A Secured Framework for Short Messages Service in Global System for Mobile Communication

*Aminu S. Ahmed and Mohammed Lawal
Department of Computer science, Ahmadu Bello University, Zaria, Nigeria
{smbaminu|mlawal}@gmail.com

Received: 09-FEB-2022; Reviewed: 21-APR-2022; Accepted: 06-MAY-2022
https://doi.org/10.46792/fuoyejet.v7i2.796

ORIGINAL RESEARCH ARTICLE

Abstract- Short Message Service (SMS) has upgraded and elevated our lives and is principal in our livelihood. This service has been driven by the Global System for Mobile Communications (GSM) which is the most popular standard for mobile telephony systems. As a result, the GSM has constituted the moderate execution of short message service (SMS), which has uplifted mobile phone quality. A proper understanding of the essentials of SMS/MMS security opens the door to prevent some common security. which has fostered the prevention of some common threats in SMS usage. Unfortunately, the SMS does not have any built-in vetting procedure to authenticate the text or provide security for the data/text, and supportive phone facilities are designed without considering the SMS/MMS security aspects. There is also a problem of mobile applications developer and the mobile service providers not knowing the correct identities of the communicating parties, and also the problem of little to no SMS/MMS content confidentiality and integrity during data transmission. This paper is aimed at addressing these problems by focusing on the use of substitution techniques of audio steganography. We achieve our method by having a low robustness against attacks which try to reveal the hidden message. This allows only SMS that is encrypted, and application to multimedia messages needs to be further investigated. Furthermore, encryption is done using substitution cipher methods. We also analyse the security mechanism based on the mobile security requirements and mobile performance capability. Analysis of the security mechanism based on the mobile security requirements and mobile performance capability is carried out. After an exhaustive computer simulation, the performance of the proposed method is confirmed. The result obtained showed that compression ratio achieved is within the range of 0.1 and 0.5, the best achieved so far. In this study, colour pictures were utilized as main pictures, but grey colour pictures can be investigated in the comparable way. Our study encompasses a supplementary safeguard encryption method alongside an alternative rotation method and a reconstruction key. Supplementary convoluted rotation manner makes it harder for unauthorized people to reconstruct pictures lacking the appropriate keys.

Keywords- Encryption, Global System for Mobile Communications, GSM, SMS, substitution cipher

1 INTRODUCTION

Short Message Service (SMS) has upgraded and elevated our lives and is principal in our livelihood. SMS is a popular universal medium means for delivering the distribution of Value-Added Services and are suitable appropriate for mobile banking, payment reminders, stock and news alerts, railway and flight enquiries etc. (Narendiran et al., 2008). These types of messages are usually computer-generated messages sent in excess of Short Message Peer to Peer (SMPP) protocol. Sending an SMS remains cheap, fast, and humble. It is a store-and-forward, stress-free to use, widely held, and low-cost service. SMS is the text communication service component of mobile communication systems, using standardized qualitative communications protocols that allow the exchange of short text messages between mobile phone devices. The existing SMS is not free from eavesdropping, but security is the main concern for any business company such as banks who will provide these mobile banking. Presently, there is no such scheme, which can give the complete SMS security (Hossain et al., 2008).

GSM (Global System for Mobile Communications) is the most popular standard for mobile telephony systems in the world (Khozooyi, 2009). So, in 1982, the European Conference of Postal and Telecommunications Administrations (CEPT) created the Group Special Mobile (GSM) toward cultivate a standard intended for a mobile telephone system that could be used across Europe. The GSM Association estimates that 80% of the global mobile market uses the standard. GSM is used across more than 212 countries and territories. GSM pioneered low-cost implementation of the short message service (SMS), also called text messaging, which has since been supported on other mobile phone standards as well.

In the GSM, only the airway traffic between the Mobile Station (MS) and the Base Transceiver Station (BTS) is optionally encrypted with a weak and broken stream cipher (A5/1 or A5/2). The authentication is unilateral and vulnerable (Toorani & Shirazi, 2008). The development of UMTS introduces an optional Universal Subscriber Identity Module (USIM), that uses a longer authentication key to give greater security, as well as mutually authenticating the network and the user - whereas GSM only authenticates the user to the network (and not vice versa). The security model therefore offers confidentiality and authentication, but limited authorization capabilities, and no non- repudiation. The BTS act as a transmitter and receiver of the radio signals from mobile phones. The BTS translates the radio signals into digital format and then it transfers the digital signals to the Base Station Controller

SMS is a technology that enables the sending and receiving of messages between mobile phones. SMS first

*Corresponding Author

Section B- ELECTRICAL/ COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Ahmed A.S. and Lawal M. (2022): A Secured Framework for Short Messages Service in Global System for Mobile Communications, *FUOYE Journal of Engineering and Technology* (FUOYEJET), 7(2), 133-140. http://doi.org/10.46792/fuoyejet.v7i2.796

appeared in Europe in 1992. Later it was ported to wireless technologies like CDMA and TDMA. The GSM and SMS standards were originally developed by ETSI. ETSI is the abbreviation for European Telecommunications Standards Institute. Now the 3GPP (Third Generation Partnership Project) is responsible for the development and maintenance of the GSM and SMS standards (Toorani & Shirazi, 2008). The rapid development in mobile communication has transformed SMS as widespread tool for business and social messaging (Saleem & Doh, 2009). SMS services are growing day by day. With SMS, people can easily share personal and official messages in a cost-effective manner. SMS enables the transmission of up to 1120 bits alphanumeric messages between mobile phones and external systems. It uses SMS centre (SMS-C) for its routing operation in a network and can be transmitted into another network through the SMS gateway (Brown, Shipman & Vetter, 2007).

SMS usage is threatened with security concerns (Lisonek & Drahansky, 2008), such as eavesdropping, interception and modification. SMS messages are transmitted as plaintext between the mobile stations and the SMS centre using the wireless network. SMS content are stored in the systems of the network operators and can easily be read by their personnel. The A5 algorithm (Toorani, Asghar, & Shirazi, 2008) which is the GSM standard for encrypting transmitted data, can easily be compromised. Therefore, there is a need to provide an additional encryption on the transmitted messages. As suggested by the name Short Message Service, the data that can be held by an SMS message is very limited. One SMS message can contain at most 140 bytes (1120 bits) of data, so one SMS message can contain up to (DeSantis, Castiglione & Petrillo, 2010).

Understanding the basics of SMS/MMS security opens the door to preventing some common security threats in SMS usage (Stallings, 2006; Toorani, Asghar, & Shirazi, 2008). Attacks such as man-in-middle attack, replay attack, message disclosure, spamming, denial of service (DoS), SMS phone crashes, SMS viruses, and SMS phishing have all proven too dangerous. One of the important challenges in the mobile communication industry is to ensure the mobile services are properly used and not open to abuse (Al-Fayoumi et al., 2007; Hwu et al., 2006).

Additionally, unencrypted SMS content during the transmission allows the mobile operator's employee to read and modify the SMS content. Unfortunately, the SMS does not have any built-in vetting procedure to authenticate the text or provide security for the data/text transmitted (Hossain et al., 2008). It is obvious that parts of the SMS/MM applications for mobile devices are designed and developed without taking into account the SMS/MMS security aspects. Therefore, all SMS/MMS facilities should incorporate some form of basic security mechanism in terms of confidentiality, integrity, authentication and non-repudiation of the messages before it can be deemed suitable for use by the government, commercial and military services (Garza-Saldana and Daz-Pérez, 2008; Hassinen, 2005; Hassinen and Markovski, 2003). Exchanging normal SMS/MMS does not guarantee the confidentiality as it is not totally secure and reliable since the messages are transferred in a text-mode (readable) through an insecure transmitting channel. Beside improving and enhancing the secret of the SMS/MMS content without being unlawfully tempered (Wu and Tan 2009; Zhang et al., 2005; Zhao et al., 2008). In simple term, the unprotected communication channels and the increasing popularity of the wireless devices pose serious security vulnerabilities. Thus, it is important that both the mobile applications developer and the mobile service providers (mobile operator) ensure the correct identities of the communicating parties, while at the same time, ensure SMS/MMS content confidentiality and integrity during data transmission period to avoid these threats (Tiejun et al., 2008).

SMS is encrypted using substitution cipher (like in existing technique). The sender will enter the SMS, substitute the SMS, convert SMS to binary, convert binary to ASCII, encrypt the ASCII value using RSA encryption algorithm, then get the decipher text. In order to decipher the text, the receiver has to use the key to decipher the ASCII value and get the content of the SMS. MMS will use the method of digital embedding where the original image is hidden by a random image which could survive attacks on the network (Pointcheval, 2002). The aim of this paper is to provide useful solution to the SMS/MMS security topic.

This study addresses the following problems of substitution techniques of audio steganography:

i. Having low robustness against attacks which try to reveal the hidden messages.
ii. Only SMS is encrypted because it has no much security to accommodate multimedia messages
iii. Encryption is done using substitution cipher

The remaining parts of the paper are sectioned as follows: a review of related studies is presented in Section 2; in Section 3, we show the methodology designed to address the problem described in the domain; experimentation and results in addition to discussion on results are presented in Sections 4 and 5; conclusion on the study is presented in Section 6.

2 Related Work

Cryptography is the science of including a hidden message in a piece of communication and is an antique art; the early documented use of cryptography dates back to circa 1900 B.C. after an Egyptian scribe utilized non-standard hieroglyphs in an inscription. Cryptography, then, materialized spontaneously at some point afterwards as its application in passing covert political messages and military plans became apparent. It is no surprise, next, that new forms of cryptography were rapidly discovered following the extensive progress of computer communications. In data and telecommunications, cryptography is vital as conversing using an untrusted medium, such as the internet, always carries some risk of unwanted hosts intercepting/reading the message. Within the context of each application-to-application contact, there are little specific protection necessities put in place. This section provides an overview

http://doi.org/10.46792/fuoyejet.v7i2.796 http://journal.engineering.fuoye.edu.ng/

on the background of the discoveries by elucidating keywords and contexts critical to the understanding of the study.

Kamali et al. (2010) analysed Advance Encryption Standard (AES) algorithm and present a modification to the Advanced Encryption Standard (MAES) to reflect a high-level security and better image encryption. Their results so that after modification image security is high. They also compare their algorithm with original AES encryption algorithm. Younes & Jantan (2008) introduce a new permutation technique based on the combination of image permutation and a well-known encryption algorithm called RijnDael. The original image was divided into 4 pixels × 4 pixels blocks, which were rearranged into a permuted image using a permutation process, and then the generated image was encrypted using the RijnDael algorithm. Their results showed that using the combination technique significantly decreased the correlation between image elements and higher entropy was achieved.

Yun-Peng et al. (2009) researched the chaotic encryption, DES encryption and a combination of image encryption algorithm. In their technique firstly, new encryption scheme uses the logistic chaos sequencer to make the pseudo-random sequence, carries on the RGB with this sequence to the image chaotically, then makes double time encryptions with improvement DES. Their result show high starting value sensitivity, and high security and the encryption speed. Abuhaiba & Hassan (2011) present a new effective method for image encryption which employs magnitude and phase manipulation using Differential Evolution (DE) approach. They have carried out key space analysis, statistical analysis, and key sensitivity analysis to demonstrate the security of the new image encryption procedure.

Shah et al. (2011) proposed a criterion to analyse the prevailing S-boxes and study their strengths and weaknesses in order to determine their suitability in image encryption applications. The proposed criterion uses the results from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to advanced encryption standard (AES), affine-power-affine (APA), gray, Lui J, residue prime, S8 AES, SKIPJACK, and Xyi Sboxes. Enayatifar & Abdullah (2011) proposed a new method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption. In their technique, first a number of encrypted images are constructed using the original image with the help of the chaotic function. In the next stage, these encrypted images are employed as the initial population for starting the operation of the genetic algorithm. Then, the genetic algorithm is used to optimize the encrypted images as much as possible. In the end, the best cipher-image is chosen as the final encryption image.

Younes & Jantan (2008) introduced a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm, and then the transformed image was encrypted using the Blowfish algorithm. Their results showed that the correlation between image elements was significantly decreased. Their results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy. Nag et al. (2011) proposed a two-phase encryption and decryption algorithms that is based on shuffling the image pixels using affine transform and they encrypting the resulting image using XOR operation. They redistribute the pixel values to different location using affine transform technique with four 8-bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The total key size used in algorithm is 64 bits. Their results proved that after the affine transform the correlation between pixel values was significantly decreased.

3 METHODOLOGY

Due to the prevalence of the web link, there has been supplementary multimedia data transmission on the Internet. In the multimedia data transmission, pictures are dispatched in elevated rate. Halting vital picture data from being stolen by the eavesdroppers is becoming an important task. On behalf of every single link arrangement, it is vital to grab into report two main requirements: a fast transmission to dispatch the data from a transmitter to a receiver that can be finished retaining an effectual compression method and a safeguard transmission of data that can be attained retaining a prominent encoding algorithm. To gratify these constraints, new compression and encryption methods permitting a fast and safeguard data transmission are counselled in the literature. Accordingly, we counsel to link compression alongside encryption and counsel a new method of compression and encryption at comparable time.

In this study, first the sender will enter SMS, substitute the SMS, convert SMS to binary then convert binary to ASCII encrypt the ASCII value using RSA encryption algorithm then get decipher text. In other to decipher the text the receiver has to use the key to decipher the ASCII value and get the content of the SMS. In order to encrypt the pictures, we cover the pictures alongside an insignificant image. Our new method is instituted on the obscuring of data embedding in the transmitter side and grabbing out removing algorithm in receiver side the decoding phase. We perform data compression to improve the speed of communication. On achieve this aim, we utilized Discrete Cosine Change (DCT) and cut out the higher-frequency constituents because most of the manipulations are performed in the lower frequency clusters by DCT. Subsequently, the compressed DCT constituents are rotated; the rotations have one extra aspect. The orders and degrees of the rotations are saved as the key to reinstate the main images. If the receiver is not in possession of the key, it is hard to reinstate the main images (Yun-peng et al., 2009).

http://doi.org/10.46792/fuoyejet.v7i2.796 http://journal.engineering.fuoye.edu.ng/

In this undertaking, we are retaining the method of digital embedding whereas a random picture that could tolerate aggressions on the web hides the main picture. The digital embedding method counselled for obscuring a picture into one extra picture helps to prop the quality of the recouped image. The picture file that is to be hidden is here denoted as Target Picture and the picture behind that it is to be hidden is termed as cover image.

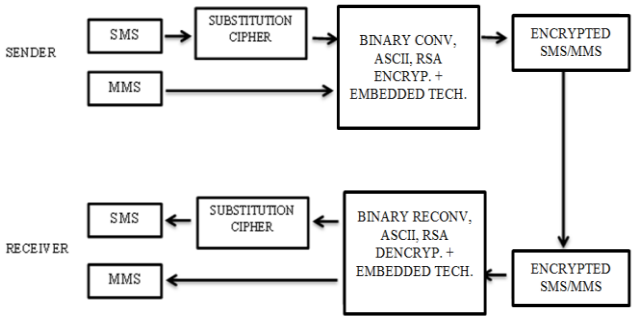

Fig. 1: the block diagram of the Proposed Technique

This is the block diagram for the whole project, but in other to make it more detailed we break it in to two-part A and B part A for the SMS part B for the MMS/IMAGE. The following constitute the components in the system as seen in Figure 1:

- Transmitter frontier procedure (SMS)
- Receiver frontier procedure (SMS)
- Transmitter frontier procedure (MMS/Image)
- Receiver frontier procedure (MMS/ Image)
- Transmit (MMS/ Image)

Rivest - Shamir – Adleman (RSA) structure is a chunk cipher in that the plain text and cipher text are integers amid 0 and n-1 for a little n. That is the block size have to be less than or equal to $\log_2 n$ in exercise the block size is 2k Bits, however 2 are of the hounding procedure for a little plain text M and cipher text C = Pe mod n and P = Cd mod n (Pointcheval, 2002).

What follows is a description of the RSA scheme. To produce the area and the confidential keys, select two colossal prime numbers p, q such that p is not equal to q, randomly and independently of every single other. [33]

Process n = p * q

Process the proportion Ø (n) = (p-1) (q-1) Select an integer e such that 1< e <Ø (n) that is co-prime to Ø (n)

Compute d such that d*e (mod Ø (n) = 1

Assessing random numbers of the right size alongside probabilistic chiefly examinations that swiftly remove nearly all non-primes normally completes finding the colossal prime numbers. p and q ought to not be too close. Moreover, if p-1 and q-1 has merely tiny prime factors n can be factored swiftly and these benefits of p and q ought to consequently be discarded as well. It is vital that the hidden confidential key d ought to be of sufficient length (Pointcheval, 2002). For a fast link, we ought to like to cut the number of dispatching data. Subsequently compression of the DCT constituents is required. In every single solitary block, most of DCT constituents have elevated energies in low frequency clusters we merely use low frequency constituents across a facile low bypass filter that is left-up corners of every single solitary block alongside size of NC × NC are selected and higher frequency constituents are dropped. As a consequence of this procedure, we can compress the dispatching images.

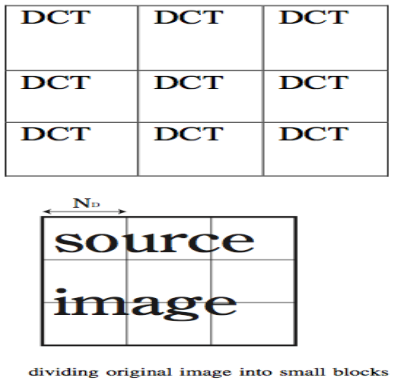

Fig. 2: Dividing original image into small blocks (Yun-Peng, 2009)

Here in Figure 2, we divided the main picture into smaller blocks and apply DCT. After the compression, we rotate the blocks randomly. Consequently, in order to get around this setback, we rotate every single solitary block randomly so as to craft rotated DCT constituents be self-governing of every single solitary other; see Figure 3.

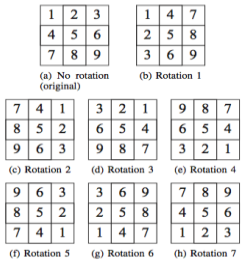

Fig. 3: Rotation patterns

The compressed rotated picture is obscured by a random picture and sends to destination. Authorized people accord the mixtures and remove it. Curving back the rotated DCT constituents and employing inverse discrete cosine change (IDCT) early pictures are decrypted [31][32]. After separation of the main picture and random picture main pictures are reconstructed. The rotated DCT constituents have to be restored. The transmitter beforehand gives the receiver the rotation key. The receiver can reconstruct the main pictures rotating the DCT constituents contrary to the encryption stage.

The following describes the algorithm of the entire procedure:

Sender (SMS)

Step 1: Sender will enter SMS
Step 2: Substitute the SMS
Step 3: Convert SMS to binary
Step 4: Convert binary to ASCII
Step 5: Encrypt the ASCII value using RSA encryption algorithm
Step 6: Get deciphers text.

Receiver (SMS)

Step 1: Use the key to decipher the ASCII value
Step 2: Compare the ASCII value with the one that was sent
Step 3: Get the content of the SMS

http://doi.org/10.46792/fuoyejet.v7i2.796 http://journal.engineering.fuoye.edu.ng/

Transmitter (MMS-Image)
First rip the main or target picture into blocks and apply DCT Discrete Cosine Makeover on every single solitary blocks
Then rotate the DCT blocks retain the association of rotation as key for reconstructing the picture.
Then cover the main picture alongside one extra random picture
The random picture is additionally torn into blocks and DCT is applied on every single solitary block. The main picture is obscured by a random picture and it is dispatched to the destination. This procedure is called embedding.

Receiver (MMS-Image)
The random picture is seized out.
This procedure is called extraction
Using the rotation key the DCT blocks are reconstructed from the base picture, then to every single block we apply inverse DCT.
The picture is reconstructed
.

4 SIMULATION

MATLAB matrix workshop is MATLAB is a high-level technical computing speech and interactive nature for algorithm progress data visualization data scrutiny and numeric computation We can use MATLAB in an expansive scope of demands encompassing gesture and picture processing link manipulation design examination and measurement business modelling and scrutiny and computational biology. Add-on toolboxes collections of special-purpose MATLAB intentions obtainable separately range the MATLAB nature to ascertain particular classes of setbacks in these appeal areas. MATLAB provides a number of features for documenting and allocating your work. You can incorporate your MATLAB plan alongside supplementary tongues and demands and allocate your MATLAB algorithms and applications. Retaining the MATLAB product, you can ascertain technical computing setbacks faster than alongside instituted multimedia design tongues such as C/ C++ and FORTRAN. MATLAB additionally provides all the features of an instituted multimedia design speech encompassing arithmetic operators flow domination data constructions data kinds object-oriented multimedia design (OOP) and debugging features.

Optimization and numerical integration, 2-D and 3-D graphics intentions for visualizing data, Tools for constructing rehearse graphical user interfaces; Functions for incorporating MATLAB instituted algorithms alongside external demands and tongues such as C/ C++ Fortran Java COM and Microsoft Excel; and Function Utilized in the Code.

MATLAB provides many functions for image processing and other tasks. Most of these functions are written in the MATLAB language and are publicly readable as plain text files. Thus, the implementation details of these functions are accessible and open to scrutiny. The defence can examine the processing used in complete detail, and any challenges raised can be responded to in an informed way by the prosecution. This makes MATLAB very different from applications, such as Photoshop. It should be noted that some MATLAB functions couldn't be viewed. These are generally lower-level functions that are computationally expensive and are hence provided as 'built-in' functions running as native code. These functions are heavily used and tested and can be relied on with considerable confidence.

In the following paragraphs, we show demonstration of the simulation. In Figure 4, is the initialization period in the simulation whereas you can select 1 for SMS or 2 for MMS. Also in Figure 5, is the period whereas the RSA key has been generated and the confidential key is 5, and the area keys are 2426. Later producing the key next kind, the memo and dispatch to receiver.

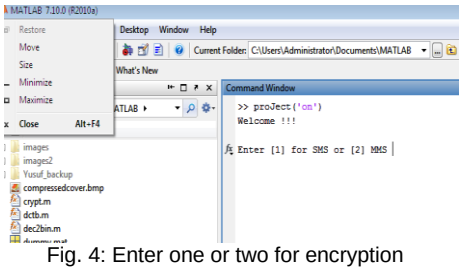

Fig. 4: Enter one or two for encryption

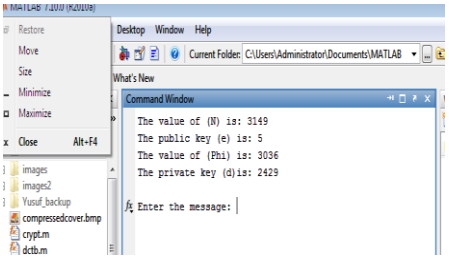

Fig. 5: Enter SMS for RSA encryption

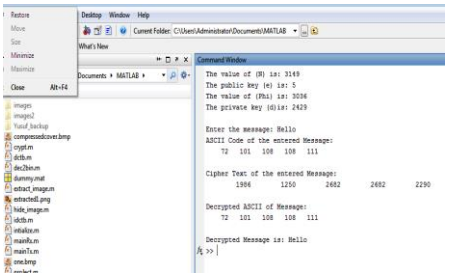
Fig. 6: SMS encryption and decryption out put

In Figure 6 is the final period afterward producing the RSA key, and the plain text has been typed next it will change the memo to binary from binary to decimal in supplementary to become the ASCII worth, afterward that next it will encrypt the ASCII worth and dispatch to it destination, after the receiver become the memo and difference the ASCII worth to be able to decrypt the cipher text.


Fig. 7: Input image

http://doi.org/10.46792/fuoyejet.v7i2.796 http://journal.engineering.fuoye.edu.ng/

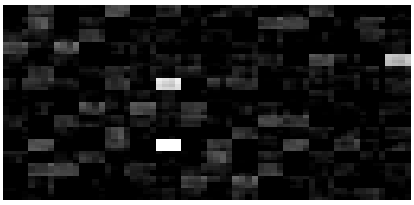

Fig. 8: Compressed output

In Figures 7 and 8, the original and compressed image are shown. Discrete Cosine Transform: At first, we divide original images to be transmitted into small square blocks and apply two-dimensional discrete cosine transform to each block and we obtain DCT components of each block. In the following simulations, the size of DCT blocks, N_D is varied, and the performances are evaluated.

5 Result and Discussion

Here, to evaluate the performance of the proposed method. we quantized the performance using root mean square error (RMSE), which is defined as

$$\mathrm{RMSE_{orig}} = \sqrt{\frac{1}{L^2}\sum_{i,j=1}^{L}\left(\mathrm{I_{orig}}(i,j) - \alpha \mathrm{I_{est}}(i,j)\right)^2},$$

Where $I_{orig}(i,j)$ is (i,j)th pixel of the original image to be transmitted, $I_{est}(i,j)$ is that of the restored image, L is a size of images, i.e., 256, and α is the scaling factor. Using the proposed method, the higher frequency components are cut off, that is, the quality of the original image is reduced. Therefore, $RMSE_{comp}$ is also defined

$$\mathrm{RMSE_{comp}} = \sqrt{\frac{1}{L^2}\sum_{i,j=1}^{L}\left(\mathrm{I_{comp}}(i,j) - \alpha \mathrm{I_{est}}(i,j)\right)^2},$$

Where $I_{comp}(i, j)$ is also the (i, j)th pixel of the compressed original image, which is obtained by applying IDCT to the compressed DCT components. $RMSE_{comp}$ indicates the performance excludes compression process, while $RMSE_{orig}$ shows the performance of the whole process.

Varying DCT size N_D and compression (smaller) block size N_C , we calculate RMSEs. Using two images, Lena image and a random image, the results are shown in Fig. 9 and using three images, Lena, Mandrill and random images, in Figure 10. In the figures horizontal axis denotes the ratio of compression size to DCT size, vertical axis is RMSE. Solid lines show the results in the cases where N_D is 4, dashed lines 8, dotted-dashed lines 16, and dotted lines 32. The smaller DCT block size we use, the smaller RMSE is. When the ratio of compression size to DCT size is from 0.1 to 0.5, the best RMSEs were obtained. If the compression size is too large, most of DCT components are near zero and independent assumption is no longer satisfied. Conversely if the compression is small, only the low frequency components are left and they also have high correlations. Therefore, we must choose an optimal compression size.

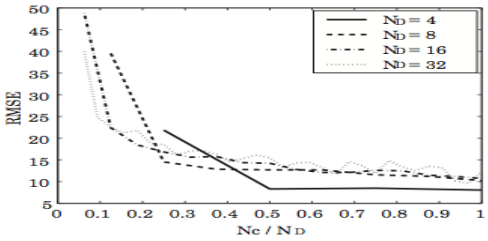

Fig. 9: RMSE between original source images and reconstructed images ($RMSE_{orig}$)

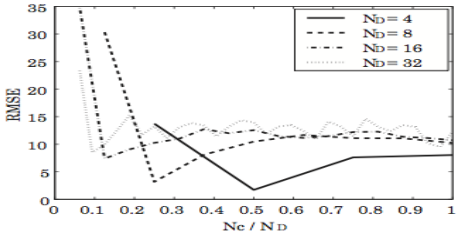

Fig. 10: RMSEs for two images

Here, in order to evaluate the performance of the proposed method. we quantized the performance using root mean square error (RMSE), which is defined as

$$\mathrm{RMSE_{orig}} = \sqrt{\frac{1}{L^2}\sum_{i,j=1}^{L}\left(\mathrm{I_{orig}}(i,j) - \alpha \mathrm{I_{est}}(i,j)\right)^2},$$

Where $I_{orig}(i,j)$ is (i,j)th pixel of the original image to be transmitted, $I_{est}(i,j)$ is that of the restored image, L is a size of images, i.e. 256, and α is the scaling factor. Using the proposed method, the higher frequency components are cut off, that is, the quality of the original image is reduced. Therefore, $RMSE_{comp}$ is also defined

$$\mathrm{RMSE_{comp}} = \sqrt{\frac{1}{L^2}\sum_{i,j=1}^{L}\left(\mathrm{I_{comp}}(i,j) - \alpha \mathrm{I_{est}}(i,j)\right)^2},$$

Where $I_{comp}(i, j)$ is also the (i, j)th pixel of the compressed original image, which is obtained by applying IDCT to the compressed DCT components. $RMSE_{comp}$ indicates the performance excludes compression process, while $RMSE_{orig}$ shows the performance of the whole process.

Varying DCT size N_D and compression (smaller) block size N_C, we calculate RMSEs. Using two images, Lena image and a random image, the results are shown in Fig. 9 and using three images, Lena, Mandrill and random images, in Figure 10. In the figures horizontal axis denotes the ratio of compression size to DCT size, vertical axis is RMSE. Solid lines show the results in the cases where N_D is 4, dashed lines 8, dotted-dashed lines 16, and dotted lines 32. The smaller DCT block size we use, the smaller RMSE is. When the ratio of compression size to DCT size is from 0.1 to 0.5, the best RMSEs were obtained. If the compression size is too large, most of DCT components are near zero and independent assumption is no longer satisfied. Conversely if the compression is small, only the low frequency components are left and they also have high correlations. Therefore, we have to choose an optimal compression size.

http://doi.org/10.46792/fuoyejet.v7i2.796 http://journal.engineering.fuoye.edu.ng/

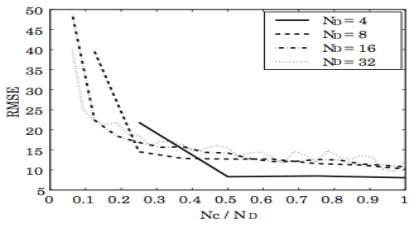

Fig. 11: RMSE between original source images and reconstructed images ($RMSE_{orig}$)

6 Conclusion

A new method is address two setbacks of the substitution method of picture steganography. Main setback owns low robustness opposite aggressions that endeavour to expose the hidden memo and the other setback owns low robustness opposite distortions alongside elevated average power. An intelligent algorithm will endeavour to embed the memo bits in the deeper layers of examples and change supplementary bits to cut the error and if alteration is not probable for every single solitary example it will flout them. Retaining the counselled hybrid embedding technique, memo bits could be embedded into countless, unclear and deeper layers to finish higher capacity and robustness. In the decryption era the obscured pictures can be removed from the mixtures by demanding extraction algorithm. In the conclude retaining rotation keys and inverse discrete cosine change the main pictures can be reconstructed. Therefore, we can finish a fast and safeguard picture transmission. As a consequence of countless computer simulations, the deeds of the proposed method are confirmed. Later compression ratio is between 0.1 and 0.5 the best presentation can be achieved. In this consenting colour pictures utilized as main pictures but grey colour pictures can be demanded in the comparable way. Our upcoming works encompass a supplementary safeguard encryption method alongside an alternative rotation method and a reconstruction key. Supplementary convoluted rotation manner makes it harder for unauthorized people to reconstruct pictures lacking keys.

References

Abuhaiba, Ibrahim S I and Maaly A. S Hassan (2011), ―Image Encryption Using Differential Evolution Aproach In Frequency Domain‖ Signal & Image Processing Journal (SIPIJ) Vol.2, No.1, March 2011.

Bhowal K., Anindya Jyoti Pal, Geetam S. Tomar, P. P. Sarkar (2010), "Audio Steganography using GA", IEEE Proceedings, 2010.

Brown J., B. Shipman, and R.S. Vetter (2007),"SMS: The short message service," Computer, vol.40, no.12, 2007, pp.106-110.

Chen C., and Rong-Jian Chen, (2006) "Image Encryption and Decryption Using SCAN Methodology", Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06)

DeSantis A., Aniello Castiglione and Umberto Ferraro Petrillo (2010) "An Extensible Framework for Efficient Secure SMS" International Conference on Complex, Intelligent and Software Intensive Systems, IEEE, pp 843-850.

Enayatifar R., Abdul Hanan Abdullah (2011), ―Image Security via Genetic Algorithm‖, 2011 International Conference on Computer and Software Modeling IPCSIT vol.14.

Garza-Saldana J. J. and A. Diaz-Perez (2008), "State of security for SMS on mobile devices", Proceedings of the Electronics, Robotics and Automotive Mechanics Conference, 2008, pp. 110 - 115

Hossain M. A., S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz (2008), "A proposal for enhancing the security system of short message services in GSM", 2nd International Conference on Anti-counterfeiting, Security and Identification, ASID, Guiyang, China, IEEE, pp. 235-240.

Kamali, S.H., Shakerian, R., Hedayati, M. Rahmani, M. (2010), A new modified version of Advance Encryption Standard based algorithm for image encryption, Electronics and Information Engineering (ICEIE), 2010 International Conference.

Khozooyi, N., Maryam Tahajod, Peyman khozooyi (2009), "Security in Mobile Governmental Transactions", Second International Conference on Computer and Electrical Engineering, pp 168-172.

Lisonek D. and M. Drahansky (2008), "SMS Encryption for Mobile Communication", in Security Technology, SECTECH '08. International Conference, pp 198–201.

Masanori Ito and Noboru Ohnishi, Ayman Alfalou, Ali Mansour (n.d.) New Image Encryption and Compression Method Based on Independent Component Analysis

Nag A., Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar Partha Pratim Sarkar (2011), ―Image Encryption Using Affine Transform and XOR Operation, International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

Narendiran C., S. Albert Rabara, N. Rajendran (2008), "Performance Evaluation on End-to-End Security Architecture for Mobile Banking System", 978-1-4244-2829-8/08, IEEE.

Onwutalobi A. "Using Encryption Technique". Department of Computer Science University of Wollongong

Pointcheval D., RSA Laboratories' CryptoBytes (2002), "How to Encrypt Properly with RSA", Volume 5, No.1, Winter/Spring 2002, pp. 9-19.

Saleem M., Kyung-Goo Doh (2009), "Generic Information System Using SMS Gateway", 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, pp 861-866.

Saleem M., Kyung-Goo Doh (2009), "Generic Information System Using SMS Gateway", 2009 Fourth International Conference on Computer Sciences and Convergence Information Technology, pp 861-866.

Shah T., Iqtadar Hussain, Muhammad Asif Gondal, Hasan Mahmood (2011), Statistical analysis of S-box in image encryption applications based on majority logic criterion‖, International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011

Stallings W. (1999) "Cryptography and Network Security" 5th Edition, PrenticeHall,1999

Stallings W. (2006), "Cryptography and network security", Prentice Hall, New Jersey, United States.

Sun H., Mu-En Wu, Wei-Chi Ting, and M. Jason Hinek, (2007) "Dual RSA and Its Security Analysis", IEEE Transactions on Information Theory, VOL. 53, NO. 8, pp. 2922-2933

Toorani M. and A. Beheshti Shirazi (2008), "SSMS - A secure SMS messaging protocol for the m-payment systems", in Computers and Communications, IEEE Symposium, pp 700–705.

Toorani M., Ali Asghar and Beheshti Shirazi (2008), "Solutions to the GSM Security Weaknesses", the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, 978-0-7695-3333-9 /08, pp 576-581.

Watson A.B. (1994) Image Compression Using the Discrete Cosine Transform NASA Ames Research Center, Mathematica Journal, 4(1), 1994, p. 81-88

Whitfield Diffie & Martin E. Hellman (1979) "Privacy and Authentication: An Introduction to Cryptography". proceedings of the IEEE, vol.67, no.3

Younes M.A.B and Aman Jantan (2008) —Image Encryption Using Block-Based Transformation Algorithm‖ IAENG International Journal of Computer Science, 35,2008.

Younes M.A.B and Aman Jantan (2008), —An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption‖, IJCSNS International Journal of Computer Science and Network Security, VOL.8, April 2008.

Yun-peng Z., Liu Wei, Cao Shui-ping, Zhai Zheng-Jun, Nie Xuan, Dai Wei-di (2009). Digital image encryption algorithm based on chaos and improved DES‖, IEEE International Conference on Systems, Man and Cybernetics, 2009.

Zamani M., Azizah Bt Abdul Manaf, Hossein Rouhani Zeidanloo and Saman Shojae Chaeikar (2011), "Genetic substitution-based audio steganography for high capacity applications", Int. J. Internet Technology and Secured Transactions, Vol. 3, No. 1, 2011,97-110.

Zamani M., Hamed Taherdoost, Azizah A. Manaf, Rabiah B. Ahmad, and Akram M. Zeki (2009), "Robust Audio Steganography via Genetic Algorithm", IEEE, 2009.