Original Research Article

SECURING DATA TRANSMISSION IN MOBILE BANKING APPLICATIONS

ABSTRACT

The advent of mobile banking applications has transformed the way customers' access banking services from brick-and-mortar to remote banking. The ubiquitous nature of this innovation has encouraged its adoption. This is because of improved banking services and accessibility to the services on a 24/7 basis using the internet. However, mobile banking applications are susceptible to numerous security threats and vulnerabilities that adversaries take advantage of to siphon money from bank customers. The aim of this study is to design and evaluate least significant bit and advanced encryption standard cryptography (LSB-AES) hybrid algorithm to protect data on transmission in mobile banking. This study employs Data Science Research design. This study was carried out in Kenya in view of banks offering mobile banking between May 2022 to May 2023. Findings of this study can be applied to other banks offering mobile banking across the world. This study utilized six color images from University of Southern California's Signal and Image Processing Institute (USC-SIPI) dataset which were stored in Tagged Image File Format (TIFF). Evaluation of the proposed algorithm was done using Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Entropy, and histogram analysis. Results from the proposed LSB-AES hybrid algorithm evaluation metrics reveals that Mean Squared Error (MSE) values ranges from 0.0001297 to 0.0005646 while Peak Signal-to-Noise Ratio (PSNR) values ranges from 80.65 to 87.71 and entropy values ranges from 6.295 to 7.762. Histogram analysis reveals that the cover and stego images are almost similar. These results infer that the proposed algorithm has good quality images with good imperceptibility and that the proposed algorithm is reliable, robust and secure for mobile banking applications. This study recommends that legislation evaluates and amends security of mobile banking policies so that the proposed LSB-AES hybrid algorithm can be adopted as a secure solution for mobile banking.

Keywords: Mobile banking applications, Least Significant Bit, Advanced Encryption Standard, Mean Squared error, Peak Signal-to-noise Ratio, and Entropy.

1. INTRODUCTION

Mobile banking is utilization of smart phones to carry out financial services related to a client's bank account remotely. These services comprise of checking of account balances, paying bills, sending money, bookings, loan repayments, and airtime top-up among others [1] [2]. This channel of banking has extended to implementation of mobile banking applications to access mobile banking services remotely. The use of mobile banking applications can now aid banks to improve after-sales services, resource management, and improved business aggression through the use of internet [3] [4].

Applications that are used in mobile banking are in demand lately due to enhanced banking services and 24/7 accessibility to the banking services. Notably, these applications are used to transfer user data such as usernames and passwords, One Time Passwords (OTPs), Personal Identification Numbers (PINs) as well as sensitive financial data such as credit card numbers, bill payment details, and money withdrawal details among others from the application to the bank server. User data on transit in mobile banking is data being transferred from the application to the banks' server and vise versa using the Internet. According to Sealpath (2020), user data on transit is vulnerable to attacks because of weak encryption techniques used both on data and wireless networks used for data transmission.

Data on transit is at risk from various attacks such as mobile malware, packet sniffing attacks (Bhattacharya & Reddy, 2022), Man-in-the-Middle (MITM) attacks [5], Domain Name System (DNS) poisoning [6], Secure Sockets Layer (SSL) strip session hijacking [7], eavesdropping attack [8], Denial of Service (DoS) attacks, and social engineering attacks [9]. Such risks have contributed to a segment of the population being reluctant to adopt such technology due to the fear of these vulnerabilities including the online fraud [10]. Therefore, the authentication mechanisms used in mobile banking applications may need to be robust to mitigate these vulnerabilities and attacks [11].

Banks have suffered significant financial losses as a result of the inherent risks and weaknesses in mobile banking. Cybercriminals may access personal and sensitive financial data by using a variety of attack vectors that exploit the loopholes that might exist in mobile banking applications. Drive-by-downloads, malware, and malware (such as Trojan horses, worms, viruses, botnets, ransomware, and spyware) are all examples of malicious software which can be utilized to gain access to the mobile banking channel [12].

Some techniques utilized to secure data on transit in mobile banking applications include steganography, cryptography as well as combination of steganography and cryptography. Using steganography, sensitive information is concealed within an image or message to produce a stego image in order to prevent detection. According to Simplilearn (2023) at its destination, the sensitive information will subsequently be retrieved from the stego image, preventing discovery (Simplilearn, 2023). In comparison to conventional encryption methods, modern cryptography approaches are more secure. They convert plaintext into ciphertext using mathematical algorithms and keys, making it significantly more difficult for unauthorized parties to access or read the original message (Sidhu, 2023). In addition, user data on transit can be protected using steganography and cryptography to add a layer of security. In this combination, steganography provides a security feature of embedding confidential message to a cover image while cryptography contributes a security feature of encrypting confidential message that is embedded in the cover image.

The wireless network infrastructure used in mobile banking applications to establish a connection between the banking clients and banking server to transmit confidential data is not immune to cyber attacks. according to digital transformation cyber security news (2016), for instance in the year 2018 hackers used reverse engineering in mobile banking applications to steal client's login credentials in which USD 2.26 million was stolen from over 900 accounts in less than 12 hours.

Despite the fact that there are several techniques available that prevent clients confidential information from being collected, they exhibit inadequacy in combating some of the emerging cybercrime methods being used to access clients' bank accounts using wireless networks. According to European mobile banking applications white paper (2022) 90 % of mobile banking applications that are tested are found to have weak cryptography. As a matter of principal, the dependability and tamper-proof connection between mobile banking applications and the banks' server is crucial to the security of mobile banking applications since it prevents cybercriminals from accessing clients' bank accounts. The clients' application and the bank server must therefore utilize secure connection in order for clients to successfully access banking services remotely without being concerned about hackers. Therefore, it is important to fortify current methods employed to secure access to mobile banking services.

This paper, therefore, proposes a new mechanism to improve security of data on transit between the mobile banking application (at the customer's end) and the mobile banking server (host server at the bank's end) in attempt to protect the customer from vulnerabilities including malware and cyberattacks. To this end, the contribution of this paper is in two folds: Formulate and design least significant bit and advanced encryption standard cryptography (LSB-AES) hybrid algorithm to protect data on transmission in mobile banking. To evaluate the performance of the proposed algorithm – the results show that LSB-AES hybrid algorithm ranged from 0.0001297 to 0.0005646, 80.65 to 87.04, and 6.295 to 7.762 performances in regards to MSE, PSNR and Entropy performance metrics. The rest of this paper is organized as follows: Section 2 presents a review of related work; algorithm formulation is presented in Section 3 while Section 4 presents the results. Conclusion is presented in Section 5.

2. RELATED WORK

The Advanced Encryption Standard (AES) is an open standard that has been subjected to many attacks. Some of these attacks are: Boomerang attack, truncated differentials, square attack, interpolation attack, algebraic attacks, hybrid attacks, related-key and distinguishing attacks, power analysis attacks, and cache attacks. Most of these attacks are based on the weakness that lies in the key schedule unit. The drawback of the key expansion unit lies in its slow diffusion process and the distribution of the key bits are insufficient [13]. A proposed study by [14] on divide and conquer approach for cryptanalysis of key-based coded permutation cipher and modified data encryption standard points out that key-extension does not result in advantageous results in terms of security. Their analysis shows that with a known plaintext attack, 56 bit key can be guessed and this can recover the remaining keys in the following round functions.

Text hiding involves embedding secret data through a cover media so that the existence of the data is invisible for adversaries [15][16] [17] . It has been widely considered as an attractive technology to improve the use of conventional cryptography algorithms in the area of multimedia security by concealing a secret message into a cover media to protect confidential information [18]. A study by [19] proposed a study on innovative image hiding encryption and decryption technique. The efficiency of the proposed model was validated by applying attacks such as novel white floor attack, RS steganalysis, chi-square attack, and visual attack. The proposed methodology showed that the embedded image has high PSNR, SSIM and reduced MSE. Results from their study points out that steganography can be used to hide secret messages in digital images. To overcome attacks on AES algorithm and LSB steganography, a more secure algorithm can be developed by combining the two algorithms.

A proposed hybrid algorithm by [20] that uses AES and LSB image steganography, first encrypts a given message using AES encryption which is then written to a cover image. The system supported 24-bit and 32-bit Bitmap images. Findings from their study infer that the system was secure and that AES and LSB can be

successfully incorporated into one system to increase the level of security of data. A proposed StegoCrypt hybrid algorithm by [21] applied LSB steganography techniques to digital images and combined with AES Base64 algorithms. Results analyzed from their algorithm indicate average the average values 0.6031, 60 dB for MSE and PSNR respectively. The proposed algorithm infers that data security can be enhanced by combining AES Base 64 cryptographic algorithm with LSB Steganography method using the blue channel. This algorithm proved to be secure for transmitting data over unsecure and vulnerable networks.

A proposed hybrid approach to data security using Discrete Wavelet Transform (DWT) compression technique, AES cryptography and LSB approach [22] utilized Structural Similarity Index (SSIM) and PSNR for imperceptibility metrics. Results from their experiment indicate average values of SSIM to be 0.93 while PSNR values are 48.9613. The proposed hybrid algorithm improved data security and its performance is good due to the additional three layers of security. A proposed hybrid algorithm by [23] incorporates Elgamal encryption and LSB image steganography. Evaluation metrics utilized in the algorithm were MSE, PSNR, SSIM, and Entropy. Results fom their experiment the average values 0.06815, 66.845, and 7.5318 for MSE, PSNR, and Entropy respectively. This infers that the system was robust and that security of data can be enhanced using a combination of LSB steganography and Elgamal encryption scheme.

From related work, AES, LSB steganography and a combination of LSB steganography and AES algorithms have been discussed. AES algorithm is susceptible to attacks such as Boomerang attack, truncated differentials, square attack, interpolation attack, algebraic attacks, hybrid attacks, related-key and distinguishing attacks, power analysis attacks, and cache attacks. On the other hand steganography is susceptible to attacks such as novel white floor attack, RS steganalysis, chi-square attack, and visual attacks. Additionally, proposed algorithms that combine LSB steganography and AES cryptography have been proposed on different areas such as on network security, Internet of Things (IoT), and e-Commerce. Thus this study established an existing gap by proposing LSB-AES hybrid algorithm for securing data on transit in mobile banking applications.

3. ALGORITHM FORMULATION

This study employs Data Science Research (DSR) methodology. This methodology is utilized in order to improve execution of system design and its output as an information technology artifact [24]. DSR's general objective is to produce information on how to construct new solutions that successfully address pressing issues [25]. DSR was used because it presents systematic structures and formula used to invent artifacts such as algorithms, interfaces, and system design approaches among others [26]. Thus DSR was utilized to come up with LSB-AES hybrid algorithm for secure data transmission in mobile banking applications.

This study focused on the design and evaluation of a hybrid algorithm that ensures secure data transmission in mobile banking applications and therefore excluded other channels of mobile banking. Results of the proposed hybrid algorithm focused on visual analysis such as MSE, PSNR, entropy analysis, and statistical analysis such as histogram analysis. The study excluded other visual analysis such as Structural Similarity Index (SSI), Normalized Cross Correlation (NCC), and Normalized Absolute Error (NAE). The Study used a combination of LSB substitution technique and AES cryptography technique.

LSB substitution technique was used because it contributes an important security feature of hiding a secret message onto a cover image to avoid detection of existence of the message. On the other hand AES was used because it contributes an important security feature of encrypting a secret message in order to deter adversaries from decrypting the message. Thus a combination of LSB-AES hybrid algorithm incorporates two security features from the two algorithms and therefore is more secure than the security of the two algorithms when used separately. The LSB-AES hybrid algorithm contains two important processes which are encryption and embedding and decryption and decoding processes. Encryption and embedding process is depicted in Figure 1.

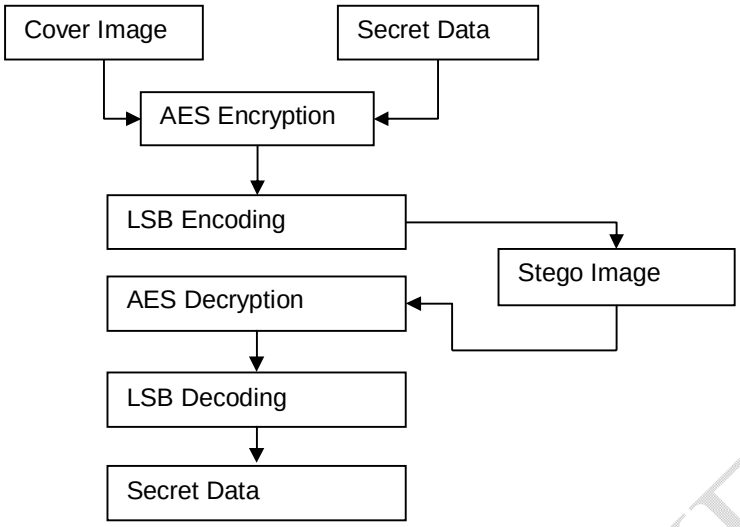


Figure 1: LSB-AES Hybrid Algorithm.

In Figure 1 the first step in the algorithm's execution is to read the cover image and the secret data followed by hiding secret data into the cover picture using LSB encoding. In order to provide protection of data on the cover image, AES is used to encrypt data resulting with a stego picture. To recover encrypted message from stego-picture, LSB and AES decryption key is used.

Hybridization of LSB-AES on-transit user-data protection algorithm combined LSB steganography with AES cryptography to yield a secure algorithm that can be used for mobile banking applications. LSB substitution technique contributes a security feature of hiding a secret message onto a cover picture to avoid detection. On the other hand, AES algorithm contributes a security feature of encrypting secret message to deter adversaries from decrypting the message. When the two algorithms are combined, the resultant algorithm is more secure than any of the individual algorithms.

Purposive sampling was used to select six color images from University of Southern California Signal and Image Processing Institute (USI-SIPI) database for test simulations of LSB-AES hybrid algorithm. Results analysis was done using visual analysis and statistical analysis. In visual analysis this study took advantage of Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and entropy. MSE and PSNR were chosen because they are the best tools that can be utilized for steganography, encryption and decryption determination [27]. These two metrics were chosen because they were crucial components in the proposed algorithms' analysis and evaluation. Entropy analysis was chosen because it measures the security level of a developed system. Additionally, statistical analysis was used in which histogram analysis selected. Finally, the results of analysis were displayed in tables.

4. DESIGN OF LSB-AES HYBRID ALGORITHM

The proposed algorithm comprised of two major interfaces which were encryption and embedding interface and decryption and decoding interface. Encryption and embedding interface comprised various tabs such as upload image that was used for uploading cover image, fetch data which was used for uploading data, encrypt which was used to apply AES encryption, and finally encode tab which was utilized for sequential insertion of encrypted data onto the cover image to yield a stego image. On the other hand, decryption and decoding interface comprised of various tabs such as fetch stego image which was used for uploading stego images into the system, decrypt tab which was used to apply AES decryption key, and decode tab which was used to sequentially retrieve embedded messages from the stego image.

4.1 LSB Algorithm

LSB steganography is a spatial domain technique in which the pixels of an image are substituted with the bit of a text or image. The uniqueness of this method is that the human eye cannot distinguish between the original cover picture and stego picture where secret data has been hidden [28]. LSB substitution method comprises of LSB embedding and LSB decoding processes. LSB embedding is illustrated in Table 1.

Table 1: Embedding Algorithm [29]

Embedding Algorithm	
Step 1	Upload the cover picture and secret message
Step 2	Encrypt the secret message with AES algorithm

Step 3	Convert message into binary bits
Step 4	Initialize sequential encoding to identify pixels of cover picture
Step 5	LSB of sequentially located pixels will be modified as per values of message bits
Step 6	The modified pixel value is fed back to its respective position. As per size of message data LSBs of picture pixels are modified
Step 7	Save and send the stego-picture

The embedding algorithm specifies steps taken in inserting message in a cover image. Once encrypted message is encoded on cover image, the resultant is a stego-picture which is saved and sent to a recipient. The initial move in the algorithm design is uploading cover picture and message to be hidden; the second step is obfuscating message with AES algorithm. Lastly is to convert message into binary mode then inject it to cover picture using sequential encoding. Moreover, the colored image has RGB color model in which data can be hidden in the LSB of any color space of the sequentially selected pixels. LSB decoding is illustrated in Table 2.

Table 2: Decoding Algorithm [29]

Decoding Steps	
Step 1	Upload the stego-picture
Step 2	Read the LSB of each identified pixel of stego-picture
Step 3	Apply AES decryption algorithm
Step 4	Apply sequential decoding to retrieve message from stego-picture

From Table 2 the first step in retrieving hidden message from the stego image is to upload the stego-image, followed by reading LSB of the pixel of stego-image, third step involves applying AES decryption key, and finally fourth step is to sequentially decrypt the message from the stego-image.

4.2 AES Algorithm

Advanced Encryption Standard (AES) offers security for digital communication. The divisions of AES are SubBytes, ShiftRows, MixColumns, and AddRoundKey. Each byte is changed with a different byte at SubByte operation. Here, substitution box commonly denoted as S-box are used to carry out this function. Due to the way this replacement is implemented, a byte cannot be replaced by either itself or by the complement of the byte that is now in use. Each of the matrix's four rows is moved to the left in ShiftRows. The right side of the row is used to re-insert any entries that slip off.

The action of MixColumns essentially entails multiplying a matrix by itself. Each row's data is multiplied by a certain matrix, which has an impact on the location of each byte. The 128 bits of the round key and the 128 bits of the matrix were combined to create a total of 128 bits in AddRoundKeys. In the event that this is the last iteration, the ciphertext will be produced. If not, the 128 bits are read as 16 bytes and a new set of operations, similar to this one, are started (Abdullah, 2017). AES algorithm is divided into encryption and decryption processes.

The proposed LSB-AES hybrid algorithm achieved more security of secure data transmission in mobile banking applications because of the security contributions of LSB and AES algorithms. LSB steganography algorithm contributed a security feature of hiding secret message onto a comer image to avoid detection from adversaries. On the other hand, AES algorithm contributed a security feature of encrypting secret message to deter adversaries from decrypting the message. When these two security features are combined, they produce a more secure algorithm than the individual algorithms. Table 3 illustrates the LSB-AES hybrid algorithm for secure data transmission in mobile banking applications.

Table 3: LSB-AES Hybrid Algorithm [30].

	LSB-AES On-Transit User-Data Protection
1	Read the input cover image
2	Read the secret data
3	Apply LSB encoding where the bits of the secret data are hidden into the least significant bit of the pixel value of the cover picture.
4	Apply AES encryption during encryption stage
5	Apply AES decryption during decryption stage
6	Apply LSB decoding to retrieve secret data from the stego-picture

5. RESULTS AND DISCUSSION

The proposed LSB-AES hybrid algorithm was implemented on MATLAB (R2021a) App designer program installed on a computer laptop using Windows 10 Operating System with Advanced Micro Devices (AMD) RYZEN 3 3300 U central Processing Unit (CPU) and 8 GigaByte (GB) Random Access Memory (RAM). Six Red Green Blue (RGB) color model for cover images were selected from USC-SIPI dataset namely airplane, female, house, couple, peppers, and sailboat which were between 512 × 512 pixels and 256 × 256 pixels. These images were chosen from the dataset for testing quality image analysis during simulation tests.

For testing image quality analysis, contemporary steganographic systems employ cover images of 10 and a minimum of 2 for test simulations [31]. This study therefore utilized 6 cover pictures with Tag Image File Format (TIFF) with 24 bits. These formats were chosen because TIFF format images do not differ from the original cover images after embedding messages on them. Additionally, TIFF format files are lossless for archiving [32]. Arbitrary data for simulation was chosen such as OTP, a password and credit card number with varying length of characters was used.

The proposed algorithm was evaluated using MSE, PSNR, entropy, and histograms on six color cover images which were chosen taking into account a variety of image attributes such as color and image format. In order to illustrate how well the proposed algorithm performed, simulation tests were shown. The following section discusses findings from the simulation tests.

5.1 MSE Analysis

Mean Squared Error (MSE) measures the average of the squares of errors between two images. In other words, it is averaged squared dissimilarity that links cover image and stego image. It therefore expresses the mean flaw between cover and stego image [33] as shown in (1) below.

$$MSE = \frac{\sum M, N\left[l_1(m,n) - l_2(m,n)\right]^2}{M \times N} \quad (1)$$

Where M and N are the number of rows and columns of the cover image matrix and I_1 and I_2 is the cover and stego images respectively. MSE is a full reference metric in which values closer to zero are better [34]. Simulation tests conducted on six cover images illustrates that their corresponding stego images were substantially similar with low MSE values as follows: Airplane 0.0001488, Female 0.0004425, House 0.0005035, Couple 0.0005646, Peppers 0.0001297, and Sailboat 0.0001297.

5.2 PSNR Analysis

Peak Signal-to-Noise Ratio (PSNR) is a ratio for the maximum possible power of a signal to the power of the corrupting noise affecting the fidelity of the presented image. Greater values of PSNR of values of above 40 decibels (dB) indicate best quality of pictures [35]. According to [36], the PSNR value should be greater than 39Db for improved image quality. This is shown in (2) below.

$$PSNR = 10Log_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

Where R^2 is highest number of pixels and MSE is the mean squared error of cover and stego image. In PSNR analysis, simulation tests conducted on six cover images illustrates that their corresponding stego images had higher PSNR values in decibel (dB) as follows: Airplane 86.44, Female 84.71, House 81.14, Couple 80.65, Peppers 87.04, and Sailboat 87.14.

5.3 Entropy Analysis

Entropy was employed in this study to gauge security level of the proposed algorithm. Entropy is a metric that expresses how much information is in an image. It is helpful for determining the typical amount of bits needed to encode message components. Entropy values should be close to value 8. [37] as shown in (3) below.

$$Entropy = \sum {}^{n}{}_{i} = 1\pi Log_2(\pi) \quad (3)$$

Where n = number of different data values, π is probability of occurring of the data value i. The ideal entropy value for an 8-bit system fall within the average range of 0 to 8 with values close to 8 considered as the best value [38]. Findings from simulation tests conducted on the cover pictures and their corresponding stego pictures reveals entropy values as follows: Airplane 6.664, Female 6.898, House 7.069, Couple 6.295, Peppers 7.67, and Sailboat 7.762. The three metrics; MSE, PSNR, and Entropy are illustrated in table 4.

Table 4: LSB-AES Hybrid Algorithm Evaluation Metrics.

Picture	Cover Picture	Stego Picture	MSE	PSNR	Entropy
Aeroplane			0.0001488	86.44	6.664
Female			0.0004425	81.71	6.898
House			0.0005035	81.14	7.069
Couple			0.0005646	80.65	6.295
Peppers			0.0001297	87.04	7.67
Sailboat			0.0001297	87.04	7.762

Table 4 illustrates MSE, PSNR, and Entropy analysis. In steganography, MSE values should be low for better message concealment in an image. MSE on table 2 ranged from 0.0001297 to 0.0005646, which are relatively low values. Low MSE values infer that the stego images were closely similar to the original cover images. Findings of MSE from this study were consistent with MSE results of Abikoye, Ogundokun, Misra, and Agrawal (2022) that ranged from 0.0002124 to 0.0009422. Similarly, these findings concur with those of Msallam (2020) which ranged from 0.0011 to 0.0015. It is recommended that MSE is low for better data concealing [39].

The PSNR values of cover and stego images spanned from 80.65 to 87.04. In steganography, PSNR values must always be greater than an acceptable threshold to show good imperceptibility. This infers that it can be

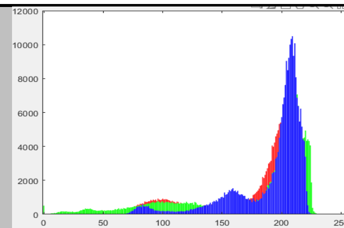
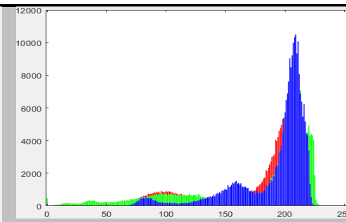
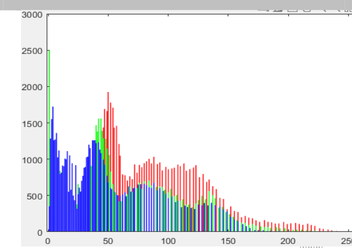
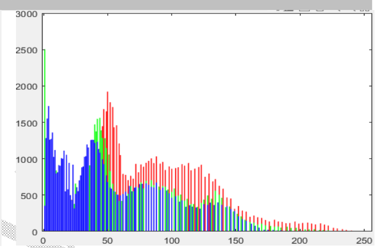
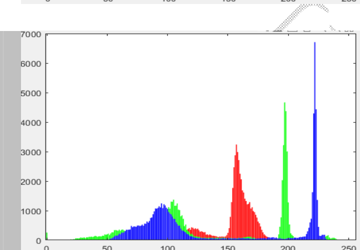
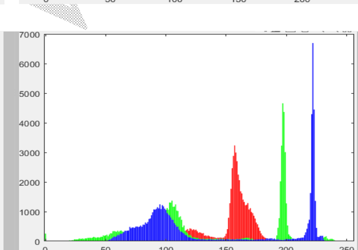
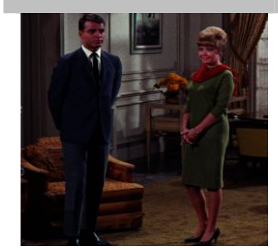
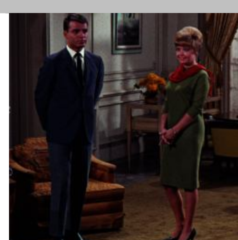
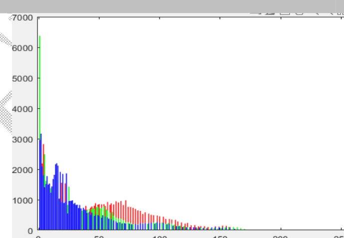
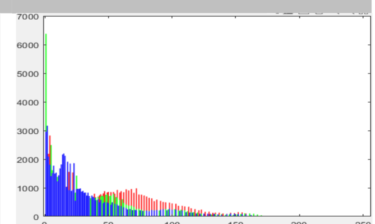
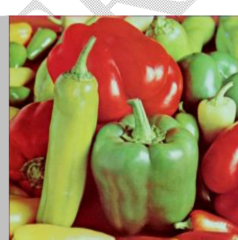
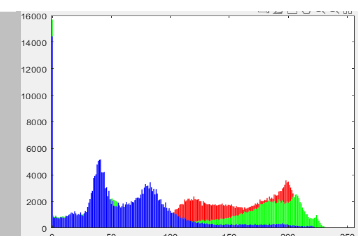
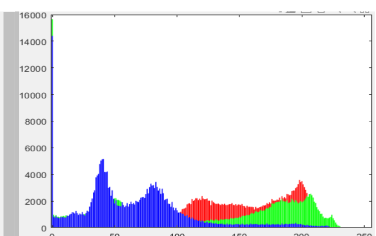
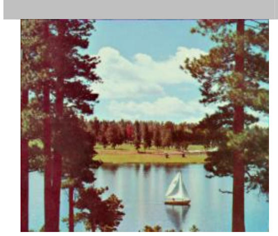
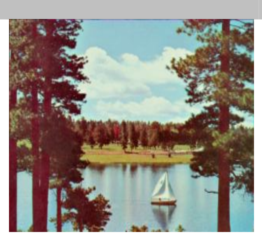
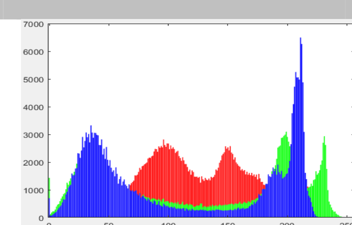
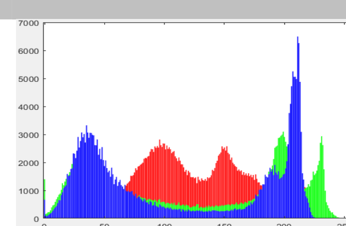
challenging to ascertain that a message is hidden inside the stego images. Findings of PSNR from this study are consistent with PSNR results of Abikoye, Ogundokun, Misra, and Agrawal (2022) that spanned from 78.389 to 84.858. Secondly, PSNR values from this study were consistent with PSNR results of [40] which ranged from 82.3599 to 83.0220. Thirdly, this study's findings are consistent with [41] whose PSNR values ranged from 48.55 to 55.38 decibel and therefore inferring good imperceptibility. If the PSNR result is above 40 dB, a stego picture exhibits adequate imperceptibility ([42].

Findings from this study reveal that entropy values ranged from 6.295 to 7.67. Entropy was used to gauge the systems security level. Adequate entropy values should be close to the value 8 (Hari, Syaiful, Moses, & Atika, 2017). As a result the system exhibited acceptable entropy levels and attained high level of security and proved to be secure for mobile banking applications. Findings of entropy from this study are consistent with results from from [40] which ranged from 7.1914 to 7.4518. [43] had entropy values ranging from 4.1443 to 5.447.

5.4 Histogram Analysis

Histogram analysis is a salient standard employed which illustrates tonal distribution in RGB model graphically. A simulation experiment was created to determine whether the distribution of colors varies when text is embedded onto cover images. Table 5 illustrates histogram analysis.

Table 5: Cover Picture and Stego Pictures with their Corresponding Histograms

Cover Image	Stego Image	Histogram of Cover Image	Histogram of Stego Image
			
			
			
			
			
			

Histogram analysis in steganography demonstrates that there is hardly any slight distortion between cover and stego images used in an experiment. A cover image is a media that is used to hide a message while stego image is media that contains embedded message. The RGB color distribution in the histograms in Table 5 indicates that there were hardly any differences between cover and stego images. This suggests that the

proposed algorithm was reliable and suitable for usage with mobile banking applications because it is difficult for an adversary to discern that there are hidden messages in any of the images used. These results were consistent with a study conducted by [44] whose experimental results indicated that the dissimilarities of cover and stego images were merely indistinguishable and therefore inferring enhanced performance of their proposed algorithm. Findings of [45] who conducted a study on secure mobile banking framework using cryptography and steganography proposed a model for security of Multimedia Messaging Service (MMS) in mobile banking by combining LSB technique and AES encryption algorithm. Simulation results from this study exhibit AES algorithm to be advantageous over other algorithms based on time taken during encryption, power saver efficient with low memory consumption.

A proposed algorithm by [46] on LSB digital image steganography yielded average MSE value of 0.3545 while average PSNR and entropy values were 52.67 and 7.6795 respectively. The proposed LSB-AES algorithm yielded average MSE, PSNR, and entropy values of 0.00013925, 86.74, and 7.167 respectively. Table 6 illustrates average performance metrics of LSB steganography and proposed LSB-AES algorithm.

Table 6: Comparison of LSB Steganography with Proposed LSB-AES Algorithm

Image	LSB Steganography			Proposed LSB-AES Algorithm		
	MSE	PSNR	Entropy	MSE	PSNR	Entropy
Airplane	0.398	52.13	7.661	0.0001488	86.44	6.664
Peppers	0.311	53.21	7.698	0.0001297	87.04	7.67
Average	0.3545	52.67	7.6795	0.00013925	86.74	7.167

Table 6 illustrates performance of LSB steganography with the proposed LSB-AES algorithm. The LSB steganography algorithm's average MSE values are not close to 0 to meet the minimum threshold because the inference made from MSE values close to 0 is that the cover picture and stego picture are almost the same. Results from average PSNR indicate that they surpassed the minimum 40dB threshold and were regarded as good for imperceptibility. Average entropy results from LSB steganography algorithm were close to the acceptable threshold and therefore regarded providing good security for the algorithm. However when compared to the proposed algorithm, the average MSE values of LSB steganography were greater than the required minimum threshold. Similarly, average PSNR values of LSB steganography were lower compared to the proposed algorithm. Even though the average entropy values of LSB steganography were higher, the overall security of the system is weaker than the proposed LSB-AES algorithm.

A proposed algorithm by [47] on AES double-layer message security yielded average MSE value of 0.07817 while average PSNR and entropy values were 62.2 and 6.193395 respectively. The proposed LSB-AES algorithm yielded average MSE, PSNR, and entropy values of 0.0002861, 86.375, and 7.284 respectively. Table 7 illustrates average performance metrics of the AES algorithm and proposed LSB-AES algorithm.

Table 7: Comparison of AES with Proposed LSB-AES Algorithm

Image	AES Algorithm			Proposed LSB-AES Algorithm		
	MSE	PSNR	Entropy	MSE	PSNR	Entropy
Female	0.03888	62.2	6.14847	0.0004425	81.71	6.898
Peppers	0.03929	62.2	6.23832	0.0001297	87.04	7.67
Average	0.07817	62.2	6.193395	0.0002861	84.375	7.284

Table 7 illustrates performance of AES algorithm with the proposed LSB-AES hybrid algorithm. The AES algorithm average MSE values are not close to 0 to meet the minimum threshold because the inference made from MSE values close to 0 is that the cover picture and stego picture are almost the same. Results from average PSNR indicate that they surpassed the minimum 40dB threshold and were regarded as good for imperceptibility. Average entropy results from AES algorithm were close to the acceptable threshold and therefore regarded providing good security for the AES algorithm. However, the average MSE values of AES algorithm were greater than the required minimum threshold. Similarly, average PSNR values of AES algorithm were lower compared to the proposed algorithm. Thus the overall security of the system was weaker than the proposed LSB-AES algorithm.

A proposed algorithm by [48] that utilized modified LSB steganography and AES encryption with two standard analysis metrics MSE and PSNR produced MSE results ranging from 0.00036 to 0.00149 while PSNR values ranged from 76.38 to 82.49. The proposed LSB-AES algorithm yielded average MSE, PSNR, and entropy values of 0.0002861, 86.375, and 7.284 respectively. Table 6 illustrates average performance metrics of the modified LSB steganography with AES encryption algorithm and the proposed LSB-AES hybrid algorithm. Table

8 illustrates average performance metrics of the modified LSB steganography AES encryption algorithm and the proposed LSB-AES hybrid algorithm.

Table 8: Comparison of Modified LSB-AES algorithm with Proposed LSB-AES hybrid Algorithm

Image	Modified LSB-AES Algorithm		Proposed LSB-AES Algorithm	
	MSE	PSNR	MSE	PSNR
Airplane	0.00036	82.49	0.0001488	86.44
Couple	0.00137	76.75	0.0005646	80.65
House	0.00149	76.38	0.0005035	81.14
Average	0.001073	78.54	0.000406	82.74

Table 8 illustrates performance of modified LSB-AES algorithm with the proposed LSB-AES hybrid algorithm. The modified LSB-AES algorithm average MSE values indicated that they were good quality images. Similarly, the average PSNR values surpassed the minimum threshold of 40 decibel and were regarded as good for imperceptibility. However LSB-AES hybrid algorithm surpassed the average values of both MSE and PSNR values of modified LSB-AES algorithm and therefore proved to be more secure and robust for mobile banking applications.

CONCLUSIONS

This paper proposes design and evaluation of LSB-AES hybrid algorithm to improve security of data on transit between the mobile banking application (at the customer's end) and the mobile banking server (host server at the bank's end) in an attempt to protect vulnerabilities in mobile banking such as malware and cyber attacks. LSB-AES hybrid algorithm combined security features from LSB algorithm and AES algorithm. LSB substitution algorithm contributed an important security feature of hiding a secret message onto the cover picture to avoid detection of existence of the message. On the other hand, AES algorithm contributed an important security feature of encrypting a secret message in order to deter adversaries from decrypting the message. The proposed hybrid algorithm can be used securely in mobile banking applications to execute financial transactions linked to a customer's bank account globally. The proposed LSB-AES hybrid algorithm can also be used in Kenyan banks that offer mobile banking platforms as well as banks that plan to offer mobile banking. This study recommends other researches to assimilate AES algorithm with audio steganography technique to improve security of mobile banking applications. Additionally, research can be conducted using a combination of different types of cryptosystems to improve security of mobile banking.

REFERENCES

1. Raharja PSJ, Tresna R. Adoption of Information and Communication Technology on Enhancing Business Performance: Study on Creative Industry SMEs in Bandung City, Indonesia. Review of Integrative Business and Economics Research. 2019; 8 (3): 20–30.
2. Malaquias RF, Silva F. Understanding the use of Mobile Banking in Rural Areas of Brazil. Technology in Society. 2020; 62: 101260.
3. Sang NM. Critical Factors affecting Concumer Intention of using Mobile Banking Applications during CCOVID-19 Pandemic: An Empirical Study from Vietnam Journal of Asian Finance, Economics and Business. 2021; 8(11):157-167.
4. Shahid S, Islam JU, Malik S, Hasan U. Examining Consumer Experience In using Mobile Banking Applications. A Study of its Antecedents and Outcomes. Journal of Retailing and Consumer Services, 2022; 65: 102870.
5. Javeed D, Badamasi UM, Ndubuisi CO, Soomro F, Asif M. Man in the Middle Attacks. Analysis, Motivation and Prevention: International Journal of Computer Networks and Computing Security. 2020; 8(7): 52-57
6. Alharbi F, Chang J, Zhou Y, Qian F, Qian Z, Abu-Ghazaleh N. Collaborative Client-Side DNS Cache Poisoning Attack. EEE Conference on Computer Communications, 2019; 1153–1161. DOI: 10.1109/INFOCOM.2019.8737514.
7. Hossain, D., Paul, A., & Islam, H. (2018). Survey of the Protection Mechanisms to the SSL-based Session Hijacking Attacks. Network Protocols and Algorithms*. 2018;* 10(1): 83-108.
8. Talom FSG, Tengeh RK. The Impact of Mobile Money on the Financial Performance of SMEs in Douala, Cameroon, Sustainability. 2020; 12(1): 183. doi.org/10.3390/su12010183.
9. Hussain M, Siddiqui S, Islam N. Social Engineering and Data Privacy. Fraud Prevention, Confidentiality, and Data Security for Modern Businesses. IGI Global; 2023

10. Hanif Y, Lallie HS. Security Factors on the Intention to use Mobile Banking Applications in the UK Older Generation. A Mixed Method Study using Modified UTAUT and MTAM- with Perceived Cyber Security Risk and Trust. Technology and Society. 2021; 67: 101693. doi.org/10.1016/j.techsoc.2021.101693.
11. Cavus N, Mohammed YB, Isah, ML. Examining User Verification Scheme Safety and Secrecy Issues Affecting Mobile Banking. Sage Journals. 2023; 3 (1): https://doi.org/101177/2182440231152379.
12. Nerwal B, Mohapatra A K, Usmani K A. towards a Taxonomy of Cyber Threats against Target Applications. Journal of Statistics and Management Systems. 2019; 22(2): 301-325. DOI: 10.1080/09720510.2019.1580907.
13. Nyberg, K. Differentially Uniform Mappings for Cryptography. Proceedings Workshop on the Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg. 1993; 55-64.
14. Yap WS, Heng SH, Goi BM. Security Analysis of M-DES and Key-based Coded Permutation Ciphers in Wireless Channels. IET Communications. 2018; 12(10):1230-1235.
15. Ahvanooey MT, Li Q, Hou J, Mazraeh HD, Zhang J. An Innovative Text Steganography Technique for Hidden Transmission of Text Message via Social Media. IEEE Access. 2018; 6: 65981–65995.
16. Rizzo SG, Bertini F, Montesi D, Stomeo C. Text Watermarking in Social Media. In Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, Sydney, Australia. 2017.
17. Patiburn SA, Iranmanesh V, Teh PL.Text Steganography using Daily Emotions Monitoring. International Journal of Education Management Engineering. 2017; 7:1–14.
18. Tahvanooey MT, LI Q, Shim HJ, Huang Y. A Comparative Analysis of Information Hiding Techniques for Copyright Protection of Text Documents. Security and Communication Networks. 2018; 5325040.
19. Kaur S, Bansal S, Bansal RK. Image Steganography for Securing Secret Data using Hybrid Hiding Model. Multimedia Tools and Applications. 2020; 80: 7749-7769. doi: 10.1007/s11042-020-09939-7.
20. Vikas M, Yashwanth E, Veeresh Krishna S, Narender M. Hybrid Approach toText and Image Steganography using AES and LSB Technique. International Research Journal of Engineering and Technology. 2018; 5(4): 1500-1502.
21. Anwar F, Rachmawanto EH, Sari CA. StegoCrypt Scheme using LSB-AES Base64. 2019 International Conference on Information and Communications Technology (ICOIACT); 85-90.
22. Loganathan M, Bharathiraja R. Advanced Image Security using new combined Approach AES cryptography and LSB steganography. International Journal of Advanced Multidisciplinary Scientific Research. 2020; 3(1): 98-109.
23. Kumbhakar D, Sanyal K, Karforma S. An Optimal and Efficient Data Security Technique through Crypto-Stego for E-Commerce. Multimedia Tools and Applications.2023; 4-11.doi.org/10.1007/s11042-023-14526-7
24. Dresch A, Lacerda DP, Antunes JAV. Design science research Springer. 2015; 67–102.
25. Kruse L C, Seidel S, Purao S. Making Use of Design Principles, *Proceedings of the 11th International Conference on Tackling Society's Grand Challenges with Design Science*. 2016; (1961): 37–51.
26. Peffers K, Tuunanen T, Gengler C E, Rossi M, Hui W, Virtanen V, Bragge J. The Design Science Research Process. A Model for Producing and Presenting Information Systems Research. 2020; (In press)
27. El-Abbadi N E, Al-Zubaidi E A, Razzaq H S. Image Quality Assessment Tools. Journal of Xi'an University of Architecture and Technology. 2020;12(3):1260-1276
28. Kaur, H., & Kakkar, A. (2017). Comparison of Different Image Formats using LSB Steganography. 4th International Conference on Signal Processing Computing and Control. 97-101.
29. Aye A M. (2018). LSB Based Image Steganography for Information Security System. International Journal of Trend in Scientific Research and Development. 2018; 3(1): 394-400.
30. Al-Omari Z Y, Al-Taani A T. Secure LSB steganography for Colored Images using Character-color Mapping. 8th International Conference on Information and Communication Systems. 2017; 104- 110.
31. Alabaichi A, Ali M A, Al-Dabbas K, Salih A. Image Stegamography using Least Significant Bit and Secret Map Techniques. International Journal of Electrical And Computer Engineering. 2020; 10 (1): 935-946.
32. Chikouche S L, Chikouche N. An Improved Approach for LSB-Based Image Steganography using AES Algorithm. *The 5th International Conference on* Electrical Engineering-Boumerdes, Algeria. 2017.
33. Gu Y Q, He C, Liu F G, Ye, J. Raman Ink for Steganography. Adv. Optical Mater. 2021; 9: https://doi.org/10.1002/adom.202002038
34. Sara U, Akter M, Uddin M S. Image Quality Assessment through FSIM, SSIM, MSE and PSNR-A Comparative Review. Journal of Computer and Communications. 2019; 7(3): 8-18.
35. Lakshmi SB, Srinives S, Kumar, Chandra, M.B. Steganography based Image Sharing with Reversibility. Journal of Discrete Mathematical Sciences and Cryptography. 2016; 19(1): 67-80.
36. Sukumar AK, Subramaniyaswamy V, Vijayakumar V, Ravi L. A Secure Multimedia Steganography Scheme using Hybrid Transform and Support Vector Machine for Cloud-based Storage. Multimed Tools. Appications.2020; doi: 10.1007/s11042-019-08476-2.
37. Hari RE, Syaiful AR, Moses SD-R.I, Atika S C.A Performance Analysis StegoCrypt Algorithm Based on LSB-AES 128-bit in Various Image Sizes. IEEE International Seminar on Application for Technology of Information andCommunication Semarang, Indonesia. 2017

doi:10.1109/ISEMANTIC.2017.8251836
38. Sneha PS, Sankar S, Kumar AS. A Chaotic Colour Image Encryption Scheme Combining Walsh–Hadamard Transform and Arnold–Tent Maps. Journam of Ambient Intelligent Human Computer. 2020; 11: 1289–1308. https://doi.org/10.1007/s12652-019-01385-0
39. Singh V, Choubisa M, Soni G K. Enhanced Image Steganography Technique for Hiding Multiple Images in an Image using LSB technique. TEST Engineering and Management: 2020; 30561-30565.
40. Msallam M M.A Development of Least Significant Bit Steganography Technique Iraqi Journal of Computers, Communications, Control and Systems Engineering. 2020; 20(1): 31-39.
41. Bandekar, P.P., & Suguna, G.C. LSB Based Text and Image Steganography usingAES Algorithm. Proceedings of the International Conference on Communication and Electronics System. 2021; 782-788
42. Setiadi D R I M, Jumanto J. An Enhanced LSB-Image Steganography Using Hybrid Canny-Sobel Edge Detection. Cybern Information Technology. 2018; 18(2): 74-78.
43. Al-Amri R M, Hamood D N, Farhan A K. Image Steganography Based on Chaotic Function and Randomize Function. Iraqi Journal of Computer Science and Mathematics. 2023; 4(1): 71-86.
44. Tauhid A, Tasnim M, Noor S A, Faruqui N, Yousuf M A. A Secure Image Steganography using Advanced Encryption Standard and Descrete CosineTransform. Journal of Information Security. 2018; 10(3): 117-129.
45. Beza T. Secure Mobile Banking Framework by using Cryptography and Steganography Methods. Global Strategy Journal. 2018; 6(8): 863-882.
46. Ganesh R S, Nagaraj V, Sivakumar S A, Shankar B M. An Intelligent and Hybrid Method of Combining Spatial Domain and Frequency Representation for Digital Image Steganography. 3rd International Conference on Intelligent Sustainable Systems. 2020; 1057-1061. Doi: 10.1109/icss49785.2020.9315918.
47. Alexan W, Hamza A, Medhat H. An AES Double-Layer based Message Security Scheme. *2019* International Conference on Innovative Trends in Computer Engineering, Aswan, Egypt, 86-91.
48. Panwar S, Damani S, Kumar M. Digital Image Steganography using Modified LSB and AES Cryptogarphy. International Journal of Recent Engineering Research and Development. 2018; 3(6): 18-27.