American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-9, Issue-3, pp-44-52
www.ajer.org
Research Paper Open Access

Enhancing Information Security in Android Smart Devices Implementing Steganography and AES to Hide Secret Messages inside an Image

Benjamin Sarpong[1] and Dr.Zhihua Li [2]
[1]School of Internet of Things and Engineering Jiangnan University-China,
[2]School of Internet of Things and Engineering Jiangnan University-China,
Corresponding Author: Benjamin Sarpong,

ABSTRACT: *The use of modern devices such as android, blackberry and other smartphones is the result of improved communication technology over the years. As a result, there are several security concerns that continue to arise because there are inadequate mechanisms in place to ensure that data and information are protected. Many have tried to use either cryptography or steganography, others have tried to combine the two techniques, but have not been able to use the optimal methods of both cryptography and steganography. However, this research combines the use of the best techniques in both steganography and cryptography to create a system that is more robust and therefore resistant to attack. With the help of steganography technology and Advanced Encryption Scheme, the authors propose a new algorithm for hiding data within the image. The suggested algorithm uses binary codes and pixels in the image. The proposed algorithm is used to develop a system called Hide Me. The system is then tested to determine the viability of the proposed algorithm. Various data dimensions are processed inside the images and the PSNR (Peak signal-to-noise ratio), for each of the images tested. Depending on the PSNR value of each image, the stego image has a higher PSNR value. The new steganography algorithm is therefore very effective in hiding the data inside the image. The process of encoding a message or data to a non-readable file format in such a way that a third party or an attacker, other than the intended receiver, does not know the meaning of the message lie as cryptography. Steganography often deals with the act of hiding a message from an unauthorized person in a cover item. This work utilizes maximal steganography and cryptography. The Least Significant Bit (LSB) technique is used to incorporate or embed a message into a cover element. The cryptography employed in this research uses the symmetric cryptography known as AES. The pairing of both the LSB insertion technique and the AES technique for use by the proposed system makes it one of the best applications to ensure data security and confidentiality on smart Android devices. It can be realized that the security and strength of the proposed smartphone system lies in the combination of cryptography and steganography. One remarkable thing about the proposed system is that unlike other existing steganographic systems that are unable to support different types of image files, the proposed system is capable of doing so.*

KEYWORDS*-Steganography, cryptography, stego image, PSNR (Peak signal-to-noise ratio), Least Significant Bit (LSB)*

Date of Submission: 25-02-2020 Date of acceptance: 05-03-2020

I. INTRODUCTION

In this 21st century, information technology has become emerging and highly resourceful; therefore, there is a need to increase global and competitive change around the world. The best way to achieve confidentiality of data transmission is through the application of cryptography and steganography. The application of cryptography and steganography has been shown to give a higher level of security to the sensitive document being transmitted. Data sharing among smartphones has become very widespread because of how prevalent smartphones have become.

This paper however proposes a new system for hiding data inside images using a steganography technique. The algorithm is designed to hide all data entered into an image in order to safeguard the privacy of the data. The system is then built on the basis of a new steganography algorithm. The proposed system includes an image interface for the user to insert the image and a text box to input the message. Once the proposed algorithm has been modified, a user can send the stego image to another smart android user so that only intended receiver can retrieve and read the data hidden in the stego image using the same proposed system. Information can, therefore, be protected without exposing the contents to other individuals.

HideMe is a system that is capable of hiding information inside the image. The system utilizes two layers of security to protect data privacy. The system is using 2 layers of security in order to maintain data privacy. Data security is the process of shielding information against fraud and unauthorized access. Data security focuses on preserving confidentiality when maintaining private or organizational data. Privacy, on the other hand, is the right of an individual or a group to isolate themselves or to disclose information regarding themselves exclusively. Data privacy or knowledge security is the interaction involving data collection and distribution, engineering, community privacy preferences, and legal issues.

Problems of data privacy may emerge from a variety of sources such as health records, inquiries and prosecutions of criminal justice, financial institutions. As more and more devices are connected to the Internet, data security or data privacy has become increasingly important. There are privacy laws regulating privacy or data protection against unintentional or deliberate divulgation or abuse by individuals. Therefore, it is vital to conceal the data in a form such as the image to ensure that the safety or privacy of important data are safeguarded.

The rest of the paper is structured as follows: Section 2 discusses the related work and section 3 describes the algorithm proposed. Section 4 describes the implementation of the system and discusses the various results generated from testing the system on the basis of the algorithm proposed with different data sizes. The image is tested with the PSNR value also. In section 5, we conclude the article.

II. RELATED WORK

This chapter provides a comprehensive review on the principles and definitions of steganography, as well as the various types of steganography that exist today. Due to the numerous attacks and threats which encompassed smart phone technologies, steganography and cryptography technologies were developed.. Although the main reason for hiding the file in an archive is to discourage a third party from discovering the contents of the document, the person who has the permission can still access the message [1].Information hiding is the practice of embedding information into digital content without creating any potential deterioration [2].

2.1 History of Steganography

Three common strategies can be used in hiding information and they are watermarking, steganography, and cryptography. Steganography is known as the Greek word for writing. This requires any mechanism that deals with data or information in relation to other data. According to [3],steganography is derived from ancient Greek "Stegano," meaning something that is hidden or confidential, and "Graphia" or "Graptos," meaning putting down something or simply writing down on paper. Cover image is used to represent an object where the data to be sent is hidden within. According to [4], steganography is shielding the presence of a message by withholding information from different carriers. The main aim is to inhibit the disclosure of hidden information. Work in the steganography method dates back to ancient Greek where, during that period, the ancient Greek custom of tattooing a secret message on the shaved head of a slave messenger and letting his hair grow back before it was sent across enemy territory where the duration of this communication system was measured in months [5]. The most popular method in classical steganography around 440 B.C. was marking the text with invisible secret ink, like the juice of a lemon to hide information. Another approach was to mark chosen characters in a document with pinholes and to create a pattern or signature [5] .

2.2 Common Strategies for Hiding Information

Nevertheless, most of the advancement and use of computerized steganography emerged only in the year 2000 [6]. In order to achieve the intended purpose of steganography, certain methods must be applied.

According to [7], one or two of the aforementioned steganography techniques may be utilized: Spread Spectrum Techniques, Transform Domain techniques, and Substitution and Insertion Techniques. Nonetheless, according to [3]however, they describe substitution, injection and propagation as the most relevant techniques under steganography. Whereas substitution swaps a small fraction of the carrier file for the hidden message to remain undetected by the attacker, injection effectively prevents detection when the file is transferred to the cover media whilst propagation, however, discerns the use of cover entities but uses the generation engine provided by unseen data to imitate the file being audio, sound and text. Steganography is a method used to conceal secret data in an entity known as an image [8]. Generally, pixel strength is the tool used to mask data in image steganography, and therefore, images are the most known and widely used cover objects in steganography.

TIFF, JPEG, PNG, GIF and BMP can all be used for image steganography, according to [9]. Nonetheless, each of these file formats has its own unique characteristics. More often than not, there are sometimes variations in the amplitude of the actual image and the underlying signal; however, this transition is so slight and gradual that the human eye scarcely detects its identification and interpretation [10]. The key advantage of the Steganography algorithm is its simple security function. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme[11] . There are several steganography techniques used for hiding data such as batch steganography, permutation steganography, least significant bits (LSB), bit-plane complexity segmentation (BPCS) and chaos based spread spectrum image steganography (CSSIS). Several researchers have carried out work in the hiding of data in an image through steganography technique. Ibrahim et al. [12] proposed an approach to conceal data in audiovisual files, the secret information must be enclosed in a cover message in their steganography algorithm. On the other hand, El-Emam [13]suggested an steganography algorithm to hide a significant amount of high-security data. This steganography algorithm is based on hiding in a color bitmap (bmp) image a large amount of data (image, audio, text) file. In his work, the image will be filtered and segmented where bits are used to remove the correct pixels. Such pixels are randomly selected instead of chronologically. Chen et al. [14] modified an approach employed in [15] using the side match method. They focused on hiding the data in sections of the image's edges. On the other hand, Wu et al. [16] made use of pixel-value differencing by partitioning the original image into non-overlapping blocks of two successive pixels. This research uses a related concept introduced by El-Emam [13]. The data is stored in an image with the pixels, and the stego image pixels can then be accessed back to get the secret data back into the images. A Bitmap (bmp) image will then be taken to cover data, but a special message ID will be assigned and as well as the text be saved in a centralized database. The data is stored in an image with the pixels, and the stego image pixels can then be accessed back to get the secret data back into the images. A Bitmap (bmp) image will then be taken to cover data.

2.3 Concept of Steganography and Cryptology

Some basic requirements are necessary to maintain a valid and deliberately usable image steganography. The indistinctness of the steganographic element to the human eye is among these requirements the most fundamental feature. According to [10], the independence of the file format, unsuspicious files, payload capacity, strength against statistical attacks and concealment are some factors which make steganography unlike any other Nobody should notice that an image holds a code, otherwise the algorithm is impaired.. The payload efficiency is, according to [17], the amount of information that is inserted into an image without substantially degrading the image. Due to the independent file format, there is increasing suspicion. Al-Ataby and Al-Naima[18]claim that when images are rotated or cut, they should not degrade or change; this makes them resilient against image distortion. An example of a suspicious file is a large file or data. Attacks make image steganography insecure on the internet due to the repeated use of the image for steganography, which has resulted in a lot of attacks including graphical attacks and statistical attacks using steganalysis [19]. Nonetheless, a number of steps and novel methods are always brought forward by researchers to deal with most of these assaults.

The process of sending data over an untrusted medium, such as the Internet, so that the content cannot viewed by a third party is known as cryptography. Cryptography is often thought to be encryption; although the two words have been used interchangeably, they are not the same. According to [20], cryptography is the process and study of secure data communication techniques in the presence of third parties without their awareness. The role of cryptography in data communication can never be underestimated.

Furht et al.,asserts that the concept of cryptography is very much linked to the principles of cryptology and cryptanalysis [21]. Cryptology as a process involves cryptanalysis and cryptography. The principle of safe and confidential data retention can be referred to as cryptography. According to [22], any method for developing a system designed to deliver some hidden message is known as cryptanalysis. Cryptanalysis in cryptography is analogous to steganalysis in steganography — one is an assault on the other.

Contemporarily, encryption is the key element of cryptography and is the conversion of text to a non-readable form or format called a cipher [23].

Encryption, using keys to encode plain text and decode a cipher is the simplest way to achieve cryptographic data security. There are four key objectives that cryptography is always aiming to achieve and they are data integrity, data confidentiality, data authentication and non-repudiation of data. Confidentiality simply implies that no one should be able to read a document except the intended receiver. [24]Suggests that verification as an impartial consideration is to guarantee that the sender or source of the message is authorized and verifiable. According to [25], data integrity is concerned with preventing unauthorized alteration of a message that is intended to mutilate or distort data with malicious intent or by mishap. Any receiver of a message must be able to check if the transmitted message has been modified along the communication route.

Like the heuristic principle of artificial intelligence, non-repudiation is a cryptographic targeting mechanism that establishes the identity of the sender of a message in order to prevent the potential rejection of the same sender[24]. The four goals governing the power of cryptography remain the core of cryptographic algorithms. It is therefore essential to ensure that these objectives have been achieved at all times.

III. PROPOSED ALGORITHM

The proposed algorithm utilizes two layers of security to maintain the privacy, confidentiality and accuracy of the data. Fig. 1 however indicates the framework for the overall process of the system. This system only hides the encrypted Message ID inside the image but saves the actual message in a secured database as well as, retrieve the data from the stego image when there is a match on the recipient side.

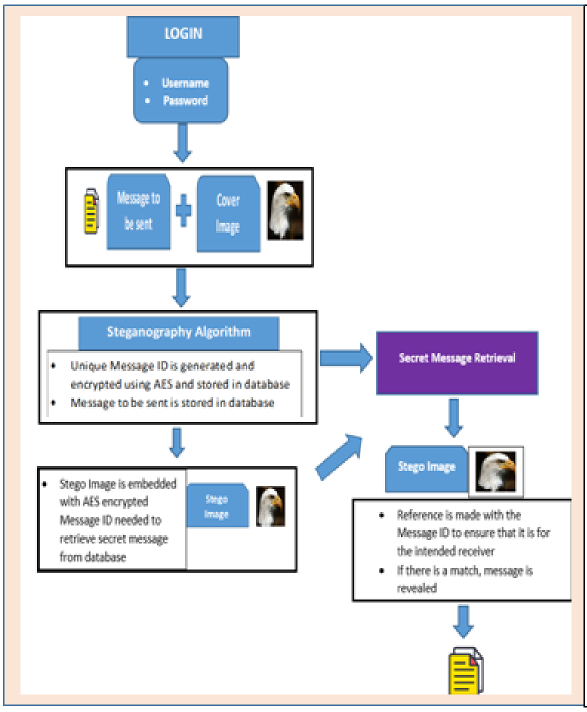
From Fig. 1, from hiding and retrieving the data, a username and password are required prior to using the system. Once the user has been able to log in into the system, the user can insert a message inside the chosen image as well as select an intended recipient. Using the steganography algorithm, the data will be saved to the secured database, and, embedded inside the image will be a unique Message ID (encrypted with AES) attached and saved as the stego image. The stego image generated will be with almost zero distortion of the original image.

For retrieving the data, the Message ID embedded inside the image needs to match with the User ID of the recipient in the database. If the Message ID doesn't match, the data can never be retrieved from the database. This is to ensure the integrity and confidentiality of the data.

For the steganography algorithm, Fig. 2 shows the algorithm for embedding the Message ID inside the image. During the process of embedding the encrypted Message ID inside the image and saving the message to the database, the Message ID generated is also needed for the purpose of retrieving the message back from the database.

From Fig. 2, the secret message that is extracted from the system is transferred to the database and then the text file is compressed into a zip file. The purpose of saving the text file to a database separately is because the database is more secured as compared with sending the message with the image file. The contents in the stego image will significantly be useless since it will only contain the encrypted Message ID which will serve no purpose if you are not the intended recipient thus making the message impossible to be detected and read.

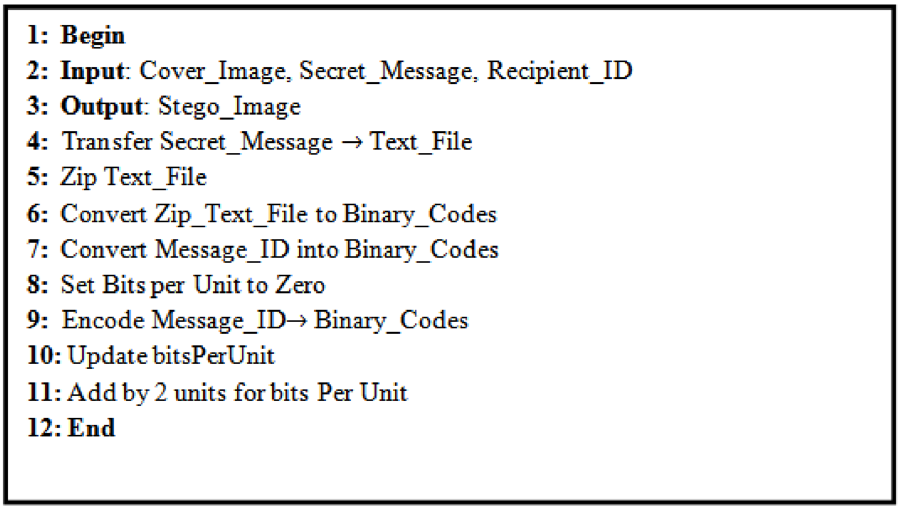
The encryptedMessage ID inthisproposedsteganographyalgorithmisplayinganessential role wherethekeyactsasalocker usedtolock or unlockthesecret message


LOGIN
Username
Password
Message to be sent
Cover Image
Steganography Algorithm
Unique Message ID is generated and encrypted using AES and stored in database
Message to be sent is stored in database
Secret Message Retrieval
Stego Image is embedded with AES encrypted Message ID needed to retrieve secret message from database
Stego Image
Stego Image
Reference is made with the Message ID to ensure that it is for the intended receiver
If there is a match, message is revealed

```
Input: Secret_Message(SM), threshold T,
Image K, cryptographic key Ke
Output: encrypted data Ie

1: R=readData(SM)
2: Z=ZipCompressR
3: CT=AES.encrypt(Z,Ke)
4: Row,Col =ReadImage(K)
5: Iei=InitilizeArray Row,Col
6: for(i=1;i≤Row;i++)
    a. POP=[Row,Col]
    b. Selindex=Rowi*T
   c. POP=Resize(Row−Rowi)
    d. Sel2index=Rowi*T
    e. POP=Resize(Row−Rowi)
   f.SEQ=CrossOver (Selindex, Sel2index)
    g. SelPixel =IsLowIntensity (SEQ 2)
    h. Iei=EmbedData (SelPixel, CT,SEQ 2)
7: end for
8: return Ie
```

Figure 1:Proposed framework and algorithm of the HideMe system.

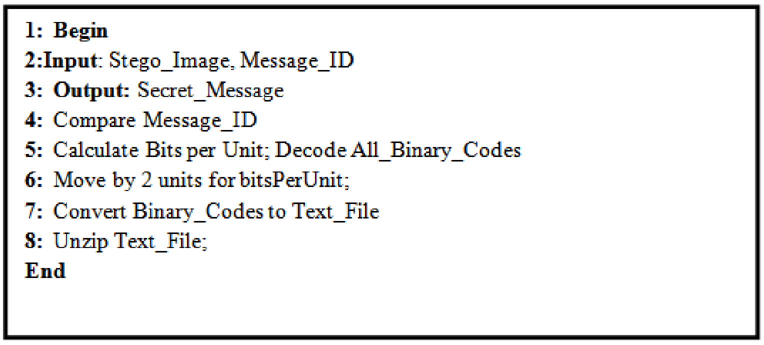


```
Begin
Input: Cover_Image, Secret_Message, Recipient_ID
Output: Stego_Image
Transfer Secret_Message → Text_File
Zip Text_File
Convert Zip_Text_File to Binary_Codes
Convert Message_ID into Binary_Codes
Set Bits per Unit to Zero
Encode Message_ID→ Binary_Codes
Update bitsPerUnit
Add by 2 units for bits Per Unit
End
```

Figure 2: Algorithm for embedding Message ID inside image

Once the Message ID is hidden inside the image, this key can be extracted back from the stego image to reveal the message. Fig. 3 shows the algorithm for extracting the Message ID from the stego image. In order to retrieve a correct message, the Message ID is needed for the purpose of verification.

From Fig.3, forthedataextractingmethod, aMessage IDis neededtodetectwhether the keymatches with thekey thatdecodesfromtheseriesof binarycode. Oncethekey ismatched, theprocesscontinuesby formingthe binary codetoa zipped textfile, unzipthe textfileandtransferthesecretmessagefrom thedatabasetoretrieve the original secretmessage.



```
Begin
Input: Stego_Image, Message_ID
Output: Secret_Message
Compare Message_ID
Calculate Bits per Unit; Decode All_Binary_Codes
Move by 2 units for bitsPerUnit;
Convert Binary_Codes to Text_File
Unzip Text_File;
End
```

Figure 3: Algorithm for extracting data from stego image

Themain objective of this proposedsteganography algorithmistheuseoftransferring thesecretmessageto a secured database file, zipping thefile, aUser key, convertingbothzippedfile and key into aseriesofbinarycodes,andtheuse of encoding each last two binary codes into pixels inimage. Theimagequality isstillrobustwherethe distortion and colorchangesofimagesarereduced to theminimumorzero-distortion. Secretmessage,onthe other hand, isdifficult to bestolen by steganalysis as it securely kept in a database

Theproposedsteganographyalgorithm consistsof two image embedding techniques which are data hiding methodanddataretrievingmethod. Datahidingmethod is usedto hide the encrypted Message ID in the cover image while data retrievingmethod usesthe Message ID to retrieve the hiddensecretmessage from the database. Hence, dataor inparticular a secretmessage, isprotectedwithoutrevealingto any unauthorized party. Figures 2 and 3 show that 2 layers of security are conserved within the system. However, the Message ID is used for verification process in order to retrieve the correct message back from the database. This Message ID is also embedded inside the image. Therefore, when a user is transmitting the image via the internet, that image contains only the embedded secret User key. However, the data can only be retrieved using the system.

IV. EXPERIMENTS AND ANALYSIS

A simple system that implements the proposed algorithm is built and based on the structure for the system as seen in Fig. 1, it is founded on 2 layers of security. The first layer is intended for login and the second layer is for the hiding and retrieving the secret message. A system of this kind is implemented in [12] but that is for Windows whiles the proposed system is built on the Android platform. From figure 4, the home interface of the proposed system can be seen.

4.1 Application of the proposed technique

From Fig. 4, HideMe has three main boxes: the first textbox is for the address of the intended recipient of the message, the image box is used for getting the image from any location and the text box is used for hiding and retrieving the message to and from image respectively. In order to hide the data inside the image, a Message ID is generated, encrypted (AES) for the purpose of security. Fig. 5 shows the interface for the Message ID which is encrypted using AES.

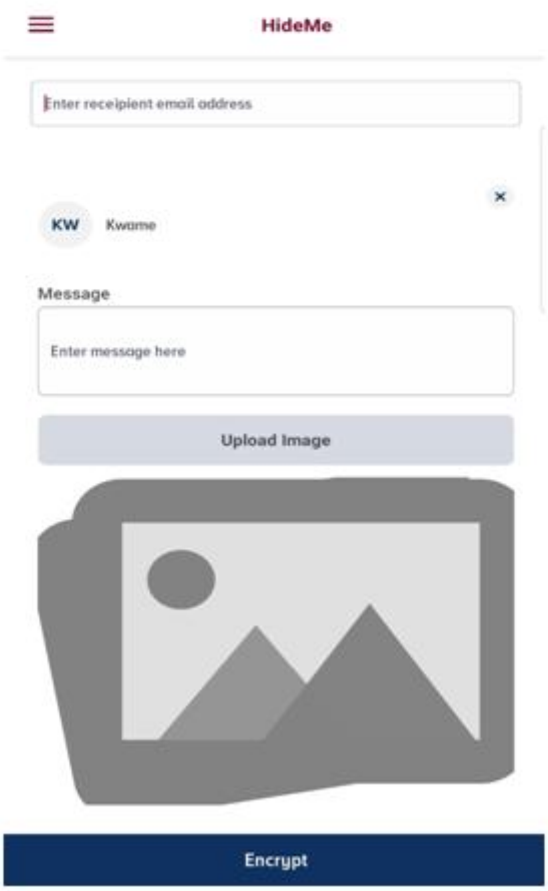
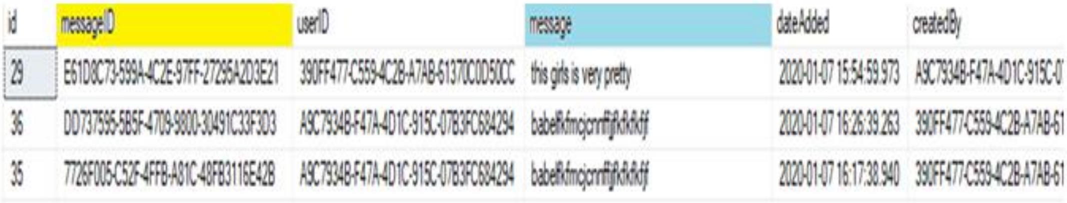


Figure 4: The main interface for HideMe

From Fig. 5, there is no need enter the Message ID as it as has already been generated for the verification purpose. This Message ID is also embedded inside the image but is also stored in the database together with the message. So when the intended recipient receives the image and there is a match, he or she can then read the message. This new stego image can then be then be sent to the recipient via the internet without hackers having access to it.

If the intended recipient wants to reveal the secret message concealed in the image, the new stego image file must be then be uploaded again using the system to check from the database if the Message ID matches with that in the database to retrieve the data. The system is tested using the images as showed in Figures 6-7



id	messageID	userID	message	dateAdded	createdBy
29	E61D8C73-599A-4C2E-97FF-27295A2D3E21	390FF477-C559-4C2B-A7AB-61370C0D50CC	this girls is very pretty	2020-01-07 15:54:59.973	A9C7934B-F47A-4D1C-915C-0
36	DD737595-5B5F-4709-9800-30491C33F303	A9C7934B-F47A-4D1C-915C-07B3FC684294	babelfkfmojcnnffjfkfkfkdf	2020-01-07 16:26:39.263	390FF477-C559-4C2B-A7AB-61
35	7726F005-C52F-4FFB-A81C-48FB3116E42B	A9C7934B-F47A-4D1C-915C-07B3FC684294	babelfkfmojcnnffjfkfkfkdf	2020-01-07 16:17:38.940	390FF477-C559-4C2B-A7AB-61

Figure 5: Database showing the Message ID and Message

4.2 Comparative Analysis

Figures 6(a) and 7(a) shows the original image before it is passed through the system whiles the figures 6(b) and 7(b) indicates the stego image after the Message ID is embedded in the cover image. It was however noticed that the stego images do not have a noticeable distortion as can be seen by the naked eyes although the file size of the stego images are slightly higher than the cover image.

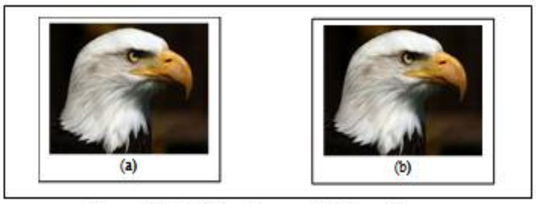


Figure 6(a) Original image (b) Stego image

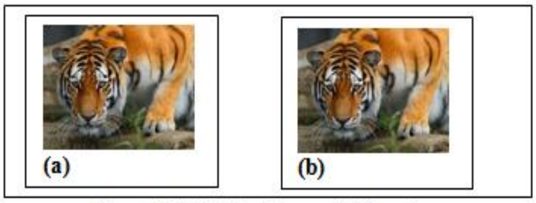


Figure 7 (a) Original image (b) Stego image

Space complexity is a measure of the quantity of working storage (main memory) an algorithm requires. That means how much memory, in the worst case, is needed at any point in the algorithm. Encryption Space Complexity of an algorithm is total amount of space consumed by the algorithm to encrypt the file with respect to the input size. Space complexity take in both Auxiliary space and space used by input file[26]. The space complexity of the proposed system is given using figure 8. In order to demonstrate the performance of proposed algorithm the X-axis illustrates the different experiments performed with the system (file size in KB) and the Y-axis contains the memory consumption of the system in terms of KB. According to the obtained results the performance of the proposed algorithm is found efficient.

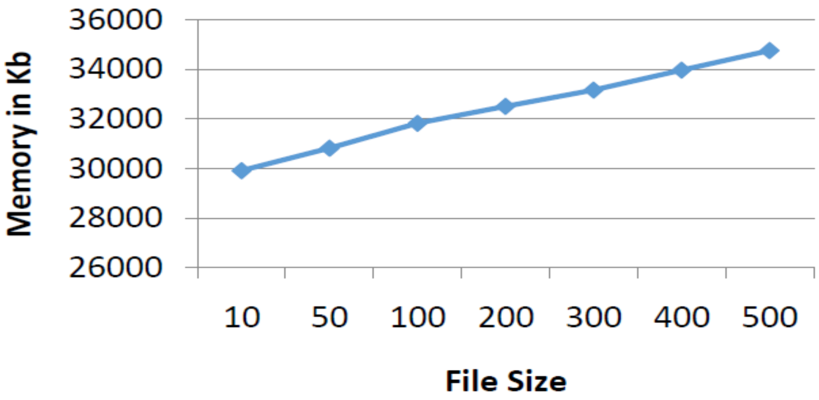


Figure 8: Encryption Space Complexity

4.3 Experimental Results

The algorithm was then tested using the PSNR (Peak signal-to-noise ratio). PSNR is a standard measurement used in steganography technique in order to test the quality of the stego images. The higher the value of PSNR, the more quality the stego image will have.

Let the cover image be C of size M × M and the stego image is S of size N × N, then each cover image C and stego image S will have pixel value (x, y) from 0 to M-1 and 0 to N-1 respectively. The PSNR is then calculatedas follows:

Take

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}}\right)$$

$$=20.\log_{10}\left(\frac{\mathrm{MAX}_1}{\sqrt{\mathrm{MSE}}}\right)\textbf{(1)}$$

$$=20.\log_{10}(\mathrm{MAX}_1) - 10.\log_{10}(\mathrm{MSE})$$

MSE is the Mean Square Error which is the measure to determine the distortion between the original and the stego image. MSE is calculated using:

Where

$$\mathrm{MSE} = \frac{1}{\mathrm{MN}}\sum_{x=0}^{M-1}\sum_{x=0}^{M-1}(C(x,y) - S(x,y))^2 \qquad \textbf{(2)}$$

Where M and N are the Height and Width of the image respectively. The minimum image pixel for width is at least 150 while the minimum image pixel for height is at least 112.
However, note that MAX is the maximum possible pixel value of the images. For example, if the pixels are represented using 8 bits per sample, then the MAX value will be 255.
If the stego image has a higher PSNR value, then the stego image has more quality image.

From table 1 the If the stego image has a higher PSNR value, then the stego image has more quality image. Table 1 shows the
PSNR value for two stego images in Figures 6 and 7. The PSNR is calculated using the equation of PSNR in Eq. (1).Based on values of PSNR from Table 1, the PSNR values show that the stego images have quality imageswithout compromising of the original image. Table 2 shows the results from the Mean Square Error (MSE) of the Cover and Stego Image in Figure 6

Table 1: The PSNR value of stego images.

Image	Reference	PSNR for 6389Bytes embedded inside the image
Eagle	Figure 6 (a): Stego Image (1)	57.143
Tiger	Figure 7 (a): Stego Image (2)	53.983

Table 2: Results from the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) of the Cover and Stego Image

CoverImage	StegoImage	Sizeof Embedded Data	MeanSquare Error (MSE)/%	Sizeof Extracted
Eagle (Figure 6a)	Eagle (Figure 6b)	6389 Bytes	0.125517	6389 Bytes
Tiger(Figure 7a)	Tiger(Figure 7b)	6389 Bytes	0.259832	6389 Bytes

Table 3: Image parameters for Cover and Stego image

Pre-Steganography				Post-Steganography			
Image	Mean	Standard Deviation	Entropy	Image	Mean	Deviation	Entropy
Eagle (Figure 6a)	142.9557	54.7812	7.6939	Eagle (Figure 6a)	142.9557	54.7812	7.6939

V. CONCLUSION

This paper proposed a new steganography algorithm with 2 layers of security. A system named HideMe has been developed using the proposed algorithm. We tested few images with various sizes of data to be hidden. With the proposed algorithm, we found that the stego image does not have a noticeable distortion on it (as seen by the naked eyes). We also tested our stego images using PSNR value. Based on the PSNR value of each images, the stego image has a higher PSNR value. Hence this new steganography algorithm is very efficient to hide the data inside the image. HideMe can be used by various users who want to hide the data inside the image without revealing the data to other parties. HideMe maintains privacy, confidentiality and accuracy of the data.

REFERENCES

[1]. Dengre, A., A. Gawande, and A. Deshmukh, Effect of Audio Steganography based on LSB insertion with Image Watermarking using AVI video. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2013. **2**(6): p. 2319-4847.

[2]. Chen, M., N. Memon, and E.K. Wong, Data hiding in document images, in Multimedia Technologies: Concepts, Methodologies, Tools, and Applications. 2008, Igi Global. p. 291-304.

[3]. Odeh, A. and K. Elleithy, Steganography in arabic text using zero width and kashidha letters. International Journal of Computer Science & Information Technology, 2012. **4**(3): p. 1.

[4]. Lou, D.-C., J.-L. Liu, and H.-K. Tso, Evolution of Information-Hiding Technology, in Information Security and Ethics: Concepts, Methodologies, Tools, and Applications. 2008, IGI Global. p. 144-154.

[5]. Schneider, Secrets &Lies, Indiana:Wiley Publishing,2000.

[6]. Cole, E., Hiding in plain sight. 2002: Wiley.

[7]. Mathe, R., V. Atukuri, and S.K. Devireddy, Securing information: cryptography and steganography. International Journal of Computer Science and Information Technologies, 2012. **3**(3): p. 4251-4255.

[8]. Apau, R., Enhancing Data Security using Video Steganography, RSA and Huffman Code Algorithms with LSB Insertion. 2017.

[9]. Eltyeb, E. and A. bed Elgabar, Comparison of LSB Steganography in BMP and JPEG Images. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2013: p. 2231-2307.

[10]. Morkel, T., J.H. Eloff, and M.S. Olivier. An overview of image steganography. in ISSA. 2005.

[11]. Jahnke, T. and J. Seitz, An introduction in digital watermarking: Applications, principles, and problems, in E-Commerce and M-Commerce Technologies. 2004, IGI Global. p. 117-141.

[12]. Ibrahim, R. and T.S. Kuan, Steganography algorithm to hide secret message inside an image. arXiv preprint arXiv:1112.2809, 2011.

[13]. El-Emam, N.N., Hiding a large amount of data with high security using steganography algorithm. Journal of Computer Science, 2007. **3**(4): p. 223-232.

[14]. Chen, P.-Y. and W.-E. Wu, A modified side match scheme for image steganography. International Journal of Applied Science and Engineering, 2009. **7**(1): p. 53-60.

[15]. Chang, C.-C. and H.-W. Tseng, A steganographic method for digital images using side match. Pattern Recognition Letters, 2004. **25**(12): p. 1431-1437.

[16]. Wu, D.-C. and W.-H. Tsai, A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 2003. **24**(9-10): p. 1613-1626.

[17]. Li, M., W. Lou, and K. Ren, Data security and privacy in wireless body area networks. IEEE Wireless communications, 2010. **17**(1): p. 51-58.

[18]. Al-Ataby, A. and F. Al-Naima, A modified high capacity image steganography technique based on wavelet transform. changes, 2008. **4**: p. 6.

[19]. Bateman, P. and H.G. Schaathun, Image steganography and steganalysis. Department Of Computing, Faculty of Engineering and Physical Sciences, University of Surrey, Guildford, Surrey, United Kingdom, 4th August, 2008.

[20]. Kundalakesi, M., Sharmathi. R, Akshaya. R (2015) Overview of Modern Cryptography. International Journal of Computer Science and Information Technologies (IJCSIT). **6**(1): p. 350-353.

[21]. Furht, B., E. Muharemagic, and D. Socek, An Overview of Modern Cryptography. Multimedia Encryption and Watermarking, 2005: p. 31-51.

[22]. Katz, J. and Y. Lindell, Introduction to modern cryptography. 2014: Chapman and Hall/CRC.

[23]. Natarajan, S., M. Ganesan, and K. Ganesan, A novel approach for data security enhancement using multi level encryption scheme. Research paper, IJCSIT, 2011. **2**(1): p. 469-473.

[24]. Delfs, H., H. Knebl, and H. Knebl, Introduction to cryptography. Vol. 2. 2002: Springer.

[25]. Garg, N. and P. Yadav, Comparison of asymmetric algorithms in cryptography. Journal of Computer Science and Mobile Computing (IJCSMC), 2014. **3**(4): p. 1190-1196.

[26]. Sethi, P. and V. Kapoor, A Secured System for Information Hiding in Image Steganography using Genetic Algorithm and Cryptography. International Journal of Computer Applications, 2016. **975**: p. 8887.