www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 199-206

e-ISSN : 2583-1062

Impact Factor : 5.725

MESSAGE ENCRYPTION IN STEGANOGRAPHY COMBINED WITH MULTIPLE ALGORITHM

R Anandhkumar[1], S Arunraj[2], Sarika Jain[3], S Geetha[4]

[1]M.Sc-CFIS, Center of Excellence in Digital Forensics, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 089, Tamilnadu, India

[2,3]Center of Excellence in Digital Forensics, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 089, Tamilnadu, India

[4]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Maduravoyal, Chennai 600 095, Tamilnadu, India

ABSTRACT

Basically, the purpose of steganography is to provide secret communication like cryptography. but steganography must not be confused with cryptography, where one transforms the message so as to make its meaning obscure to malicious people who intercept it. therefore, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message.

Keywords: Steganography, encryption, RSA algorithm, DES algorithm, blowfish algorithm.

1. INTRODUCTION

Steganography has been deduced from Greek word “Stego” which means “Covered” and “Graphia” which means “jotting”. Steganography is an ancient fashion of covert communication. The foremost form of Steganography has been reported by the Chinese. The secret communication was written in veritably fine silk or paper, and also it was rolled into a ball and covered with wax. The runner would either swallow the ball or hide it in his lower corridor.

2. LITERATURE SURVEY

(Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, and Hung-Min Sun, 2008) To increase the embedding capacity of image steganography and provide an imperceptible stego-image for human vision, a novel adaptive method of substituting the number of least significant bits with a private stego-key based on grayscale is proposed in this paper. The new technique embeds a binary bitstream into a 24-bit colour image (blue channel) or an 8-bit grayscale image. The method also verifies whether the attacker tried to modify the secret hidden (also orstego-image) information in the stego-image. This technique embeds the hidden information in the spatial domain of the envelope image and uses a simple digital signature (based on the Ex-OR operation) using a 140-bit key to verify the integrity from the stego image. Furthermore, the embedded confidential information can be extracted from the stego-images without the help of the original images. The proposed method can insert 4.20 bits into each pixel.

(Ki-Hyun Jung, Kyeoung-Ju He, Kee-Young Yoo., 2008) in the proposed method, a new data hiding method based on least significant bit (LSB) substitution and multi-pixel differentiation (MPD) method is introduced to improve the capacity of hidden secret data and provide imperceptible visual quality. First, the sum of the different values for a four-pixel subblock is calculated. A low sum value can be placed on a smooth block and a high value is placed on a faceted block. The secret data is hidden into the envelope image by the LSB method in smooth block, while the MPD method is hidden in edged block. Experimental results show that the proposed method has higher capacity and maintains good visual quality.

(Hanling Zhang Guangzhi Geng Caiqiong Xiong., 2009) to increase the capacity of hidden secret information and provide a stego-image imperceptible to human vision, a new steganographic approach based on pixel value differentiation is presented. This approach uses the largest difference value between the next three pixels near the target. pixel to estimate how many secret bits will be embedded in a pixel. Theoretical estimation and experimental results show that the proposed scheme can provide excellent embedding. Furthermore, the embedded confidential information can be extracted from the stego-images without the help of the original images.

(Chen, W. J., Chang, C. C. and Le, T. H. N..,2010) steganography is the art and science of hiding data in information. A secret message is hidden in such a way that no one but the sender or intended recipient can see it. The least significant bit (LSB) substitution mechanism is the most common steganographic technique for embedding a secret message in a high-capacity image, while the human visual system (HVS) would not be able to detect the hidden message in the cover image. In this paper, in addition to using the LSB substitution technique as the base stage, we

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
www.ijprems.com
editor@ijprems.com
Vol. 03, Issue 04, April 2023, pp : 199-206
e-ISSN : 2583-1062
Impact Factor : 5.725

take advantage of edge detection. Experimental results show that the proposed scheme not only achieves high embedding capacity, but also improves the quality of the stego image from HVS by the edge detection technique. Moreover, based on the fact that the secret message is replaced by different LSBs, our scheme can effectively resist image steganalysis.

(Shashikala Channalli and Ajay Jadhav,2009) in today's world, the art of sending and displaying hidden information, especially in public places, has received more attention and faced many challenges. Therefore, various methods have been proposed so far to hide information in different cover media. This article presents a method to hide information on a billboard. It is well known that encryption provides secure channels for communicating entities. However, due to the lack of secrecy on these channels, an eavesdropper can identify encrypted streams using statistical tests and capture them for further cryptanalysis. In this paper, we propose a new form of steganography, the online hiding of information on device output screens. This method can be used to announce a secret message in a public place. It can be extended by other means such as an electronic billboard around a sports stadium, train station or airport. This method of steganography is very similar to image steganography and video steganography. A private labelling system using symmetric key steganography and LSB technique is used here to hide secret information.

3. EXISTING SYSTEM

We consider the previous project coming under the steganography they have an only single encryption algorithm used to encrypt the text. They are website oriented. The former consists of linguistic or language forms of hidden writing. The later, such as invisible ink, try of hide messages physically. One disadvantage of linguistic steganography is that users must equip themselves to have a good knowledge of linguistry.

In recent years, everything is trending toward digitization. And with the development of the internet technology, digital media can be transmitted conveniently over the network. Therefore, messages can be secretly carried by digital media by using the steganography techniques, and then be transmitted through the internet rapidly. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exists a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. So, we prepare this application, to make the information hiding simpler and user friendly.

3.1 Drawback

- They have a one algorithm option to encrypt the text
- Depend upon the third-party webservers

4. PROPOSING SYSTEM

- I create an application to do a message encryption in steganography combined with multiple algorithms.
- I give a multiple encryption algorithm chose to the user.

4.1 Architecture Diagram

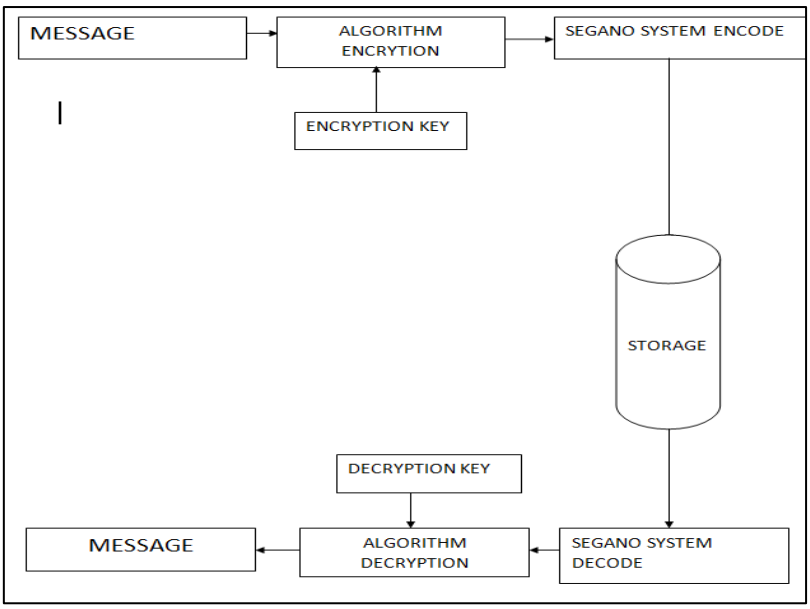

Figure. 1 Architecture Diagram

4.2 List of phases

There are 6 phases

- Technologies
- Working of the System
- Algorithms used
- Spatial Method
- System Design

4.3 Technologies

- Cover-Image: Original image which is used as a carrier for hidden information.
- Message: Actual information which is used to hide into images. Message could be a plain text or some other image.
- Stego-Image: After embedding message into cover image is known as stego-image.
- Stego-Key: A key is used for embedding or extracting the messages from cover-images and stego-images.

4.4 Image Steganography Classifications

- Generally, image steganography is categorized in following aspects shows the best steganographic measures.
- High Capacity: Maximum size of information can be embedded into image.
- Perceptual Transparency: After hiding process into cover image, perceptual quality will be degraded into stego-image as compare to cover-image.
- Robustness: After embedding, data should stay intact if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.
- Temper Resistance: It should be difficult to alter the message once it has been embedded into stegno-image.

4.5 Working of the System

Technical Details

- Using java.awt.Image, ImageIO
- The package contains all the necessary classes and methods along with interfaces that are necessary for the manipulation of the images.

The Encoding Process

The steganography technique used is LSB coding. The offset of the image is retrieved from its header. That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process. For encoding, we first take the input carrier file i.e., an image file and then direct the user to the selection of the text file.

Creation of user Space

- User Space is created for preserving the original file, so that all the modifications are done in the user space.
- In the object of Buffered Image, using ImageIO.read method we take the original image.
- Using create Graphics and draw Rendered Image method of Graphics class, we create our user space in Buffered Image object.

The text file is taken as input and separated in stream of bytes. Now, each bit of these bytes is encoded in the LSB of each next pixel. And, finally we get the final image that contains the encoded message and it is saved, at the specified path given by user, in PNG format using ImageIO.write method. This completes the encoding process.

Technical Details

- Using java.awt.Image, ImageIO
- The package contains all the necessary classes and methods along with interfaces that are necessary for the manipulation of the images.

4.6 The Encoding Process

The steganography technique used is LSB coding. The offset of the image is retrieved from its header. That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process. For encoding, we first take the input carrier file i.e., an image file and then direct the user to the selection of the text file.

4.7 Creation of user Space

- User Space is created for preserving the original file, so that all the modifications are done in the user space.
- In the object of Buffered Image, using ImageIO.read method we take the original image.
- Using create Graphics and draw Rendered Image method of Graphics class, we create our user space in Buffered Image object.

The text file is taken as input and separated in stream of bytes. Now, each bit of these bytes is encoded in the LSB of each next pixel. And, finally we get the final image that contains the encoded message and it is saved, at the specified path given by user, in PNG format using ImageIO.write method. This completes the encoding process.

4.8 Algorithms Used

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is an electronic data encryption specification introduced by the US National Institute of norms and Technology (NIST) in 2001. AES is extensively used moment because it's much stronger than DES and triadic DES, although it's more delicate. to perform. AES is the Advanced Encryption Standard algorithm. It's a type of symmetric, block encryption and decryption algorithm. It works with crucial sizes of 128, 192 and 256 bits. It uses a valid and analogous secret key for both encryption and decryption. In AES, a block cipher is used. This means that the data to be translated is converted into encryption blocks. The original data value is translated using different padding bits, similar as 128, 192, or 256 bits.

DES Algorithm

The DES algorithm is a symmetrical block cipher algorithm that takes plain textbook in blocks of 128 bits and converts them to reckon textbook using keys of 128, 192, and 256 bits. Since the DES algorithm is considered secure, it's in the worldwide standard. 1 crucial metamorphosis We've noted original 64- bit crucial is converted into a 56- bit crucial by discarding every 8th bit of the original key. therefore, for each a 56- bit crucial is available. From this 56- bit crucial, a different 48- bit Sub Key is generated during each round using a process called crucial metamorphosis. For this, the 56- bit crucial is divided into two halves, each of 28 bits. These halves are circularly shifted left by one or two positions, depending on the round. For illustration if the round figures 1, 2, 9, or 16 the shift is done by only one position for other rounds, the indirect shift is done by two positions. The number of crucial bits shifted per round is shown in the figure. After an applicable shift, 48 of the 56 bits are named. for opting 48 of the 56 bits the table is shown in the figure given below. For case, after the shift, bit number 14 moves to the first position, bit number 17 moves to the alternate position, and soon.

However, we will realize that its Page 1 of 2 contains only 48- bit positions, if we observe the table precisely. Bit number 18 is discarded (we won't find it in the table), like 7 others, to reduce a 56- bit crucial to a 48- bit crucial. Since the crucial metamorphosis process involves permutation as well as a selection of a 48- bit subset of the original 56- bit crucial it's called Compression Permutation. Expansion Permutation Recall that after the original permutation, we had two 32- bit plain textbook areas called Left Plain Text (LPT) and Right Plain Text (RPT). During the expansion permutation, the RPT is expanded from 32 bits to 48 bits. Bits are permuted as well hence called expansion permutation. This happens as the 32- bit RPT is divided into 8 blocks, with each block conforming of 4 bits. also, each 4- bit block of the former step is also expanded to a corresponding 6- bit block, i.e., per 4- bit block, 2 further bits are added. This process results in expansion as well as a permutation of the input bit while creating affair. The crucial metamorphosis process compresses the 56- bit crucial to 48 bits. also, the expansion permutation process expands the 32- bit RPT to 48- bits. Now the 48- bit crucial is XOR with 48- bit RPT and the performing affair is given to the coming step, which is the S- Box negotiation.

Blowfish

The Blowfish cipher is a symmetric block cipher designed to be slow and insecure in the DES algorithm. Blowfish is a keyed, symmetric cryptographic block cipher constructed by Bruce Schneier in 1993 and placed in the public sphere. Symmetric encryption uses an individual encryption key to both cipher and decipher information. The sensitive information and the symmetric encryption key are used in the encryption algorithm to convert the sensitive information into ciphertext. Blowfish is included in a huge number of encryption suites and encryption products similar as SplashID. A block cipher is generally a computer routine that takes some quantum of plaintext and converts it to ciphertext or ciphertext. It implements this routine on gobbets of textbook known as blocks. And in order for the textbook to be decrypted on the other side of the transmission, the function should also induce a key to unlock the translated textbook. Blowfish is also one of the fastest block ciphers in public use, making it ideal for a product like SplashID, which runs on a wide range of processors set up in mobile phones and in laptops and desktops. Blowfish has a 64- bit block size and a crucial length from 32 bits to 448 bits. It's a 16- round Feistel cipher and needs large crucial dependent S- boxes. The structure is the same as CAST- 128, which needs fixed S- boxes.

The Blowfish algorithm is one of the most popular, but it demanded significant computing power with some rudiments that made it a victim of too numerous bushwhackers. It can reduce the size of the" s- box" and thereby design and apply it on a neural network (NN). The input to the neural network is textbook (plaintext or ciphertext) and the affair attained from the network is the same textbook, and the key used in both encryption and decryption is the

original weights of the neural network, which are trained using a backpropagation network. Blowfish uses a specific form of crucial generation. The alternate element of the Blowfish routine is crucial expansion, which transforms a single key of over to 448 bits into a 4168- byte table of subkeys. Generating subkeys further improves security because a hacker would have to crack further than just the original key. The continuity of the blowfish algorithm rests on subkey generation and its introductory obfuscation and propagation design. Blowfish is a symmetric master encryption system dependent on the Feistel network. Bruce Schneider introduced the algorithm. It's a 64- bit block size cipher and the full interpretation needs 16 rounds to complete the block cipher and uses a high number of subkeys, a variable key length from 32 bits to 448 bits.

Spatial Method

In the spatial method, the most commonly used method is the LSB substitution method. Least the significant bit (LSB) method is a common, simple approach to embedding information in a cover file. The LSB substitution method is used in steganography. I.e., because every picture has three components (RGB). This pixel information is stored in an encoded format in one byte. The first bits containing this information for each pixel can be modified to store hidden text. A prerequisite for this is that the text to be stored must be smaller or equal the size of the image used to hide the text. The LSB-based method is a spatial domain method. But it is sensitive to clipping and noise. In this method, the MSBs (most significant bits) of the message image are to be hidden stored in the LSB (least significant bits) of the image used as the cover image. It is known that the pixels in the image are stored in the form of bits. There is intensity in the grayscale image each pixel is stored in 8 bits (1 byte). Similarly for a colour (RGB-red, green, blue) image, each a pixel requires 24 bits (8 bits for each layer). The human visual system (HVS) cannot detect changes in colour or intensity and pixel when the LSB bit changes. This is psycho-visual redundancy because it can be used as an advantage to store information in these bits while not noticing any fundamental difference in the bits. Algorithm of LSB method of steganography. There might be two different phases of LSB method, embedding phase and extracting phase. Algorithms of both of the phases are given below:

4.9 Insertion Phase Procedure

Step 1: Extract all the pixels from the given image and store them in some named array (image array).

Step 2: Extract all characters from the given text file (message file) and store it in an array called (message array).

Step 3: Get the characters from the Stego key and store them in an array called key array. Astegokey is used to control the hiding process to limit detection and/or recovery embedded data.

Step 4: Take the first pixel and characters from the Key-matrix and place them in the first component pixel. If there are more characters in the key field, put the rest in the first component of the following pixels.

Step 5: Place some termination symbol to indicate the end of the key. 0 was used as the termination symbol in this algorithm.

Step 6: Place the message box characters in each folder of additional pixels by replacing them.

Step 7: Repeat step 6 until all characters are entered.

Step 8: Place some termination symbol again to indicate the end of the data.

Step 9: The obtained image will hide all the entered characters.

4.10Masking and Filtering:

Masking and filtering techniques, usually limited to 24-bit or grayscale images, include and another approach to hide the message. These methods are basically similar to paper watermarks, creating marks in the image. This can be achieved, for example, by editing brightness of parts of the image. While masking changes the visible properties of an image, this can be done in such a way that the human eye does not notice the anomaly. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and various types of image processing. the information is not hidden in the noise level but is inside the visible part of the image which making it more suitable than LSB modification in the case that a lossy compression algorithm like JPEG is used.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 199-206

e-ISSN : 2583-1062

Impact Factor : 5.725

5. Modelling and analysis

System Design

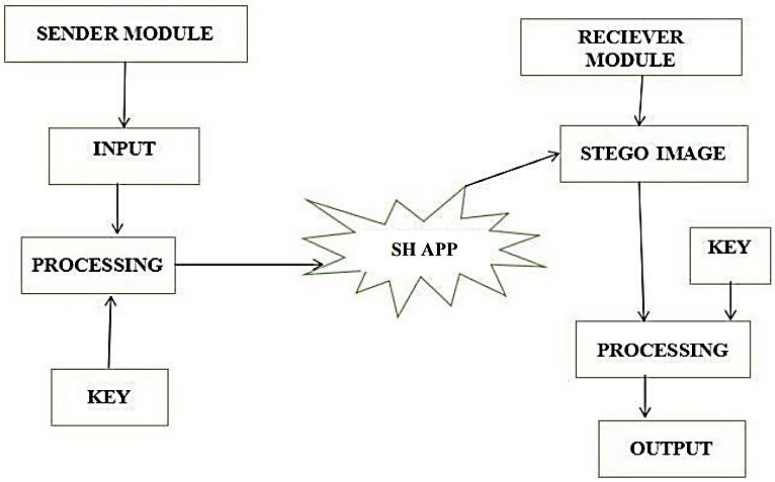

Figure 2. System Design

Screen Shots

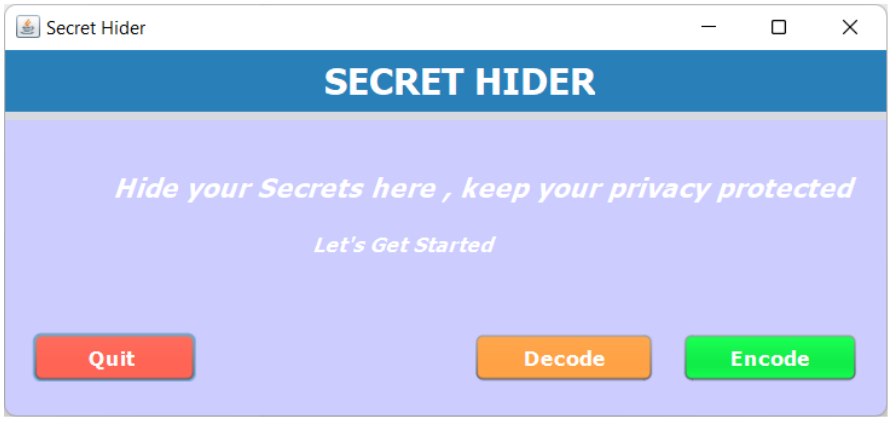

Figure 3. Home Page

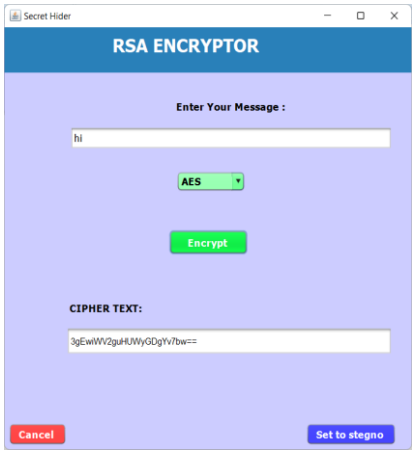

Figure 4. Encryption Process

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 199-206

e-ISSN : 2583-1062

Impact Factor : 5.725

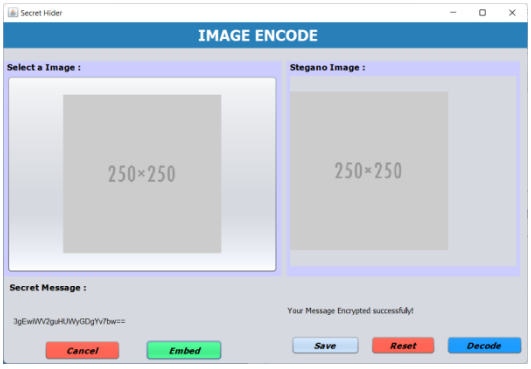

Figure 5. Stenographer Encode Process

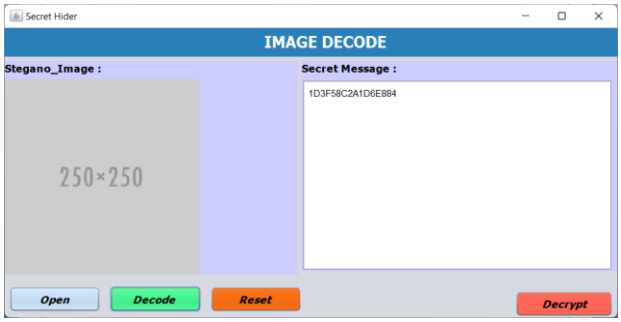

Figure 6. Stenographer Decode Process

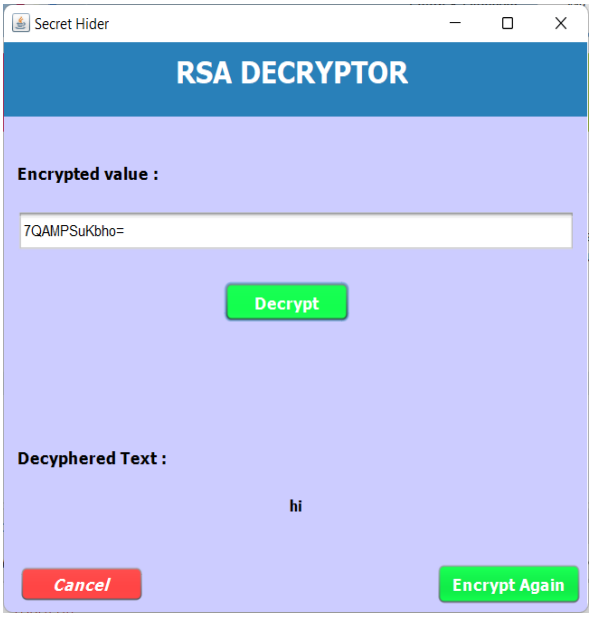

Figure 7. Decryption Process

6. CONCLUSION

Steganography is useful for hiding messages or images for transmission. One of the major discoveries of this investigation was that each steganographic implementation carries with it significant trade-off decisions, and it is up to the stenographer to decide which implementation suits him/her best. Since we have added the multiple algorithms, the user doesn't even consider about the implementation.

7. REFERENCES

[1] H. Yang, X. Sun, G. Sun. A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution. Journal: Radio engineering Year: vol. 18, 4 Pages/record No.: 509-516, (2009).

[2] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, Member, IEEE, and Hung-Min Sun, Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems, IEEE Transactions on Information Forensics and Security, vol. 3, no. pp. 488-497. 3rd September (2008).

[3] Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo. Image data hiding method based on multi-pixel differencing and LSB substitution methods. In Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08). Daejeon (Korea), Aug. 28-30, p. 355-358, (2008).

[4] Hanling Zhang Guangzhi Geng Caiqiong Xiong, Image Steganography Using Pixel-Value Differencing, Electronic Commerce and Security, ISECS '09. Second International Symposium on May (2009).

[5] https:www.phash.org/demo/

[6] http:freshmeat.sourceforge.net/projects/phash

[7] Chen, W. J., Chang, C. C. and Le, T. H. N., High Payload Steganography Mechanism Using Hybrid Edge Detector, Expert Systems with Applications (ESWA 2010), vol. 37, no. pp. 3292-3301, 4th April (2010).

[8] Al-Husainy, M. A., Image Steganography by Mapping Pixels to Letters, Journal of Computer Science, vol.5 no.1, pp. 33-38, (2009).