PROPOSING DOUBLE ENCRYPTION DOUBLE COVER [DEDC] INNOVATIVE MODEL FOR SECURE COMMUNICATION USING STEGANOGRAPHY

Dr. Amit Chaturvedi[#1], Parvaiz Ahmad Bhat[*2]

*Engineering College, Ajmer[#1], M.Phil (IT) Student,Bhagwant Univ., Ajmer[*2]*
amit0581@gmail.com[#1]

Abstract: *Steganography provides the facility to hide the secret message inside a cover object and that cover may be an image, or audio file. Encryption algorithm plays an important role for the security of the message. So, we have used AES-128 encryption algorithm in our proposal. During the survey of literature related to steganography we found that generally single cover is used. So, In this proposal of DEDC, we introduced the concept of Double Encryption Double Cover]. This increases the complexity for the attacker as well as security of the message. Besides this we use the concept of Least Significant Bit (LSB) plane for the first cover. With this we can confuse the attacker that the message is in the text form or hidden in the form of LSB plane. Hence, DEDC is a good method for transferring the secret message using steganography.*

Keywords: **Steganography, Steganalysis, AES, cryptography, encryption, decryption, secret key, LSB image.**

1. INTRODUCTION

Steganography provides a secure mechanism for transferring messages over the common communication channels without any doubt from the upper side that there is any hidden message inside the cover. Securing message is a two-step procedure in the steganography, at the first step message is encrypted using any encryption algorithm and then placing the encrypted message inside a cover. Steganographic message often appears to be something else than the original (secret) message, like a picture, sound, larger text, etc. Steganography provides a secure method for communication, but various steganalysis tools, also provides the facility to unhide the concealed message from the given cover. In this thesis work, we have presented the various proposals for improving the steganography or way of concealing the message inside the cover and steganalysis methods.

2. AES (Advanced Encryption Standard) Encryption Algorithm

There are two types of encryption standards used for converting plaintext into cipher-text. One is the symmetric key encryption method and another is the asymmetric key encryption method. In the symmetric key encryption method, a symmetric key i.e. same key for encryption and decryption is used. Whereas in the asymmetric key method, two different keys called as private and public keys are used for encryption and decryption respectively. Private key is kept safe with user who does the encryption and public key is distributed to all the recipient of the cipher-text. When asymmetric key is used a lot of computational power have to be done. But if symmetric key is used comparatively less computational power is required and results proves that process with the application of symmetric key are around 1000 times faster than the processes with the applications of asymmetric key. And because they are faster, symmetric ciphers are much more useful for bulk encrypting large amounts of data.

AES is a symmetric key encryption standard i.e. it uses same key for encryption and decryption of the plaintext into cipher-text and vice-versa. It is an open standard that is free to use for any public, private, commercial, or non-commercial use. The AES encryption algorithm encrypts and decrypts data in blocks of 128 bits. It can do this using 128-bit, 192-bit, or 256-bit keys. AES using 128-bit keys is often referred to as AES-128, and so on. AES-128 key is very secure as it requires around one billion billion (one quintillion) years to break it with world's fastest supercomputers.

As discussed above the AES algorithm has three different key lengths and the main difference among these are the number of rounds that the data goes through in the encryption process, 10, 12 and 14 respectively. Hence, if we compare them on security margins then 192-bit and 256-bit provide a greater security margin than 128-bit. As far as AES is concerned for our work, 128-bit AES is enough and also for most practical purposes.

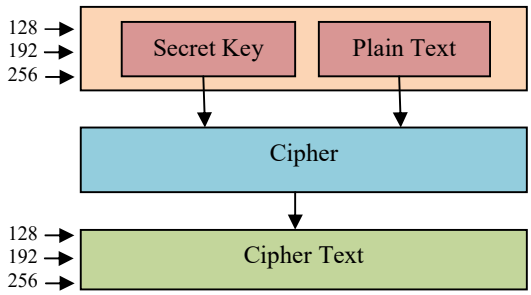


Figure 1: Design of AES encryption process

3. Proposed Model and Methodology

In this research work, we have focused on the steganography methods and propose an innovative model called as "DEDC [Double Encryption Double Cover] model" for hiding the message. In the DEDC model, the concept of double encryption and double cover is introduced that is more secure and it is an innovative model for steganography. Our model performs this task in four phases. In the first phase, a picture (either the JPG, JPEG, PNG), say "cover1.jpg" taken to generate a LSB plane and the algorithm "create_lsb()" produces LSB plane or LSB image of the given picture say "LSB_cover1.jpg".

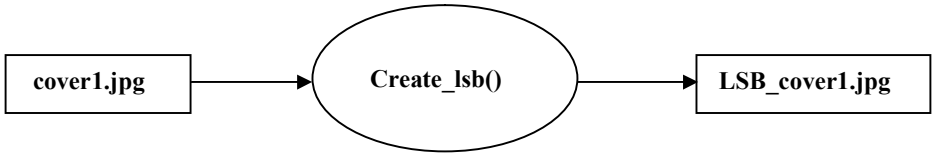


Figure 2: Phase-1 of DEDC model

There are various encryption algorithms available to encrypt the message and among these we have used AES128 for this encryption purpose. Now, in the second phase a message file (text file like "message1.docx") is taken that is to be hide and then convert this message.docx file into encrypted form using AES-128 encryption method and the encrypted message is saved with encrypted_message.docx.

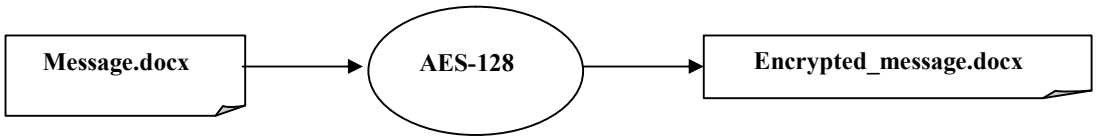


Figure 3: Phase-2 of DEDC model

In the third phase, the encrypted message file i.e. encrypted_message.docx will be hided within the previously generated LSB images (or LSB plane) as cover i.e. in the "LSB_cover1.jpg" file using the tool and then produces an output file that is also an LSB image file, say "Output1.jpg".

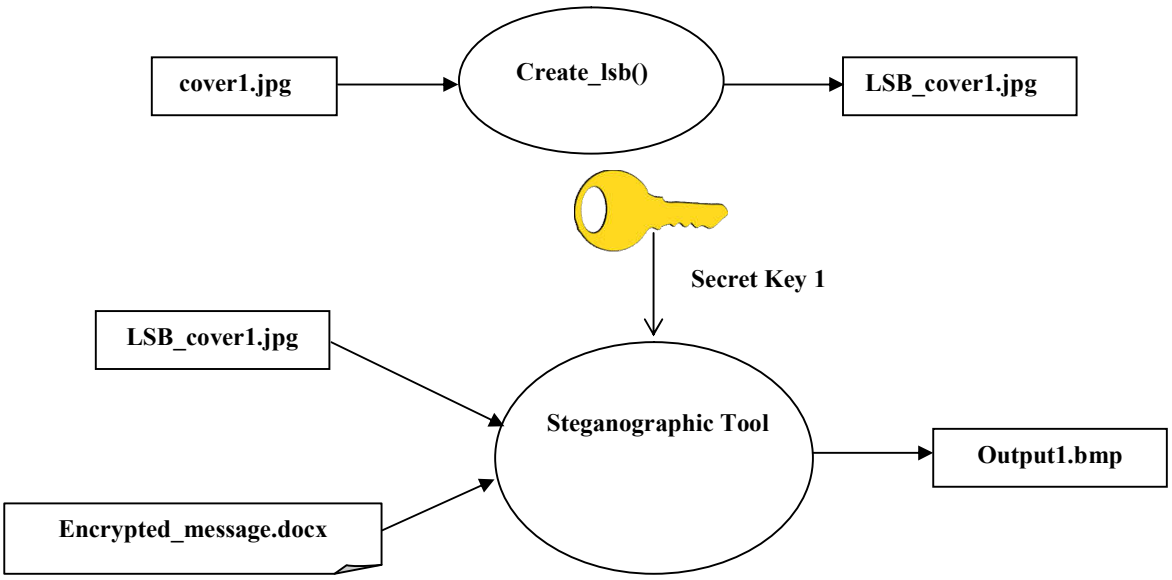
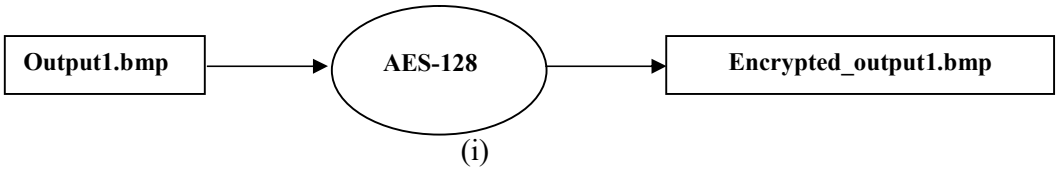
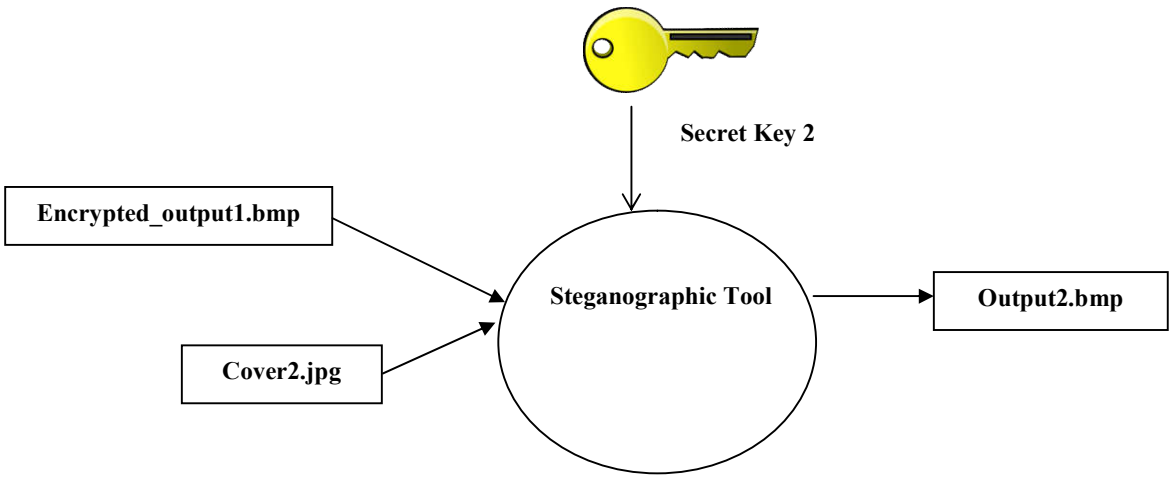


Figure 4: Phase-3 of DEDC model

In the fourth phase, this output1.bmp file is used as the message file and applying the AES128 algorithm to encrypt it again say Encrypted_output1.bmp and taking another image cover i.e. cover2.jpg file. This cover2.jpg image file is a simple jpg image file. We don't change its type as LSB or any other, because we have to send it through the communication channel. As we have to hide the output1.bmp image data into it so we don't change the outer most cover image. Using the steganographic tool, the final output file i.e. ouput2.bmp is generated by hiding ouput1.bmp message file in the second cover i.e. cover2.jpg. This ouput2.bmp is the final file to be send using the communication channel and it is more secure than before used methods for steganography.



(i)



(ii)

Figure 5: Phase-4 of DEDC model

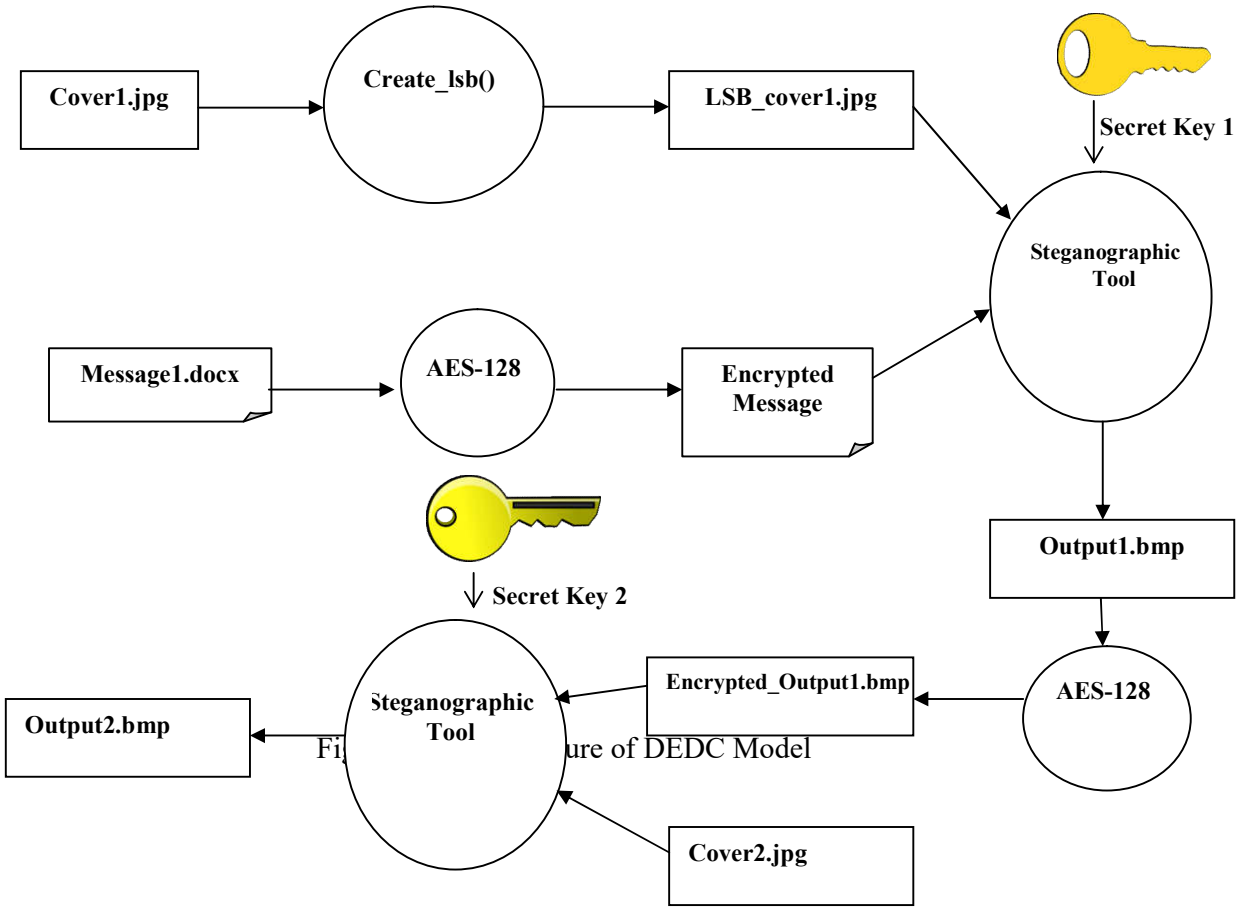


Figure 6: Basic Structure of DEDC Model

Algorithm of the create_lsb()

Step 1: Read the input JPG file as cover1 into a variable c2.
Step 2: convert the image data stored in variable c as double data type and store this value to a variable cd2.
Step 3: take the floor value of cd/2 and then take mod with precision 2 to create LSB image or plane of the input jpg file and store it into a variable co.
Step 4: Save this LSB image that is stored in the variable co at an appropriate location.
Step 5: Show the LSB image or LSB plane of the input colored image

How to obtain the hidden message under the cover?

As we have seen above, there are four phases in the DEDC model to hide the secret message inside the double cover. Now we will understand the steps to open the hidden message that is hidden in the double cover.
Let us assume that the final image i.e. output2.bmp has been received at the receivers end and the receiver have both the secret keys i.e. secret key 1 and the secret key 2. Then the process to obtain the hidden message will be complete in two phases. In the first step, output2.bmp image file is to be supplied as an input image and secret key-2 supplied with it in the steganographic tool. This tool separates the cover and hidden image. This hidden image is the LSB image with the hidden message.

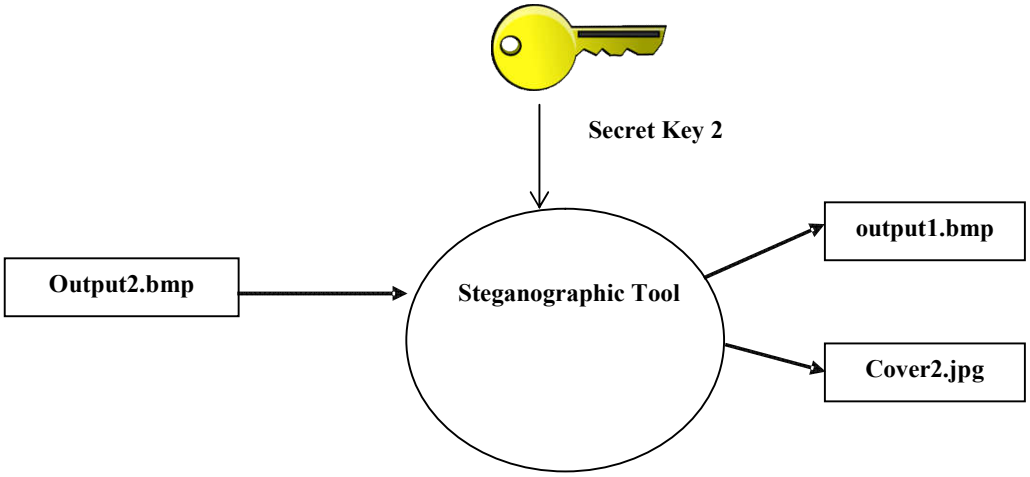


Figure 7: Step-1 for obtaining hidden LSB image under cover2.jpg

In the second step, obtained output1.bmp image is used as input file in the steganographic tool with the secret key-1 and this will again separate the LSB_cover1.jpg file and message1.docx file.

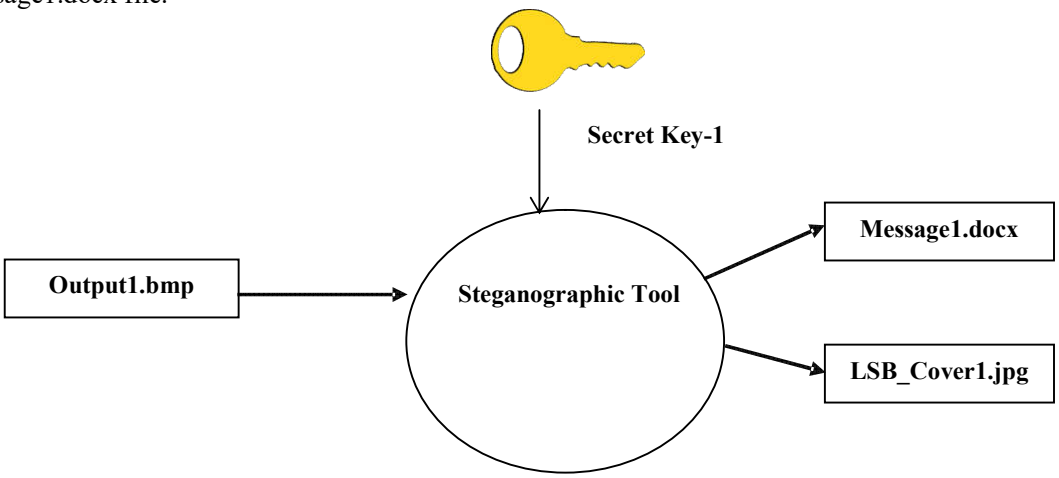


Figure 8: Step-2 for obtaining hidden message under LSB_cover1.jpg

In this whole procedure, the noticeable point is the application of LSB image as cover. When any one unauthorized person receives the output2.bmp image and assumes that there is any hidden message then first it has to use the correct steganographic tool, which also requires to select, the correct encryption/decryption algorithm as we have used AES-128. This encryption/ decryption algorithm also requires correct password or secret key. It is hard to find the secret key-2 and cracking the secret required lot of computation. If any how the unauthorised receiver cracks the first security key i.e. secret key-2. There is another security key i.e. secret key-1 that is different from the secret key-2. Hence, we can say that our proposed model DEDC [Double Encryption Double Cover] introduced innovative concept of double cover along with converting the first cover into LSB image and then using it as cover1. This proposed model DEDC uses two secret keys with encryption/decryption standard AES-128, which increases its complexity in multiples and it is very hard to crack it. So, it is a secure steganographic model to send secret message one user to another user over the common communication channel.

4. Implementation of the DEDC Model

Let us understand the implementation of DEDC model through the use of actual data. We have now taken an JPG image as input image as the first cover file. Here the file is passport.jpg of 64KB as shown below in the figure 9. By taking this passport.jpg file as input cover1, the LSB plane or LSB image of this image is created by using the above mentioned create_LSB( ) function and named it as passport_LSB.jpg as shown in figure 10..



Figure 9: passport.jpg

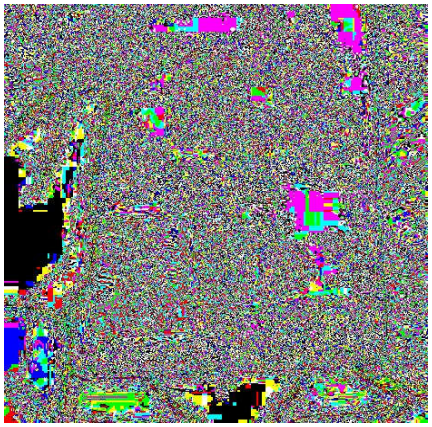


Figure 10: passport_lsb.jpg

Let there is a message file “message.docx”, which contains a message text inside it of about 12KB of data.

Kashmir is the northernmost geographical region of the indian subcontinent. Until the mid-19th century,the term ‘kashmir’denoted only the Kashmir valley between the great Himalayas and the pir panjal range.Today,it denotes a larger area that includes the indian administered territories of jammu and Kashmir and ladakh, the Pakistani administered territories of Azad Kashmir and gilgit Baltistan,and Chinese administered territories of aksai chin and the trans karakoram.

Figure 11: message.docx

This text message will then be encrypted with AES-128 encryption scheme with an encryption key defined by the user. This text message will be show below:

aj09cpJ9m1zgcDzCntScfAfqVv6lmKaaJcsR9ilhExgDFc84f04xzwdO8zulVnCXx
EMLIJQ2BlEdrPO81AMmp//XhQt3HPSXnG8z44Feo0Ys/CUp1o9JR6H3VA2xE
ThIxIIRwLvJ+5BnzSRqva6d6Te4TvPcUm0h5Qxwcu1GGsR+N8kzY5F4FjpPGF
NQIE2Z5VVp8yiQxSFXZLv+898meEQK1Weed/eES+tW/CTbZVTYEoFAKi+k
uHHW6atXWuHXjY4R0SBGpWceYiI/JsXWqegqxP4LKzYYbseqQRFsQv2kW
DCD5IiHhhfYyX4C6zYk0Dz42P+Tu+GJYi7AJv9W+4CjX23Mxn6czBKnMb9b
RhzwisvW39Cl2JbEhN5f/UK8NDb3h5sm3Q5L95koWhrLw7TDPpGrYN2vQlh+
d/HFJsl6vvEs84Jm2yorcVvEmgojLYo4/EBobs6dHJq0LLao1Px0MGvhCbtGCG
MlEzgTYwnKE+pJG8LBJoYc2US3MhrKHauB3ILujnUPQPCgfxxG07sdYkhyd
Hcjdw9WCU2chYiLwyQIoCrPYQTPqTIP/i9RHmBDBSq3MRk8jHuWODKYd1
//oJOXsGN89OA6BF8uJ1OiJm0PdCmtpeEGbCBffirjHgki/mfZae2PLEqUdwlpT

Figure : encrypted_message.docx

When this encrypted message is hided within the LSB image i.e. passport_lsb.jpg using steganographic tool it gives an .bmp file as output and we named it as output1.bmp. This

output1.bmp file contains passport_lsb.jpg as an image cover for the encrypted message contained in the encrypted_message.docx. The size of this output1.bmp file is 664 KB.

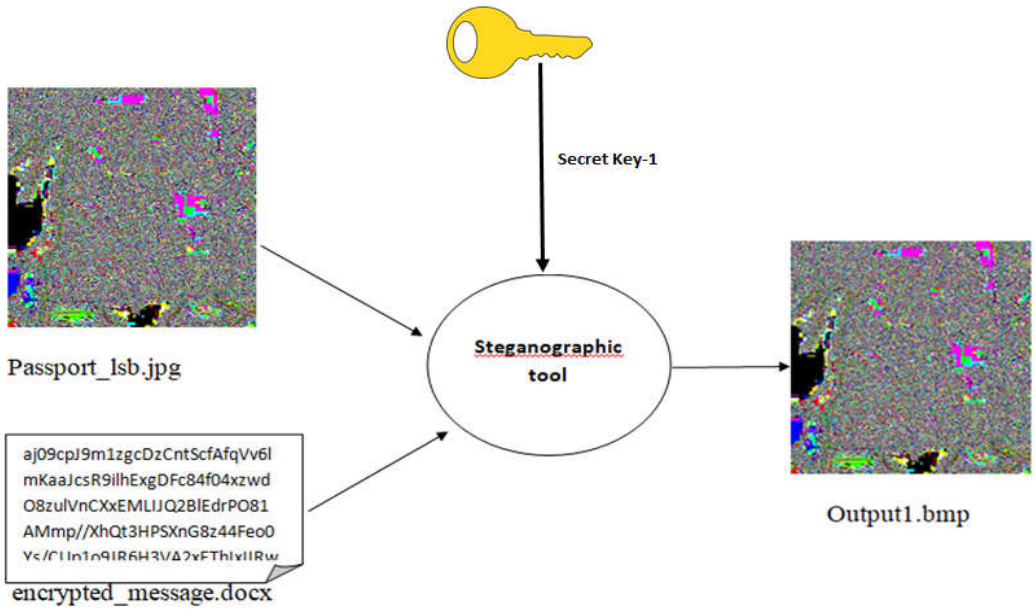


Figure : Illustration of phase 3 of DEDC model

Now this output1.bmp file is used as the message file and will be encrypted using AES-128 encryption technique and the outcome will be called as encrypted_output1.bmp. In the next phase, this message file i.e. encrypted_output1.bmp file will be hided in another image cover file cove2.jpg using a steganographic tool. The final outcome of this phase is final image with the encrypted message and ready to be sent over the communication channel.

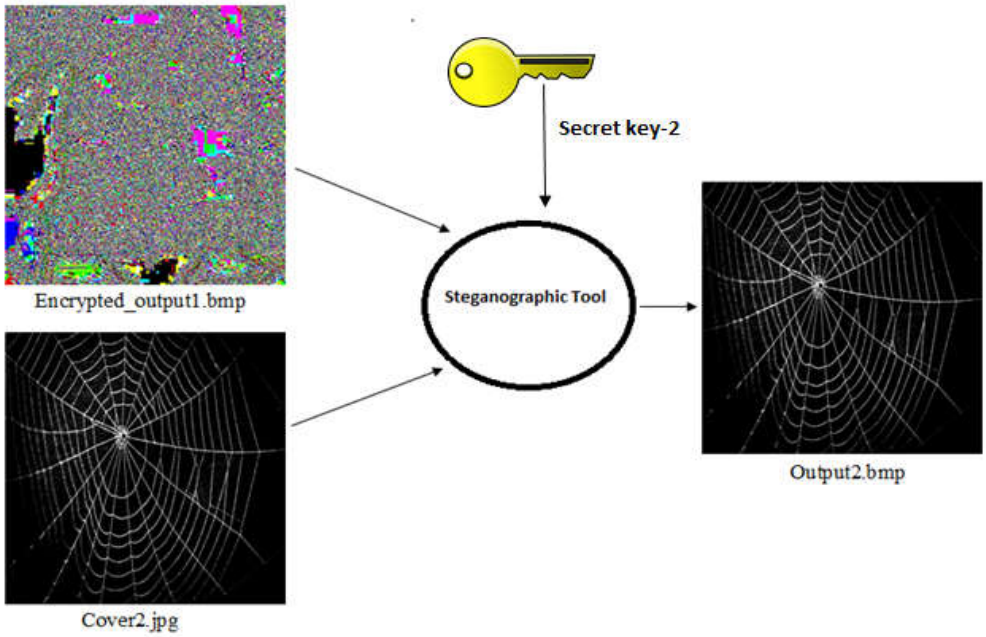


Figure : Illustration of phase 4 of DEDC model

There is the two step procedure to reveal the hidden message in the DEDC model. These two steps are illustrated below in the perspective of the above given example.

Step 1: Let the receiver receives the final image i.e. output2.bmp and the receiver have the secret key-2. Now if the receiver has the correct steganographic tool, it will input the output2.bmp as well as secret key-2 to reveal the hidden LSB image under the cover2.jpg file. This process is illustrated in the below given example.

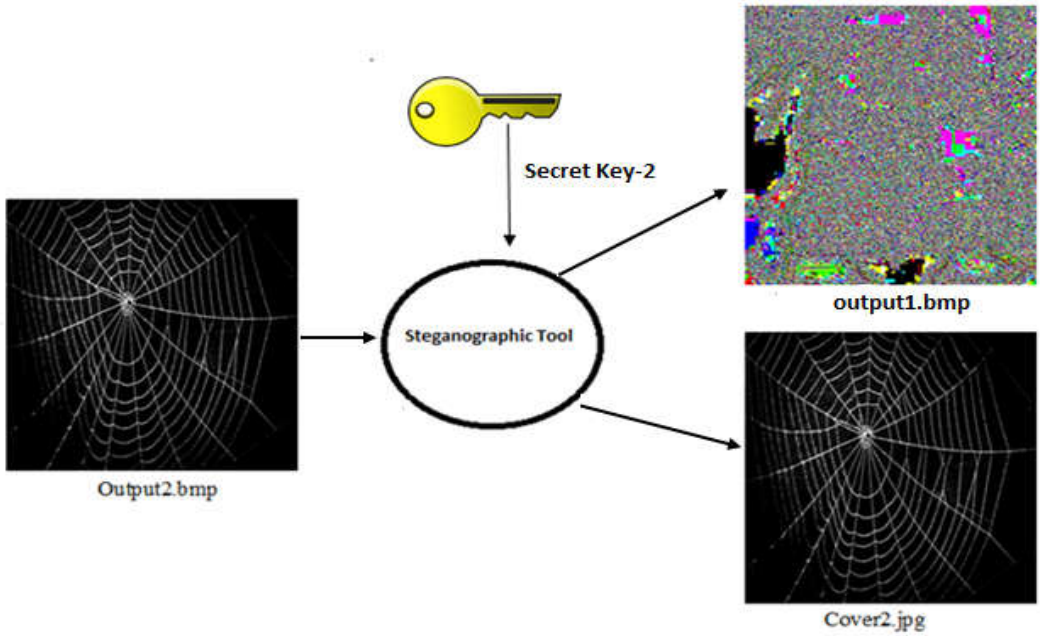


Figure : Step 1 of revealing process of hidden image in DEDC model

As shown above in the figure that when output2.bmp image and secret key-2 is supplied to the steganographic tool. Then the steganographic tool will separate the cover2.jpg and the hidden file output1.bmp. If the receiver is not authorised, it will consider the output1.bmp as the final message file and engaged to obtain the message from it and it is not possible at this stage. Hence, secret message is safe.

Step 2: The output1.bmp is the hidden file under the cover2.jpg. Now this output1.bmp file is used as an input image for this second step with correct secret key-1 in the steganographic tool to reveal the actual message hidden in the cover1. The process is illustrated below:

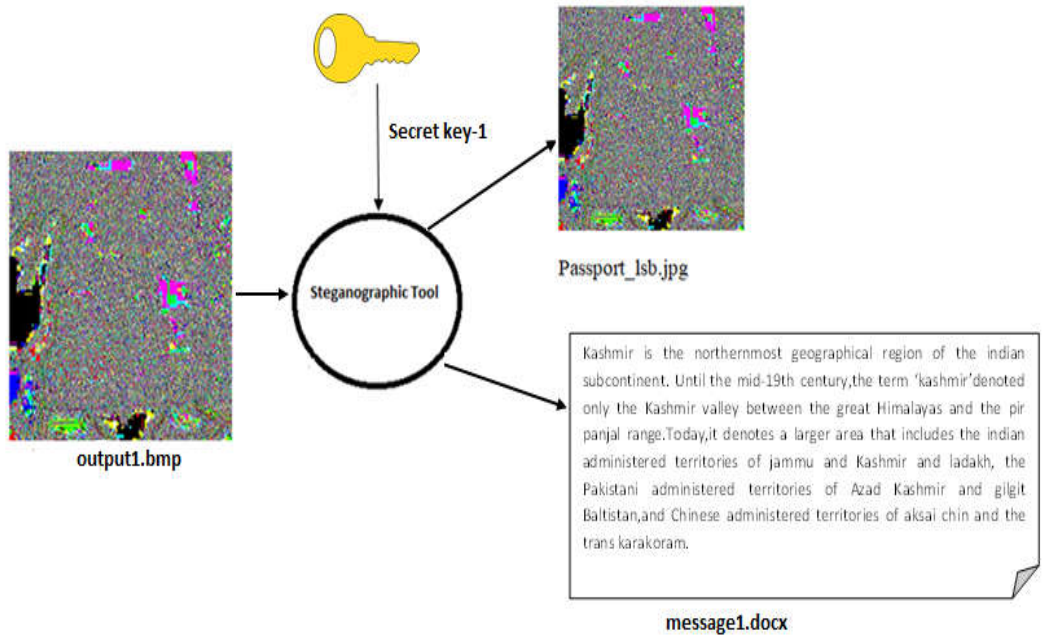


Figure : Step 2 of revealing process of hidden image in DEDC model

As shown above in the figure that when output1.bmp image and secret key-1 is supplied to the steganographic tool as input image and key then the steganographic tool will separate the cover i.e. passport_lsb.jpg file and the message file i.e. message1.docx.

5. Conclusion

Sending the secret messages safely from one place to another place is a challenging task from ancient times. At the ancient times messages are carried by a responsible person of confidence. In the present time, the medium are the communication channel like internet. Internet is a shared communication medium for all. Hence, a different level of secrecy or confidentiality is required. As we have discussed in the first chapter, cryptography and steganography are the two ways that we may use to setup such a secure communication method.

In our proposed model DEDC [Double Encryption Double Cover], we have applied both the cryptography and steganography techniques to design such a strong mechanism for securing our secret message. In DEDC model, the LSB image is used to confuse the unauthorized receiver that the secret message is in the message1.docx file or in the LSB image. As we have to increase the complexity of the security. So, we have use the AES-128 encryption or decryption technique to encrypt or decrypt the secret message, as well as we have developed a new algorithm create_lsb() to create a LSB image from the cover1.jpg file and use the LSB_cover1.bmp file as the cover1.

In the DEDC model, we have introduced the concept of double cover and double encryption. In this model, two secret keys are used that increases the complexity exponentially. Hence, we can say that DEDC is a very secure steganographic model to send the secret message over the shared communication channel.

Appendix

An appendix, if needed, should appear before the acknowledgments.

Acknowledgments

Understanding the art of steganography and creating LSB images is really a tough task. We are giving our sincere thanks to all the contributors of this paper directly or indirectly.

REFERENCES

[1] *Amrita Khamrui, J K Mandal, "A Genetic Algorithm based Steganography using Discrete Cosine Transformation", Elsevier, volume 10, 2013, ISSN: 105-111, pp. 105-111*

[2] *Daphney Jerly, Dsouza Girish S, "A method of data hiding in QR code using image steganography", INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY, volume 4, 2018, ISSN: 2454-132x, pp.1111-1113*

[3] *Della Babya, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michaela," A Novel DWT based Image Securing Method using Steganography", Elsevier, volume 46, 2015, ISSN: 612-618, pp.612-618*

[4] *Gandharba Swain , " A steganography method combining LSB substitution and PVD in a block ", Elsevier, volume 85, 2016, ISSN: 39-44, pp. 39-44*

[5] *Ratnakirti Roya, Anirban Sarkara, Suvamoy Changdera, "Chaos based Edge Adaptive Image Steganography", Elsevier, vol. 10, 2013, ISSN: 138-146, pp. 138-146*

[6] *V.Nagaraj, Dr. V. Vijayalakshmi and Dr. G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function",Elsevier ,volume 4, 2013, ISSN: 17-24, pp.17-24*

[7] *J. K. Mandal and Debashis Das, "Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain", International Journal of Information Sciences and Techniques, volume 2,2012, pp.83-94.*

[8] *Abdelhamid Awad Attaby, Mona F.M. Mursi Ahmed, Abdelwahab K. Alsammak, "Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3", Ain Shams Engineering Journal,2017, pp.1-12*

[9] *Abhijeet Bhaskar, Mr. Upendra Kumar Acharya "IMAGE STEGANOGRAPHY USING MODIFIED LSB",2013, pp.1-5*

[10] *Mohammad Alia and Khaled Suwais, "Improved Steganography Scheme based on Fractal Set", The International Arab Journal of Information Technology, volume 17,2017 ,pp. 128-137*

[11] *Akash Nag, "Low-Tech Steganography for Covert Operations", Modern Education and Computer Science press, volume 1,2018,ISSN:18-30,pp.18-30*

[12] *Biswajita Datta Upasana Mukherjee , Samir Kumar Bandyopadhyaya, " LSB Layer Independent Robust Steganography using Binary Addition", Elsevier, vol.18, 2016, ISSN: 425-432, pp. 425-432*

[13] *Ashita and Smitha, "RANDOMIZED STEGANOGRAPHY IN SKIN TONE IMAGES", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),volume 8, 2018, pp.1-9*

[14] *P. Malathi, T. Gireesh kumar, " Relating the embedding efficiency of LSB Steganography techniques in Spatial and Transform domains", Elsevier, vol. 93, 2016, ISSN: 878-885, pp. 878-885*

[15] *A. Antony Raj, M. Vickraman, A. Vishnu, M. R. Mahalakshmi, "Secure RGB Image Steganography based on Fused Distortion Measurement", International Journal of Research in Engineering , Science and Management ,volume 2,2019,ISSN:2581-5792,pp.175-178*

[16] *Gija Susan Issac ,Jobi Jose, "Secured Transmission Of Image/Video By Performing Reversible Color Transformation", Elsevier, volume 24, 2016, issn:1032-1038, pp. 1032-1038*

[17] *Avinash Sharma, Rajendra Kumar Buraniya, Prashant Kumar Singh, "STEGANOGRAPHY: AN OVERVIEW", International Journal For Technological Research In Engineering ,volume 6,2019,ISSN:2347-4718,pp.5084-5086*

[18] *Ghania Al Sadi, "Image Steganography Approach", International Journal of Computer Science and Mobile Computing, volume 4, 2015, ISSN:2320-088X, pp.166-169*

[19] *Ammar Odeh, Khaled Elleithy, Miad Faezipour, "Steganography in Text by Using MS Word Symbols", Proceedings of 2014 Zone 1 Conference of the American Society for Engineering Education, 2018, pp.1-7*

[20] *Vipul Sharma ; Madhusudan, "Two New Approaches for Image Steganography Using Cryptography", 2015 Third International Conference on Image Information Processing (ICIIP), pp. 202-207*

[21] *Abdelhamid Awad Attaby, Mona F.M. Mursi Ahmed, Abdelwahab. Alsammak, "Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3", Ain Shams Engineering Journal,2017, pp.1-12*

[22] *Dr.P.Sujatha, " Detection of Hidden Information With Bit Plane Analysis", International Journal of Linguistics and Computational Applications (IJLCA), volume-1, 2014, ISSN:2394-6385,pp.1-21*

[23] *Roshidi Din, Azman Samsudin, Zalizam,Muda, Lertkrai, Angela Amphawan, and Mohd. Nizam Omar, "Fitness Value Based Evolution Algorithm Approach for Text Steganalysis Model", INTERNATIONAL JOURNAL OF MATHEMATICAL MODELS AND METHODS IN APPLIED SCIENCES, volume 7,2013,pp.551-559*

[24] *Dr. Monisha Sharma and Mrs. Swagota Bera, "A REVIEW ON BLIND STILL IMAGE STEGANALYSIS TECHNIQUES USING FEATURES EXTRACTION AND PATTERN CLASSIFICATION METHOD", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Volume 2, No.3, June 2012,pp.117-135*

[25] *Gaurav Rajput, R.K. Agrawal, and Namita Aggarwal, "Performance Evaluation of Exponential Discriminant Analysis with Feature Selection for Steganalysis", Defence Science Journal,volume 62, No. 1, January 2012, pp. 19-24*