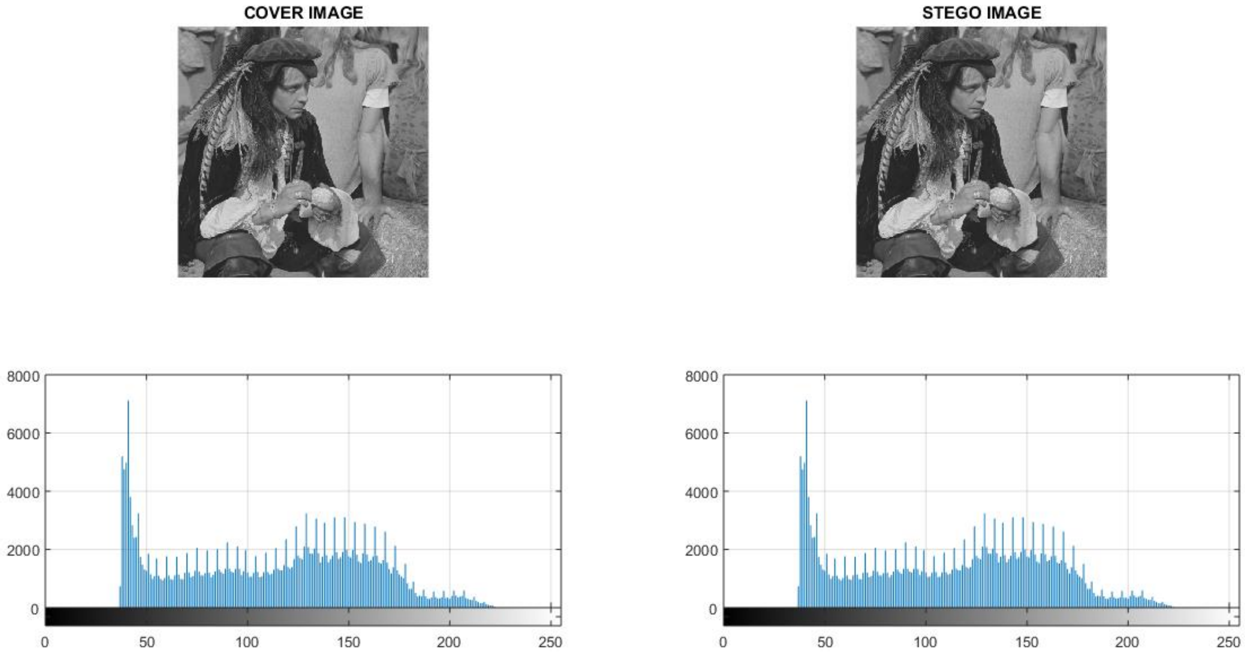

Figure 4.11: Result for Cover image Pirate, its Stego image and corresponding Histograms

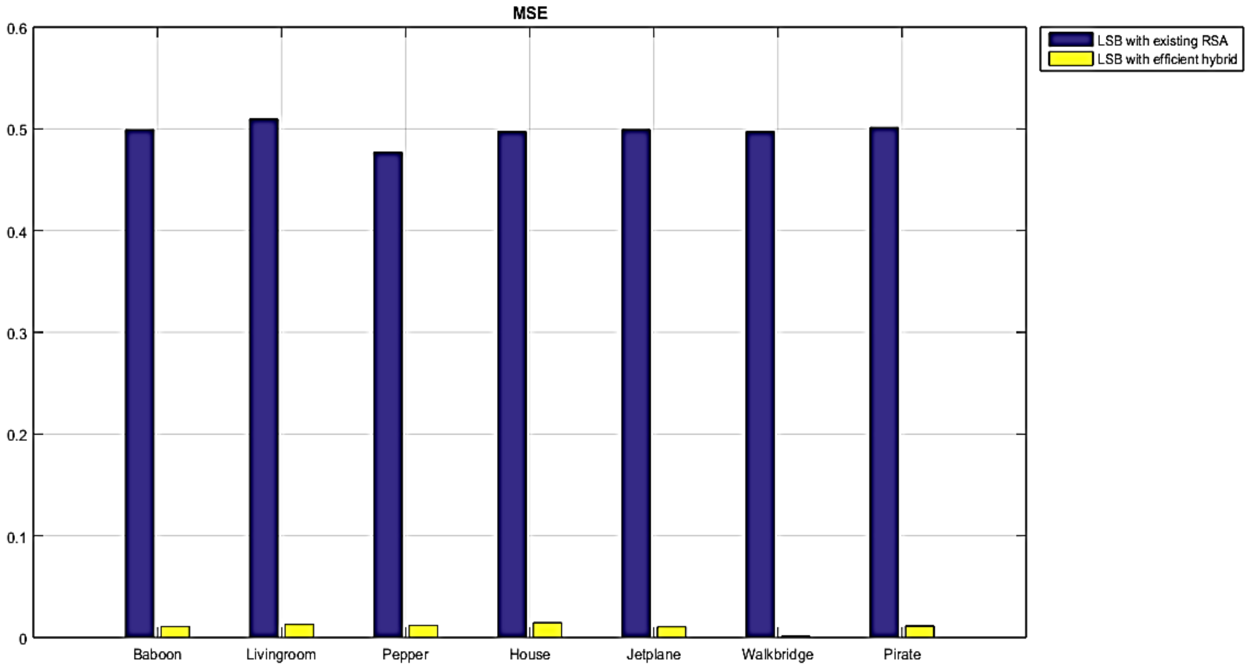

Figure 4.12: Graph showing MSE values for LSB with RSA and LSB with hybrid (modified) RSA

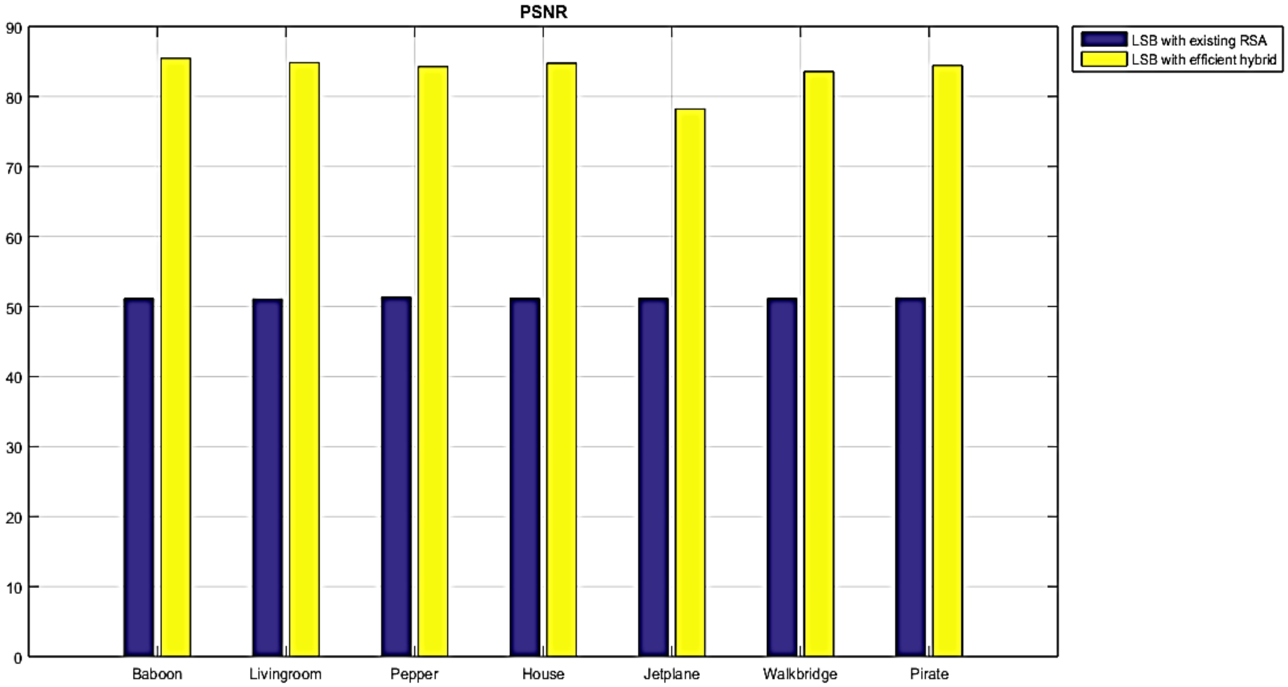

Figure 4.13: Graph showing PSNR values for LSB with RSA and LSB with hybrid (modified) RSA

4.0 DISCUSSION

Generally, the output analysis displayed in table shows that the hybrid RSA algorithm has a straight increase in time complexity during encryption. During decryption, the hybrid RSA takes almost the same time of execution compared to the existing RSA algorithm.

Security and performance are the major parameters used to compare the hybrid RSA with the existing RSA algorithms. From the angle of security of the hybrid RSA algorithm, a mathematical transformation over the modulus *n* is applied in a bid to get a replacement for *n* which clearly makes it hard for an intruder/attacker to find the component factor of modulus *ø*. By this arrangement, the security level of the hybrid RSA scheme is raised to a second layer, security level which improves the security of the RSA scheme is a greater extend. To strengthen the security, a major action is taken to eliminate the possibility of a brute-force attack by modifying the existing RSA such that the *n* distribution in the public and private key is replaced by a new value, *t* with the range (n-q)<t<n while still satisfying same conditions stipulated for *n*; thus the new distribution becomes (e,t) and (d,t) for (e,n) and (d,n) respectively. In terms of performance, the transformation from n to t defined on the interval (n-p) <t<n to some extent tends to increase the time, t complexity of the algorithm done to the formation of an extra, second security layer, but with very little or no noticeable effect on the decryption time(s). With all these, the hybrid RSA algorithm has been used to produce different values of private keys t and ciphers, thus transforming them to larger values to produce more complex cipher values which make the

The hybrid RSA algorithm provides a more robust and secure encryption, effectively countering attacks like factorization and brute-force. The distribution of keys as (e, t) and (d, t) enhances the confidentiality of secret keys. This approach combines the hybrid RSA algorithm with the least significant bit (LSB) image steganography technique, increasing data security. The effectiveness of the hybrid RSA-LSB system is evaluated using standard performance metrics: mean square error (MSE), peak signal-to-noise ratio (PSNR), entropy, and histogram equalization.

The hybrid RSA-LSB system's performance is tested by examining the quality of stego images and measuring PSNR to assess imperceptibility. A high PSNR in grayscale stego images indicates that the human visual system (HVS) is unable to detect differences between the cover and stego images. Thus, a high PSNR and low MSE suggest minimal distortion between the original cover and stego images. MATLAB R2015a was used to implement this new technique, which analyzed seven standard USC-SIPI grayscale images (512x512 TIFF format) as datasets to conceal encrypted customer banking credentials.

Table 4.5 displays entropy values for the cover and stego images, showing a slight increase in entropy for the stego images due to the embedded data. Table 4.6 presents PSNR and MSE results from using both hybrid RSA with LSB and conventional RSA with LSB, where the hybrid RSA system shows lower MSE and higher PSNR as shown by the graphs in Figures 4.12 and 4.13 respectively.

The high PSNR and low MSE values mean the stego image visually resembles the cover image, minimizing detection risk by potential intruders.

Throughput, as shown in Figures 4.3 and 4.4, compares existing and hybrid RSA algorithms during encryption and decryption. For the existing RSA, as file size increases, throughput decreases during encryption—observed as file sizes increase from 4,800 KB to 5,000 KB and 48,000 KB to 50,000 KB. The hybrid RSA algorithm shows a similar trend, but significant throughput increases are observed for larger file ranges (e.g., 500 KB to 48,000 KB and 50,000 KB to 582,000 KB). During decryption, throughput for the existing RSA remains steady within certain ranges before eventually declining as file sizes grow.

5.0 CONCLUSION

This research has gone deep in mitigating security challenges bedeviling the ever-increasing strategies explored by hackers to undermine state of the arts measures put across by experts in cybersecurity.

In the research, the standard RSA cryptography method has modified by tempering with the public key functionality e, to enable it have additional layer of security than combining it with LSB steganography to form a formidable support. This is in addition to other security layers discussed and resulting to five (5) security layers knitted to form a hybrid multilayered system that has the capacity to stem down various forms of malicious attacks ranging from the man-in-the middle attacks, content manipulation and different forms of assaults that are meant to temper with, or steal customer account credentials or even hijack the entire transaction session.

CONFLICT OF INTEREST

Authors declare that there is no conflict of interest.

FUNDING

This study was funded by Tertiary Education Trust Fund (TETFund) with Institution Based Research (IBR) reference number (TEFT/ DR&D/UNI/MUBI/RG/2023/VOL.1. through Adamawa State University Mubi

REFERENCES

Adee, R., &Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109.

Dhawan, S., & Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. *Information Security Journal: A Global Perspective*, *30*(2), 63-87.

Ettiyan, R., & Geetha, V. (2023). A hybrid logistic DNA-based encryption system for securing the Internet of Things patient monitoring systems. *Healthcare Analytics*, *3*, 100149.

Hassija, V., Chamola, V., Agrawal, A., Goyal, A., Luong, N. C., Niyato, D., ... &Guizani, M. (2021). Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *23*(4), 2802-2832.

Jadhav, S. P., Balabanov, G., &Poulkov, V. (2021). Technique for Enhancing the Efficiency and Security of Lightweight IoT Devices. In *Advances in Computing and Data Sciences: 5th International Conference, ICACDS 2021, Nashik, India, April 23–24, 2021, Revised Selected Papers, Part I 5* (pp. 528-537). Springer International Publishing.

Kannadhasan, S., & Nagarajan, R. (2021). Secure Framework Data Security Using Cryptography and Steganography in Internet of Things. In *Multidisciplinary Approach to Modern Digital Steganography* (pp. 258-278). IGI Global.

Pramanik, S., Ghosh, R., Ghonge, M. M., Narayan, V., Sinha, M., Pandey, D., &Samanta, D. (2021). A novel approach using steganography and cryptography in business intelligence. In *Integration Challenges for Analytics, Business Intelligence, and Data Mining* (pp. 192-217). IGI Global.

Pritilata, & Mahmood, M. A. (2022). Strengthening Data Security Using Multi-Level Cryptography Algorithm. In *Advanced Computational Paradigms and Hybrid Intelligent Computing: Proceedings of ICACCP 2021* (pp. 315-324). Springer Singapore.

Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A. A., Ahmed, A., & Haleem, M. (2023). A Comprehensive Study of Digital Image Steganographic Techniques. *IEEE Access*, *11*, 6770-6791.

Rathore, M. S., Poongodi, M., Saurabh, P., Lilhore, U. K., Bourouis, S., Alhakami, W., ... & Hamdi, M. (2022). A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. *Computers and Electrical Engineering*, *102*, 108205.

Sarjiyus, O., Baha, B. Y., &Garba, E. J. (2021). Enhanced Security Framework for Internet Banking Services. *Journal of Information Technology and Computing*, *2*(1), 9-29.

Shankar, K., Elhoseny, M., Kumar, R. S., Lakshmanaprabu, S. K., & Yuan, X. (2020). Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique. *Journal of Ambient Intelligence and Humanized Computing*, *11*, 1821-1833.

Verma, R. K. (2021). Exploring The Robustness of Digital Watermarking Algorithms Based on Transform Function and Machine Learning. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(11), 237-252.