Journal of Information Technology and Computing
https://jitc.sabapub.com
ISSN: 2709-5916

2021 Volume 2, Issue 1 : 9 – 29
DOI: 10.48185/jitc.v2i1.162

Enhanced Security Framework for Internet Banking Services

Omega Sarjiyus [*], B. Y. Baha, E. J. Garba
Department of Computer Science, Modibbo Adama University of Technology, Yola, Nigeria.

Received: 14.04.2021 • Accepted: 12.05.2021 • Published: 30.06.2021 • Final Version: 30.06.2021

Abstract: This research, Enhanced Security Framework for Internet Banking Services is aimed at developing a suitable framework, a system based on consolidating two algorithms, improved RSA with LSB steganography capable of providing secure transmission of customer Internet banking credentials as this is imperative since the online transactions are carried out using public networks that are vulnerable to varying forms of cyber threats and attacks on data confidentiality, integrity and authenticity. In conducting this research, a thorough analysis of the existing banking system used by most banks such as First bank, Stanbic IBTC and UBA, the FINACLE 10.8 and intellect(TM) PRIVACY security system used by POLARIS bank was carried out in order to ascertain the existing security features while at the same time, reviewing the existing, current Internet banking security models in a bid to concretely establish the gaps filled by this research. The data gathered for this research were collected using the key informant interview method (KIIM), visiting banks IT unit and observation of operational procedures and other technicalities as regards Internet security. Lecture notes, newsletters and journal articles relating to Internet banking security were thoroughly reviewed. It was however found that the existing applications were unable to stop offline credential stealing attacks, were also vulnerable to malicious attacks when credentials are stored on customer PCs. Hence, the use of steganography in this research to consolidate cryptographic algorithms (beginning from the use of PKI-cards on card readers). In building the system, the OOAD approach was used with tools such as Class Diagram, Sequence Diagram, DFDs, and UML use cases to capture the system functionalities in a bid to come up with a successful design. MATLAB R2015a was used to process images imported from JAVA platform and analysis carried out on five (5) standard gray USC-SIPI images of size 512 × 512tiff formats as data sets selected to conceal customer data after encryption by the RSA technique yielding very high PSNR and very low MSE values as required for a secure credential transmission.

Keywords: Attack, Credentials, Cyber threats, Functionalities, Transmission.

1. Introduction

For decades, the global platform known as Internet has taken control of the globe. A vast majority of people have been depending on this platform to make life-styles simpler and to speed up everyday activities [1]. Comparatively, of all the spheres making up everyday life, the banking sector is reputed to have benefited immensely more than any other sector from the Internet. Therefore, business experiences between customers and banks are increasingly evolving with technological advancements and shifts in life styles, from the handling of business by customers in person, in

[*] Corresponding Author: sarjiyus@gmail.com

physical banks to having control over the financial services they need through user-friendly interfaces provided by Internet technologies.

The advent of Internet banking has made it possible for banks to deliver easy, highly efficient services to the customers. It is also termed e-banking. E-banking basically, is referring to the use of the global platform by bank customers to carry out various transactions termed financial services [2]. There are various types of financial services provided by e-banking ranging from fund transfers, account verification management and payment of bills. In addition, Internet banking allows bank customers the liberty of accessing banking services in their comfort zones via the banks websites without the need to physically travel to the banks [3]. Financial institutions benefit in the sense that Internet provides them with opportunity to minimize the costs of operations by reducing physical infrastructure, paperwork, and staff support.

E-banking has also posed several security concerns. In spite of the advantages that banks offer to customers via online services [1]. Cyber hackers have established many clever, complicated means of stealing the money of online banking customers, and this menace is growing alarmingly. While online banking has many benefits, security problems also deny bank customers the liberty of using the platform since customers now discover that e-banking exposes customers' financial assets to high threats and risks ([4, 5]). With the rising number of banks deploying financial services through the Internet to their many customers, and this growth is also triggered by a corresponding increase in the number of hackers who are hell bent on committing their skills via the Internet banking system to carry out fraudulent activities. In several reports, it has been reported that the problems of security like phishing threats are being used by hackers to access the accounts of e-banking clients ([6, 7]). Financial institutions tend to drag customers to security risk which ultimately pushes them away if the security of the e-banking platform is not improved [8].

In essence, e-banking services involving customer sensitive and confidential data are conducted across a public network thereby raising security and trustworthiness challenges. On a public network, criminal hackers usually capitalize on existing security lapses to carry out attacks. These criminals are increasingly becoming proficient in the act of posing serious threats such as capturing keystrokes, pharming, spoofing and phishing [9]. In order to mitigate e-banking challenges, the issue of authentication must be overcome by any online banking system, meaning that e-banking account is made accessible only to qualified, genuine persons and not impostors; confidentiality, meaning, all sensitive data involved in the transaction is kept and maintained as secretly as possible; integrity, meaning that unauthorized persons do not have the right to alter, tamper or change customer information and non-repudiation, meaning that all the transactions carried out on an e-banking platform can be traced and verified (when necessary) [10]. Basically, classification of Internet banking security methods is done in accordance to their ability to resist the various types of threats and attacks ranging from stealing offline passwords, breaching of online networks and content manipulation attacks [11].

This research comprises of five sections. The first section introduces the topic by presenting an overview of the research background, the second section gives a brief review of existing relevant literatures in the field of the problem domain, section three discusses the methodology used in building the proposed security system, section four presents and discusses experimental results while the last section, section five concludes the research.

1.1. Objective of the Research

The main objective of the research is to develop and enhanced framework for online banking transactions based on improved RSA algorithms and LSB steganography in order to mitigate the issue of authenticity, confidentiality and integrity of data on transit through an insecure channel.

2. Literature Review

Cryptography and Steganography are known as being independently ineffective in providing protection to information across networks when used separately; thus a more effective and successful mechanism can be accomplished by combining the two techniques [12]. The combination of these strategies would ensure that secret information security is strengthened in order to meet the safety and robustness requirements for the transmission of critical data across insecure networks. Figure 1 offers a systematic approach for the integration of both strategies.

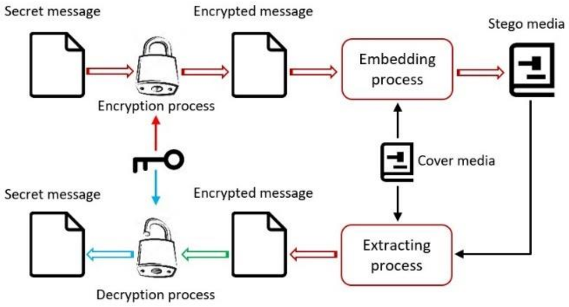


Figure 1. Basic combination diagram for steganography and cryptography [13].

Owing to the variation in data size and type in terms of data transmitted across the Internet, attention is increasingly being paid to information security.A commonly used panacea involves using a combination of cryptographic and steganographic mechanisms and their consolidation to produce a single, improved technique. The basic methodology for combining these schemes has been postulated by several researches, even though previous reports have not provided answers correctly. Combining steganography with cryptographic methods such as key based protection algorithm, AES algorithm, random key generation, etc has been checked [14]. The amount of reported data protection threats has gradually risen to an unprecedented level in the previous years thereby posing a high security risk which can best be overcome by the use of cryptographic and steganographic schemes. Existing research shows that when used separately compared to the individual components, all approaches are combined to obtain an efficient, safer, more effective system, having improved capabilities in terms of security. An encryption method that combines embedding techniques based on cryptographic and steganographic schemes was suggested by [15]. In view of the cryptographic portion, the use of SCMACS was proposed, known to be a highly efficient encryption scheme which takes into account, the complementary method of one (1), and utilizes the symmetric key algorithm. The use of the commonly preferred LSB steganography was recommended by them. However, there remains the problem of key control and management as a single key is being used for both encryption and decryption which can be compromised.

For the security of sensitive user messages to be guaranteed during transit, a consolidation of a robust encryption scheme with steganography has been proposed [16]. By this approach, AES-128 key encryption method is used to encrypt the secret data which is followed encoding it into a QR code. Then the encrypted message is transformed into a format of base 64 in the UTF-8 form in order to ensure its consistency with further processing. Finally, the scrambled QR code is then hidden in a securely transmitted carrier to deliver the secret data. This secret data is obtained from the carrier through a decoding process upon receipt of the information at the receiving end, which ensures that a fourth tiered level security is realized during information transmission.

The use of quick response code (QR) in combining with AES-128 cannot guarantee high security. This is because there is a physical attack on the QR code which seeks to modify the QR code, changing its colour from black to white or vice-versa, thus, replacing a known QR code with a fake one.

A method of image steganography was introduced that used the DES algorithm for encryption of text messages [17]. In the technique, a 16 round and 64-bit block size is used. Later on the pixel clustering of the k-means algorithms being used to cluster the given image into so many segments to embed sensitive data in each of the segments. Multiple algorithms for clustering were used for segmentation of images. A large set of pixel-shaped data was segmented; in which case, each pixel undergoes subdivision into three (3) colour components- red, green and blue (RGB). After the formation of these clusters, the Least Significant Bits (LSB) scheme into K number of tiny segments to be hidden per cluster. The use of DES and the fact that it uses a 56-bit key for encryption, despite all of these, makes it unsuitable and unsafe for this program to use. In extending the performance capacity of the stego image [18], a method was proposed. This approach advocated the use of the Adaptive Pixel Value Differencing method for the steganographic mechanism and Advanced Encryption Standard (AES) used for cryptography.

A gray scale image with the size of about 256 x 256 pixels should be used as the cover image. This range has been cut into pixels of larger sizes and before use, cover images (colour format) are transformed to the corresponding grayscale image format. The information 256 x 256. This range has been cut to pixels of larger sizes, and before use, color cover images are transformed to the corresponding grayscale image format. The information is being embedded in the cover image with the aid of the APVD scheme. The AES scheme is being used to embed the stego image.

The use of adaptive pixel value differencing (PVD) in combination with AES does not guarantee strong data hiding. A better option will even have been PVD combined with LSB to boast the stego image quality before combing with AES

In accordance with the LSB substitution technique [19] on several algorithms such as RSA, DES and AES a performance analysis survey was conducted. Based on the success in any application, the study focuses on the three encryption techniques. It also revealed that since the method utilizes only less buff portion, with very less time for encoding and decoding AES was considered to be stronger than the other two- RSA and DES.

An approach that deploys Blowfish encryption for secret information encryption prior to LSB-based steganography was shown to be effective in containing attacks using known algorithms[20]and[21]. To encrypt secret data, the AES algorithm was used and SHA-1 was used to avoid external attacks. Later, they encrypted the image information using an LSB method. To retrieve the message, the recipient must use the hash that is given by the sender. It is possible to use various types of media to conceal secret data, offering greater levels of protection. Combining this system with bluefish algorithm decreases its security strength since bluefish algorithm cannot provide authentication and nonrepudiation since two people are having the same key. Moreover, the information recovery process, decryption can be very slow.

Classified data embedding by the use of steganography and cryptography has been broadly explained [22]. They suggested a new technique that can protect information without altering the appearance of an image as a courier. To find the matched data bits that correspond to the most significant bit of the cover image, the method of steganography was used. In order to find this similarity, a divide and conquer strategy was used. The matching results were the location of the bit index that they later used to encrypt the DES process. Using DES algorithm to encrypt bit index positions is not safe for the fact that DES algorithm is inadequate due to its 56-bit key being too short.

A modern approach where the data to be hidden is first translated into an encrypted format using an RSA technique has prevented many security risks. The proceeding step deals with inserting the encrypted data into an audio with the aid of LSB audio steganography. The reciepient of the mssage first extract the encrypted text from the audio followed by the application of RSA decryption scheme to decode the message. Consequently, the method increases the merged characteristics of the cryptography and steganography used, while offering a higher degree of data protection [23]. The use of traditional RSA algorithms usually leaves the system vulnerable to factorization and brute force attacks, making it easy for an attacker to penetrate. The Blowfish cryptographic scheme was applied and used for the encryption of the hidden image [24]. The use of Blowfish algorithm was considered due to its strength and speed with high efficiency when compared to the likes of DES, 3DES, AES, RC4 and RC6. In this case, the hidden image is being selected and encoded by applying the Blowfish technique in BMP format, where the encrypted image was then being embedded using the LSB steganography into the video frames. The strategy allows for data integrity, privacy (confidentiality), and non-repudiation. The use of video framing appears to lose data in the event of image transformation in the same way that protection is realized to a large extent.

A new method was proposed by [25] in which the 128-byte key size was used by the RSA scheme for encrypting sensitive data before it is embedded into the cover image using the F5 steganographic algorithm . They DCT coefficients were randomly applied using the F5 steganography to embed the secret message into the cover image.A matrix embedding scheme was used in minimizing the possibility of altering the length of specific information, favouring parameters such as steganographic capacity, increased speed and improved security against threats and attacks. A major downside here is that there are images that cannot be correctly estimated by the F5 algorithm due to the double compression effect. This happens more if the image sent to F5 is already JPEG-compressed.

A study conducted by [26] sought the combination of feature of RSA cryptography and improved LSB steganographic techniques in other to provide “double level” security with high PSNR values so as to make an unauthorized third party not to notice any change in the cover image in relation to the stego image and cause hacking of sensitive data.
Finally, most of the methods reviewed above for combining cryptography with steganography due to one weakness or the other as noted could not produce an excellent stego image with respect to the corresponding cover image. Hence, they produce stego images with very low expected PSNR values and in most cases their mean square error values (MSE) are high.

3. Methodology

The approach used in this study is the method of object-oriented analysis and design (OOAD) since the system components captured for the design are closely related and the use of UML as a visual language makes it possible to model processes, applications and systems in order to express the system architecture design clearly.

In conducting this research, a thorough analysis of the existing Internet banking security system used by most banks such as First bank Plc, Fidelity bank, Stanbic IBTC and UBA, the FINACLE 10.8 and intellectTM PRIVACY used by POLARIS bank was carried out in order to ascertain the strength of the existing security system while at the same time reviewing the existing, current Internet banking security models in a bid to concretely establish the gaps filled by this research. The primary data gathered for this research were collected using the Key Informant Interview Method (KIIM) were discussions were held with critical stakeholders and Senior, experienced ICT officers of these banks were interviewed regarding different operational levels of the system. Moreover, visitations to branch offices of the banks to physically observe internal operations, processes and other technicalities were also carried out. For the secondary method, lecture notes, newsletters and journal articles were reviewed all in an effort to elicit the data needed for this study.

3.1. Analysis of the Existing System

The new online banking system requires the user to type his card details into the system's web browser. The information entered is then encrypted with a higher end key over the Internet network and the entire encoded data is transmitted and sent to the bank server. Even though the encryption of data and algorithms used for the system is checked to have a very high degree of security, but skilled hackers could still be exploit it. Basically, it is because only a key has been encrypted with the data and it will not be difficult to crack the key. Apart from using the encryption method to hide the key, there are no other techniques to consolidate the hiding of such information. A new stronger security feature called a one-time password (OTP) is issued and sent to a registered mobile phone number attached to the card. All of these are to ensure that a legitimate owner is any person using the card and not a fraudulent one. OTP generation however does not take place on specific foreign sites and in many cases, due to network issues. Because of such events, the user is forced to turn to the use of his master key to complete the transaction. One big downside to using the master key is the fact that there is no OTP generation pattern for the given transaction, so hacking the master card can be used for so many fraudulent and malicious transactions.

Most Nigeria banks are using the finacle system. First bank, UBA were bank Stanbic IBTC, Heritage Bank and FCMB all use Finacle 10.8 with the exception of fidelity bank which is still on finacle 7.0. This system hosts the One Time Password Security (OTP) system currently in use.

However, the Intellect (TM) Privacy, which is an internet banking security card used by online banking customers, is the security system for internet banking used by Polaris Bank. It is a plain plastic card that can be used by customers to create a One Time Password (OTP) by inserting the information of the card into the mail sent directly to the server by the browser. Correspondingly, an OTP linked at the server end is the managed phone number that is identified to the server and sent to the customers to enable transactions to be carried out.

If mounted on the client's PC (customer PC), malicious software attacks such as viruses or a Trojan horse can easily record all keyboard inputs (since passwords are entered 'raw' into the browser before being encrypted) and regularly email the data collected to an intruder-controlled predefined address. So the same thing happens to the OTP as it is entered into the browser.

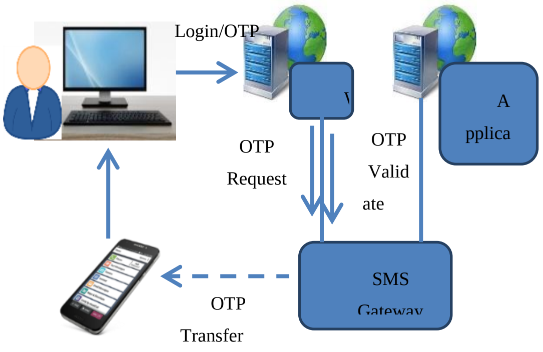


Figure 2. Architecture of the Existing System

3.2. Analysis of the Proposed System

Using improved RSA cryptography in conjunction with LSB steganography for the encrypting customer card details and relevant online credentials, improved RSA cryptography in consolidation with LSB steganographic technique for encoding and embedding customer credentials and other banking details into an image respectively. Steganography is used here to eliminate any risk of having to hack customer credentials which is a major limitation of the current (existing) system.

The proposed system does not allow credentials to be sent “raw’’ straight to the browser, but instead they are first of all encrypted in the tamper resistant card using asymmetric cryptographic algorisms, the RSA and a RESPONSE string is obtained before being entered for onward transmission. The server in turn generates a cover image which is automatically sent to the browser to embed the RESPONSE string. The stego-image so formed is thereafter transmitted to the server through the communication network. This is to enable the system deal with the vulnerability of customer credentials to malicious attacks due to Trojan horses and man-in-the-browser by pre-exposing user credentials. Basically, in order to secure customer private key and other credentials, the use of a certified tamper resistant card and a card reader becomes imperative, so that secret customer transaction including entering a PIN now switch from a potentially vulnerable, untrusted PC to a reader device that is trusted, where interaction takes place through the protected interface of the card reader between the user and the smart card. The security architecture and enhancement of the proposed system focuses on enhancing the Secure Socket Layer (SSL) with two additional layers, an arrangement that places one at the application layer of TCP/IP network and another at the IP layer as described in Figure 3:

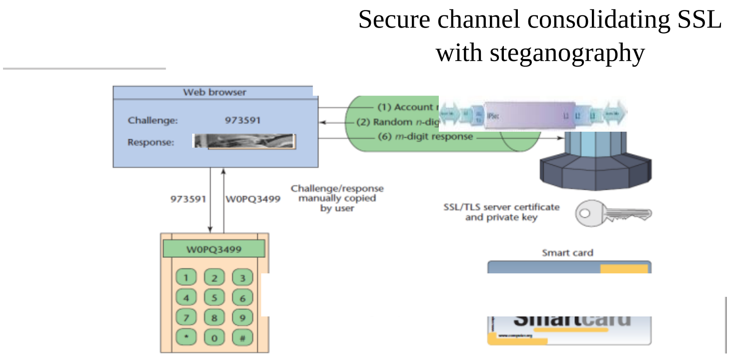
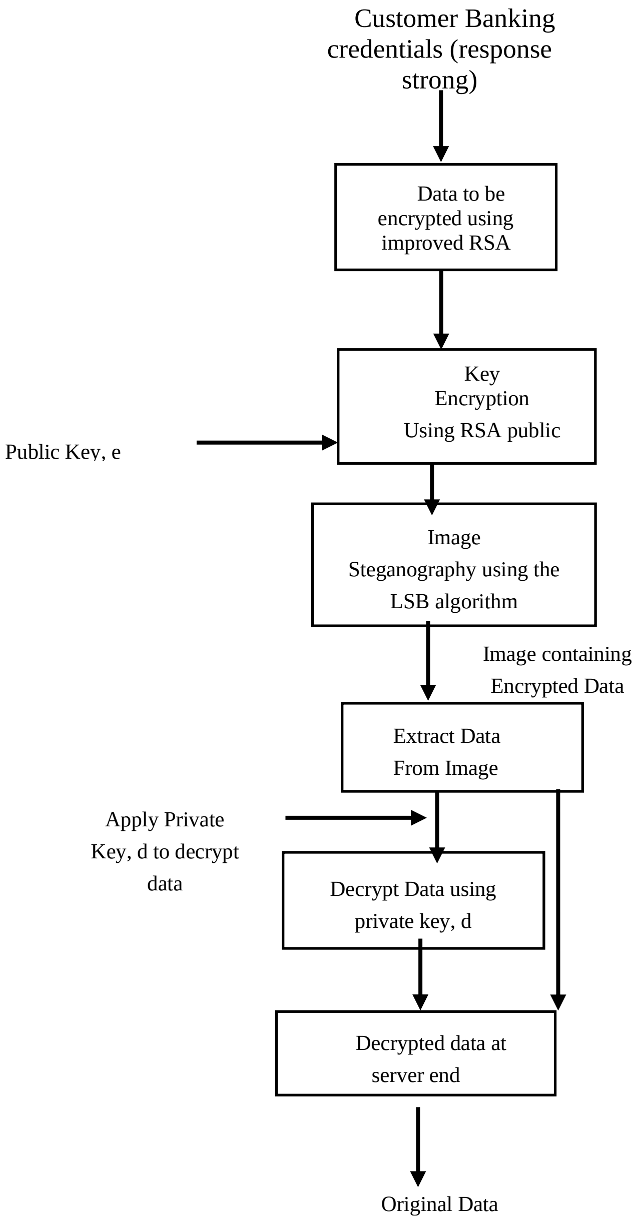


Figure 3. A model of the Proposed Security system

3.3. Building the System

The structure used to build this platform is made up of consists of a full, standard, high-performance and scalable client- server architecture having optimized business platform with extensible data for real-time transaction clients.

For a typical client system, a Personal Computer (PC) is included. The server system is meant to establish access to the resources being used for the e- banking platform, which takes into account, a client support, standing order and bill payment. To generate the transaction RESPONSE string, a public key infrastructure (PKI) tamper resistant smartcard was inserted into a card reader where the customer's ID number, IDc and CHALLENGE get encrypted to generate the string (RESPONSE which when entered into the browser, is automatically embedded into a cover image using LSB steganography and transmitted to the server. It should also be of note that immediately the smartcard is entered into card reader, the bank's server and the smart card authenticate each other using a pair of matched public/private keys (PUc, PRc; PU_B PR_B). The card has the bank's in-built public key $PU_{B,}$ public/private key pair of the user, PU_C and $PR_{C,}$ and an RSA encryption scheme. Often times, financial institutions issue every online customer with a single pair of matched public/private for which a matching digital certificate is provided by some trusted authority that certifies that the username is associated with the public key given and that the username is linked with the given public key and the customer is holding the corresponding private key. This secret key (private key) with the matching digital certificate thereafter creates a mutually authenticated SSL/TLS between the customer's devices (PC) with the server, hence curbing down channel breaking attacks. In building the system for this study, the LSB steganography technique was selected and used due to its simplicity and to a large extent, being highly secure since it is hardly possible for criminal hackers to access information from the stego image without the key. Thus, the use of steganography ensures that the customer's credentials are transmitted securely across the network. At the server side, the encrypted message (credentials) is first extracted from the stego image, then the message is decrypted using the private (secret) key to authorize customer access to the bank's online resources for further transaction. Basically, the proposed system is built to reflect the security model shown in figure 3, with network system architecture depicted in figure 4 and figure 5.


Customer Banking credentials (response strong)
Data to be encrypted using improved RSA
Key Encryption Using RSA public
Public Key, e
Image Steganography using the LSB algorithm
Image containing Encrypted Data
Extract Data From Image
Apply Private Key, d to decrypt data
Decrypt Data using private key, d
Decrypted data at server end
Original Data

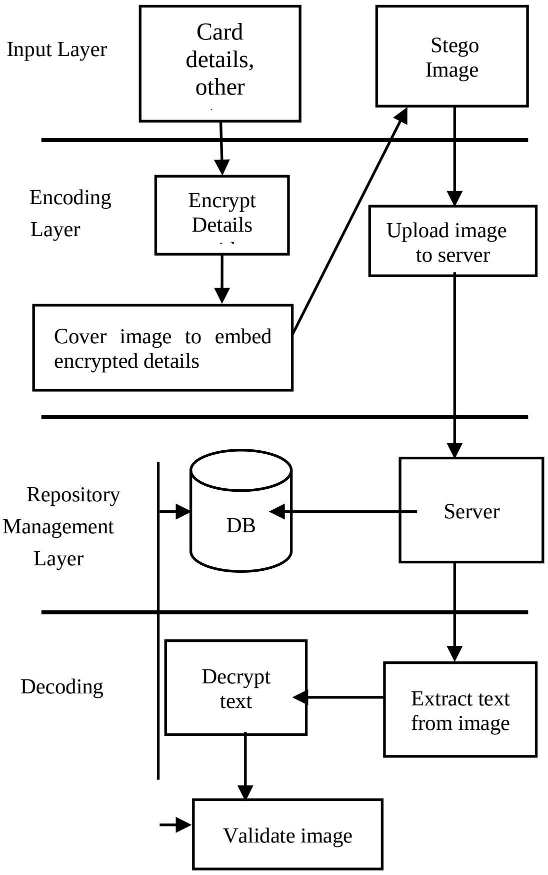


Figure 5. Network System Architecture to ensure user details are securely transmitted over the network

Figure 4. Encryption and steganographic process between client and

The CLASS DIAGRAM for customer interaction with other system functionalities is as shown in Figure 6.

.

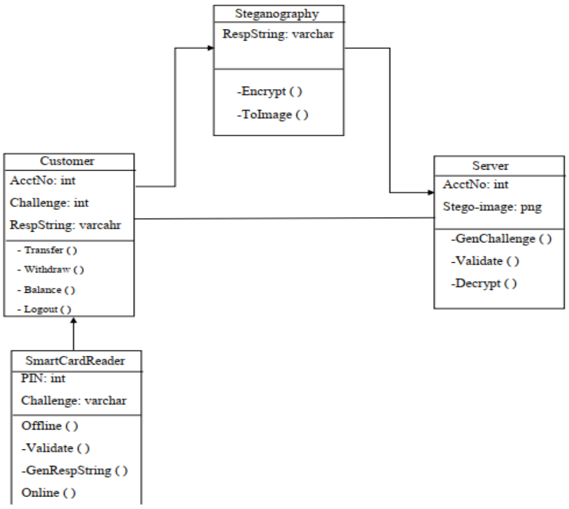


Figure 6. Class diagram for the System

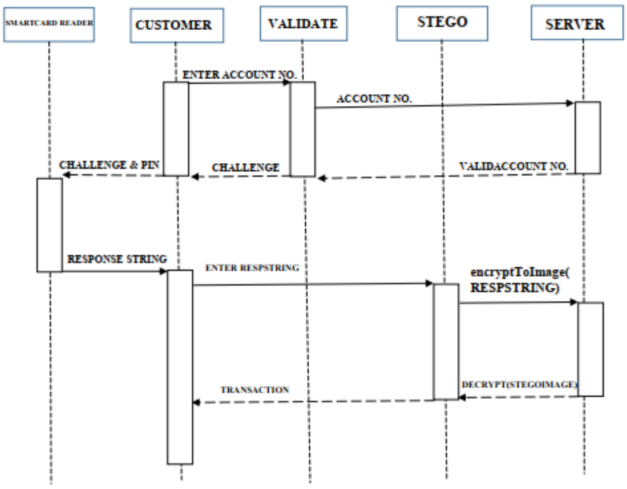


Figure 7. Sequence Diagram for the System

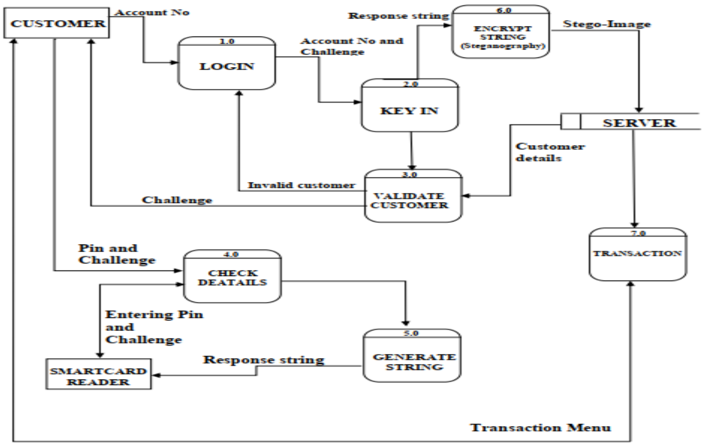


Figure 8. Data Flow Diagram (DFD) for the system

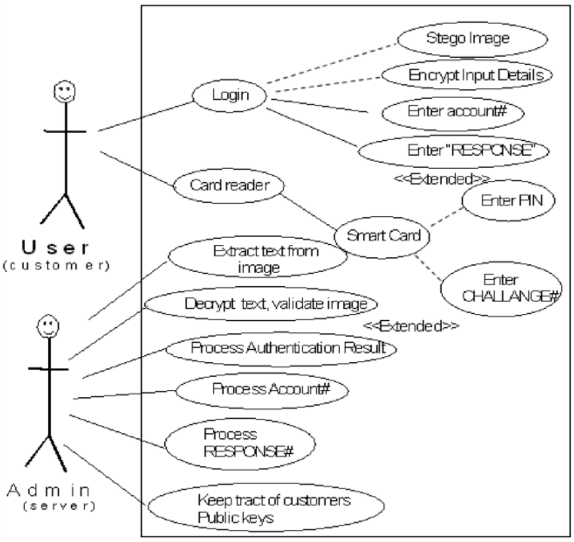


Figure 9. UML Use Case diagram for the Security System

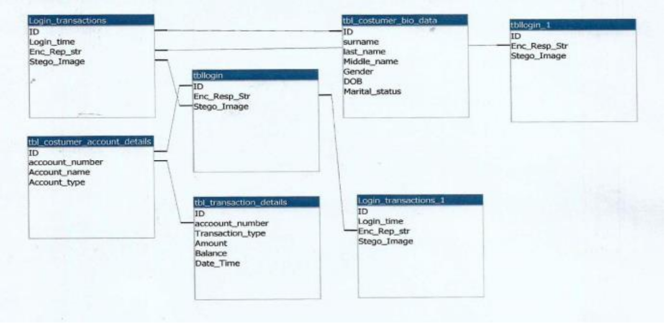


Figure 10. Entity relationship diagram (E-R) of the system

3.4. Process Model for the System.

Phase 1: Link the browser to the server
Phase 2: Input the account number
If the account number exist in the database ,
Then CHALLENGE# is supplied by the server.
Else an INVALID account number message is prompted.
Phase 3: Put a smart card in the card reader.
Phase 4: For smart card authentication, enter PIN#.
If PIN# is correct
A welcome message is then prompted
Else the incorrect PIN# message is shown,
Phase 5: To generate the RESPONSE string, enter CHALLENGE# in a smart card.
Phase 6: Enter encoded “RESPONSE” string into browser.
Phase 7: Image automatically embeds RESPONSE string – STEGO-IMAGE.
Phase 8: STEGO-IMAGE sent to server.
Phase 9:Server removes image, decrypts string, compares content of RESPONSE with CHALLENGE
Phase 10: If “RESPONSE” matches CHALLENGE#
Then customer is authenticated.
Else GOTO phase 2.
Stop

3.5. RSA modification algorithm based on public key

A. Key Generation

1. Select two large prime numbers p and q.

2. Compute the value of the modulus, n.
   n =p*q.
3. Now, Compute Euler's function also called the totient function Φ(n)
   Φ (n)= (p-1)*(q-1)
4. Determine the public key function,e such that:
   1<e<Φ (n) and gcd (e, Φ (n)) =1
5. Select random 'e' from list of co-primes above
6. Compute e transform as:
   f= ((e*2) +1).
7. Compute d from the relation {de mod n = 1}
8. Public key is now (f, n) where 'f' serves as a new public key which will hide the original e value.
9. The Private key is (d, n)

B. Encryption Phase

$C = M^{((e*2)+1)} \bmod(n)$

C. Decryption Phase

$D = C^{d} \bmod(n)$

3.6. Algorithm combining improved RSA with LSB

1. Start
2. Get cover images from USC – SIPI Datasets.
3. Retrieve the grayed image of the original cover image.
4. Transform image into 24 bits or 3 pixels.
5. Get LSB of each pixel.
6. Obtain secret data to be hidden.
7. Convert secret data into binary bits.
8. Apply the rules (XOR).
9. Get the resultant bit after carrying out 8 above.
10. Obtain a resultant stego-image of the original cover image.
11. Compare the resultant stego-image with original cover image to obtain performance parameters; MSE, PSNR, Entropy values and histograms.
12. Stop.

3.7. Measures of Performance of Algorithms Used (Improved RSA with LSB Algorithm)

The main performance metrics used to determine the strength of combining RSA Cryptography and LSB- Steganography algorithms are the Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) obtained after comparing the Cover image to the Stego image.

While the PSNR gives the image quality in which case, the higher the value of PSNR, the greater the Stego image quality. So, the value of the PSNR, has a direct relationship with the quality of the image.

MSE shows the extent of differences or similarities between the Cover image and Stego image. The lesser the MSE value of image, the better its quality and extent of distortion from the image. The MSE therefore has an inverse relationship with the image quality. Thus;

$$MSE = \frac{\sum M\, N\, (T(r,c) - T^{1}(r,c))^{2}}{M * N} \ldots\ldots\ldots\ldots\ldots\ldots (i)$$

From (i); M is the total number of rows, where N is the total number of columns, (r,c) are the respective rows and columns, T is the original (Cover image) and T^1 is the changed image (Stego image).

Again, PSNR gives the ratio of between maximum possible power and corruption noise which distorts the representation of the image. Hence;

$$PSNR = 10 * \log_{10}\left[\frac{R^2}{MSE}\right] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. (ii)$$

Where R is the maximum variation (shift) in relation to the input image data type.

In analyzing Cover image and the Stego image, another parameter that is often used in the entropy, which is defined by the average information contained in an image. It is a measure of the proportion of the details of the image. It is basically measured in bits. Hence:

$$E(P) = \sum_{i=0}^{G-l} P(i) \log P(i) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (iii)$$

Where P(i) is the probability density function (Pdf) of any given image. l and G represent the total number of grey level in the image.

Where the Entropy value of an image is high, then it is said to be having more details.

4. Results and Discussion

4.1. Results

Table 1 and table 2 show the result of encrypting data given different public keys and the result of encryption after transforming public key ‘e’ to

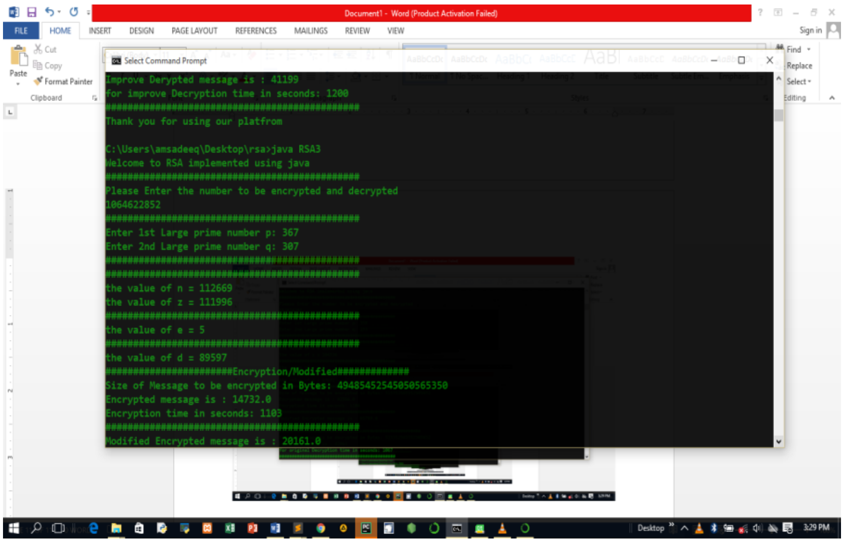
f =((e*2)+1) respectively.

Table 1. Results of encrypted text given different public key ‘e’ p = 7, q = 11

		cipher		
e	d	m=4	m=5	m=6
13	37	53	26	62
17	53	16	3	41
19	19	25	75	13
23	47	9	59	62
29	29	58	31	13

Table 2. Result for p = 7, q = 11

			Cipher	
e (existing RSA)	e (Improved RSA)	d	Existing RSA	Improved RSA
13	27	37	53	71
17	35	53	16	23
19	39	19	25	36
23	47	47	9	16
29	59	29	58	68



```
Improve Derypted message is : 41199
for improve Decryption time in seconds: 1200
##############################################
Thank you for using our platfrom

C:\Users\amsadeeq\Desktop\rsa>java RSA3
Welcome to RSA implemented using java
##############################################
Please Enter the number to be encrypted and decrypted
1064622852
##############################################
Enter 1st Large prime number p: 367
Enter 2nd Large prime number q: 307
##############################################
##############################################
the value of n = 112669
the value of z = 111996
##############################################
the value of e = 5
##############################################
the value of d = 89597
#######################Encryption/Modified############
Size of Message to be encrypted in Bytes: 49485452545050565350
Encrypted message is : 14732.0
Encryption time in seconds: 1103
##############################################
Modified Encrypted message is : 20161.0
```

Figure 11. Interface showing the existing and the improved RSA with p = 367 and q = 307

Table 3 and Table 4 display the result of Performance on various file sizes of the existing and improved RSA encryption and decryption implemented on JAVA platform using an AMD processor, 1.5GHZ, 4GB with 64-bit windows 10 Operating System

Table 3. Encryption time (Existing VS Improved RSA)

	Encryption	
	Time in Second/s	
Size (KB)	Existing	Improved
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. Decryption time (Existing VS Improved RSA)

	Decryption	
	Time in Second/s	
Size (KB)	Existing	Improved
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

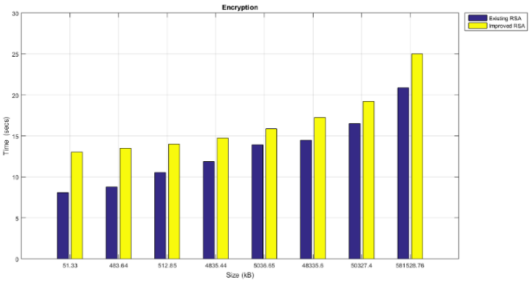


Figure 12. Graph showing the encryption times for existing and improved RSA algorithm.

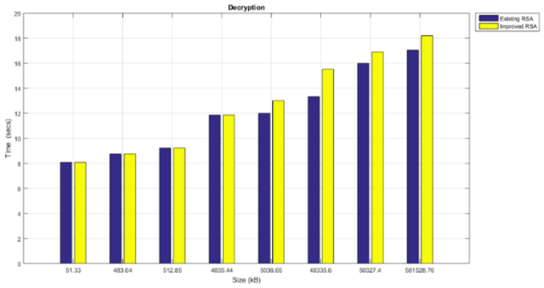


Figure 13. Graph showing the decryption times for existing and improved RSA algorithm.

Table 5. Showing experimental values for entropy of Cover image(s) and Stego image

	Entropy	
Nature of Image	Cover Image	Stego Image
Baboon	7.343351	7.343355
Lenna	6.867662	6.868540
Pepper	7.593654	7.593673
Barbara	7.546314	7.546690
Cameraman	6.904609	6.904623

Table 6. Gives a Comparison Between the Experimental Results in Terms of PSNR and MSE Obtained Using LSB with Existing RSA and LSB with Improved RSA.

Name of image file	Result obtained using LSB with RSA (Shetti *et al*., 2015)		Results obtained using LSB with Improved RSA	
	PSNR	MSE	PSNR	MSE
Baboon	51.149000	0.499100	83.231353	0.000309
Lenna	51.072800	0.509700	82.822303	0.000340
Pepper	51.345300	0.477000	82.822303	0.000395
Barbara	51.165500	0.497200	82.725789	0.000347
Cameraman	51.149200	0.499300	77.001414	0.001300

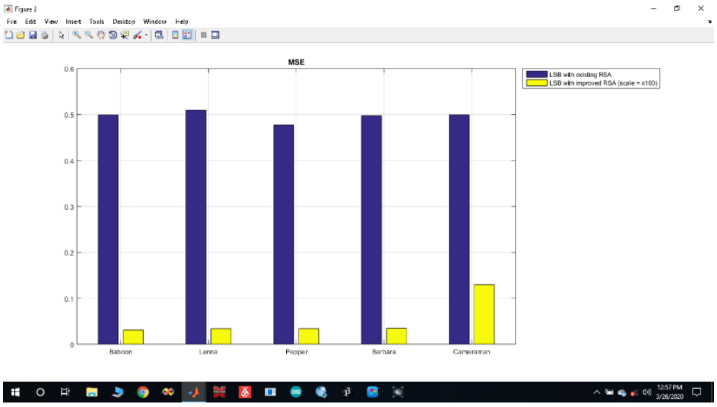


Figure 14. Graph showing MSE values for LSB with RSA and LSB with improved RSA algorithm

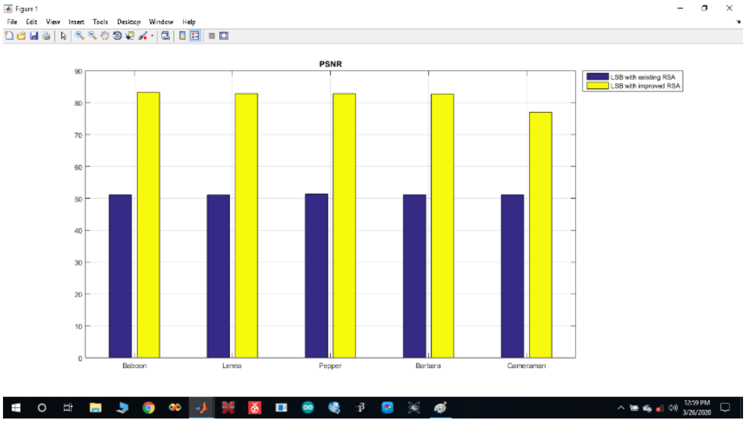


Figure 15. Graph showing PSNR values for LSB with RSA and LSB with improved RSA algorithm

Figures 16 – 20 gives the results for various cover images and their corresponding stegoimages with their histograms

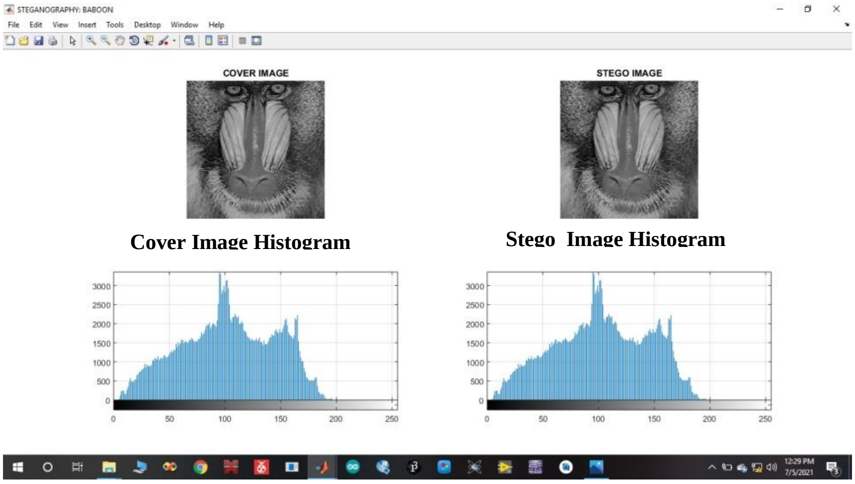


Figure 16. Shows the result for Cover image Baboon, its Stego image and their corresponding Histograms

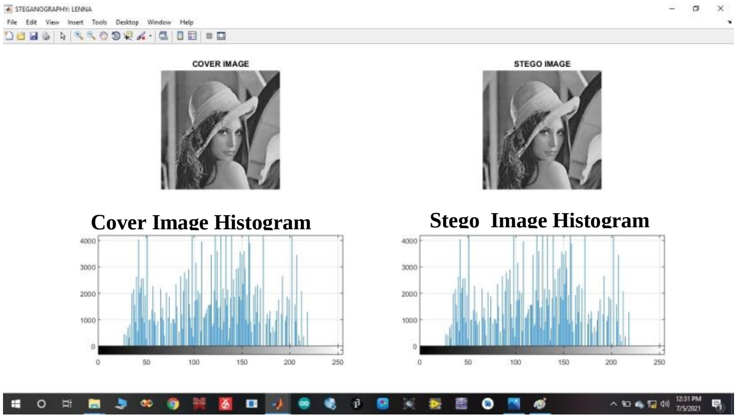


Figure 17. Shows the result for Cover image Lenna, its Stego image and their corresponding Histograms.

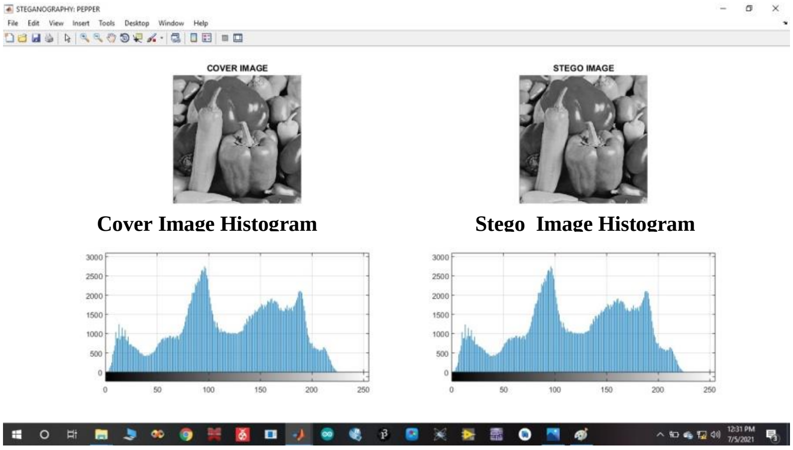


Figure 18. Shows the result for Cover image Pepper, its Stego image and their corresponding Histograms.

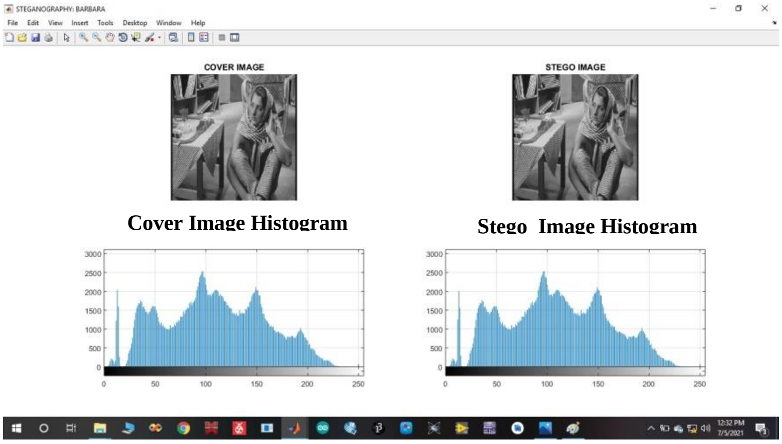


Figure 19. Shows the result for Cover image Barbara, its Stego image and their corresponding Histograms.

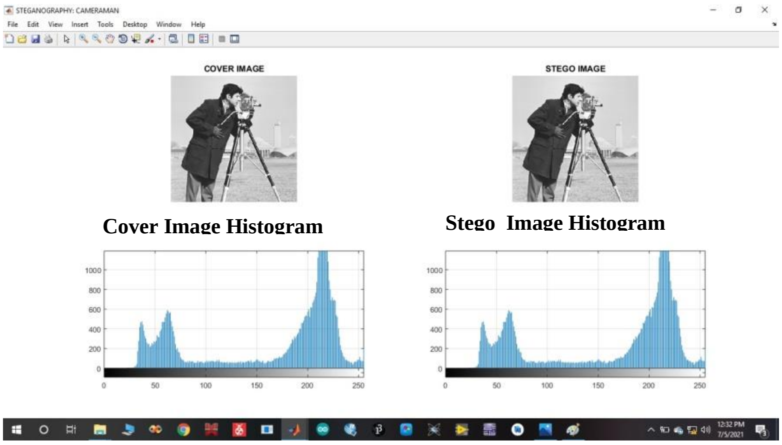


Figure 20. Shows the result for Cover image Cameraman, its Stego image and their corresponding Histograms.

4.2. Discussion

This research presented of public key values ‘e ’that have been assessed and thoroughly checked based on two criteria-Security and Performance; the premise upon which the modified RSA algorithm is compared with existing RSA algorithm. As regards Performability, transforming the public key functionality from ‘e’ to f = ((e*2)+1) slightly increases the time complexity of the algorithm due to key generation and encryption process but has no effect on the decryption process this is also illustrated in Figure 12 and Figure 13.

With regards to Security, the improving the RSA scheme on the basis of public key ‘e’ transformation to f = ((e*2) +1) produced more complex ciphers than the original RSA scheme. Hence, various values of public key ‘e’ have been seen to produce different values of private keys and cipher then converting to new, larger value which produced more complex cipher values and makes the improved RSA algorithm more secure especially against factorization and brute force attacks. This is shown in Table 2.

The framework of this research has been implemented on an improved RSA encryption algorithm with LSB image steganography technique to improve the confidentiality of the customer’s credentials. The strength and performance of the LSB-Improved RSA scheme was examined and evaluated in the context so many performance criteria-The Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Entropy value and histogram equalization.

Basically, the performance of the proposed merged, improved RSA-LSB technique is determined by measuring the imperceptibility of the Stego image quality. This is a measure of how much difference in terms of distortion, caused as a result of hiding data in the original Cover image. A higher Stego image quality implies better information hiding. The Stego image quality is therefore measured using the Peak Signal to Noise Ratio (PSNR). So, larger PSNR value of a grey scale Stego image will make it almost impossible for the Human Visual System (HVS) to differentiate between the Cover image and the Stego image. Hence for better result, it is important to obtain very high PSNR and low MSE values (Since MSE gives a measure of the distortion of the Stego image in relation to the original Cover image). So low MSE implies low distortion or variation of the stego image from the original Cover image.

This new technique with improved security was implemented on MATLAB R2015a and the analysis carried out on five (5) standard grey USC-SIPI images of size 512 x 512 tiff formats, as data sets and selected to conceal fixed sizes of secret customer banking credentials (encrypted as Response String).

Table 5, shows the entropy values obtained by processing the Cover images and Stego images. The entropy values of the images obtained revealed clearly that the values of the Stego images are evidently higher compared to those of the Cover images. This is due to the fact that the Stego image is holding some hidden information.

Table 6 gives the results of PSNR and MSE values obtained using improved RSA with LSB algorithm and the ones obtained using LSB with RSA algorithm.

By comparing the MSE and PSNR values of all the images; MSE of the images used are less while PSNR of the images in the new system (Improved RSA and LSB) are much higher than those obtained from the existing (RSA with LSB) Technique. This is shown and supported by the graphs in Figure 14 and 15 respectively.

Essentially, very high values of PSNR and very low value of MSE are required in getting output image (Stego) almost nearly the same with the input Cover image; thereby giving a better result. Very high PSNR values obtained in this research imply that the stego images obtained appear almost the same to the human vision with very little or no distortion. Hence, the stego image is safe from any suspicion of concealing sensitivecustomer banking credentials by potential hackers. Also the very low MSE values obtained means better quality of stego images having good similarity with the cover images. Hence, the results reveal that the improved method has higher PSNR values ranging between 78 dB and 84 dB and much lesser MSE values than those obtained by Shetti *et al*.(2015) and Sandeep *et al*. (2018) which is an indication of the suitability of the improved method in securing online banking transaction.

Figures 16, 17, 18, 19 and 20, Shows the various Cover images, their corresponding Stego images obtained and their Histograms. All the five Cover images when compared with their corresponding Stego images look very much similar from the human point of view. Base on the Human Visual System (HVS) they are very much the same due to their high PSNR values and low MSE values. A comparison is made between the Histogram representation of the Cover images and those of the resulting Stego images. It can be seen clearly that there are no significant changes in the Cover image Histograms with regards to visual quality in comparism with the Histograms of the resultant Stego images of all the five (5) images.

Clearly, since the result of the histogram equalization analysis shows that there are no significant differences between the Histogram of the Cover images and the Stego images, it also goes to show their robustness to common statistical attacks.

5. Conclusion

This research combines cryptography and steganography to achieve an improved and appreciable security level. The cryptography algorithm is the modified RSA obtained by tampering with the public key functionality ‘e’ by transforming it to f= ((e*2) +1), while the steganography technique is the least significant bit (LSB) technique. In the first instance, customers credentials are encrypted using the RSA algorithm and the encrypted message is then embedded into the cover image using LSB algorithm. The comparison of the quality of Cover image and the Stego image was achieved by employing MATLAB2015a with two performance metrics. The very high PSNR and very low MSE values obtained in this research represent the satisfaction of employing these algorithms in improving the security of online banking transactions.

REFERENCES

[1] Al-sharafi, M. A., Arshah, R. A., Abu-shanab, E., & Elayah, N.: The Effect of Security and Privacy Perceptions on Customers Trust to Accept Internet Banking Services: An Extension of TAM. *Journal of Engineering and Applied Sciences*, 10. https://doi.org/10.3923/jeasci.2016.545.552 (2016).

[2] Jolly, V.: The Influence of Internet Banking on the Efficiency and Cost Savings for Bank's Customers. *International Journal of Social Sciences and Management*, *3*(3), 163–170. https://doi.org/10.3126/ijssm.v3i3.15257 (2016).

[3] Safeena, R., Hema, D., & Abdullah.: Customer Perspectives on E-Business Value: Case Study on Internet Banking. *Journal of Internet Banking & Commerce*, *15*, 1–8 (2010).

[4] Wong, D., Kuen, H., Loh, C., & Randall, B.:To trust or not to trust : the consumer ' s dilemma with e-banking. 3–6 (2009).

[5] Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P.: Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties Within Phishing and Malware Networks. *British Journal of Criminology Advance Access*, 1–19. https://doi.org/10.1093/bjc/azw009 (2016).

[6] Arachchilage, N., Love, S., & Konstantin, B.: Phishing Threat Avoidance Behaviour: An Empirical Investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065 (2016).

[7] Chiu, L. C., Chiu, L. J., & Mansumitrchai, S.: Privacy, Security, Infrastructure and Cost Issues in Internet Banking in the Philippines: Initial Trust Formation. *International Journal of Financial Services Management*, *8*(3), 240–271 (2016).

[8] Sharma, S. :A Detail Comparative Study on E- Banking vs Traditional Banking. *International Journal of Applied Research*, *2*(7), 302–307 (2016).

[9] Devadiga, N., Hardik, J., Sankhe, S., & Kothari, H.: E-Banking Security using Cryptography, Steganography and Data Mining. *International Journal of Computer Applications*, *164*(9), 26–30 (2017).

[10] Kashif, R. & Phaneendra, H. D.: Implementation of Methods for Transaction in Secure Online Banking. *International Journal of Technical Research and Applications*, 3(4), 41-43 (2015).

[11] Khrais, L. T.: Highlighting the Vulnerabilities of Online Banking System. *Journal of Internet Banking & Commerce*, *20*(3) (2015).

[12] Aung, P. P., & Naing, T. M.: A Novel Secure Combination Technique of Steganography and Cryptography. *International Journal of Information Technology, Modeling and Computing*, *2*(1), 55–62. https://doi.org/10.5121/ijitmc.2014.2105 (2014).

[13] Taha, M. S., Shafry, M. R., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M.: Combination of Steganography and Cryptography: A short Survey. *2nd International Conference on Sustainable Engineering Techniques (ICSET)*, 1–13. https://doi.org/10.1088/1757-899X/518/5/052003 (2019).

[14] Sharma, H., Sharma, K. K., & Chauhan, S.: Steganography Techniques Using Cryptography: A Review Paper. *International Journal of Recent Aspects*, 106–108 (2015).

[15] Dhamija, A., & Dhaka, V.: A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, (ICGCIoT)*, 346–351. https://doi.org/10.1109/ICGCIoT.2015.7380486 (2016).

[16] Karthikeyan, B., Kosaraju, A. C., & Gupta, S. S.: Enhanced Security in Steganography Using Encryption and Quick Response Code. *International Conference on Wireless Communication, Signal Processing & Networking (WisPNET)*, 2308–2312 (2016).

[17] Pillai, B., Mounika, M., Rao, P. J., & Sriram, P.: Image Steganography Method Using K-means Clustering and Encryption Techniques. *International Conference on Advances in Computing, Communications and Informatics, ICACCI 2016*, 1206–1211. https://doi.org/10.1109/ICACCI.2016.7732209 (2016).

[18] Joseph, F., & Sivakumar, S.: Advanced Security Enhancement of Data Before Distribution. *International Journal of Engineering Research and General Science*, *3*(1), 1363–1367 (2015).

[19] Padmavathi, B., & Kumari, S. R.:A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique. *International Journal of Science and Research (IJSR)*, *2*(4), 170–174. Retrieved from www.ijsr.net (2013).

[20] Barhoom, T. S., Mohammed, S., & Mousa, A.: A Steganography LSB Technique for Hiding Image Within Image Using Blowfish Encryption Algorithm. *International Journal of Research in Engineering & Science (IJRES)*, *3*(31), 61–66. Retrieved from www.ijres.org (2015).

[21] Thomas, S. E., Philip, S. T., Nazar, S., Mathew, A., & Joseph, N.: Advanced Cryptographic Steganography Using Multimedia Files. *International Conference on Electrical Engineering & Computer Science (ICEECS)*, (May 2012), 239–242 (2014).

[22] Alamsyah, Muslim, M. A., & Prasetiyo, B.: Data Hiding Security using Bit Matching-Based Steganography and Cryptography without Change the Stego Image Quality. *Journal of Theoretical & Applied Information Technology*, *82*(1), 106–112 (2015).

[23] Gambhir, A., & Mishra, A. R.: Crypticsteganography: A New Data Hiding Technique with Multilayer Security System. *International Journal of Innovations & Advancement in Computer Science*, *4*, 134–136 (2015).

[24] Sharma, M. H., Mithlesharya, M., & Goyal, D.: Secure Image Hiding Algorithm using Cryptography and Steganography. *Journal of Computer Engineering*, *13*(5), 1–6(2013).

[25] Mishra, M., Tiwari, G., & Yadav, A. K.: Secret Communication using Public Key Steganography. *International Conference on Recent Advances & Innovations in Engineering (ICRAIE)*, 1–5 (2014).

[26] Sandeep, N., Nobeen, H.S., Lakshni, V.V., Sivaji. S. And Krishna, V.G: an Improved Method of Stegnograrphy combined with cryptography *International journal of advance Eginerring and Reasearch Development 5(3), p-543-544 (2018).*