Journal of Engineering Technology and Applied Physics

A Survey on Crypto-Steganographic Schemes and A Use Case in Healthcare System

Mei Ling Phang and Swee Huay Heng*
Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450, Melaka, Malaysia.
*shheng@mmu.edu.my
https://doi.org/10.33093/jetap.2019.1.2.6

***Abstract* - Information sharing has become prevalent due to the expansion of social networking in this 21st century. However, electronic devices are vulnerable to various kinds of attacks. Information might be disclosed, modified and accessed by an unauthorised third party which consequently leads to the breach of confidentiality, integrity and availability of the information. Therefore, it is of utmost importance to employ the technology of cryptography and steganography to protect information assets. Cryptography and steganography have weaknesses when they are working alone. Therefore, crypto-steganography, the combination of cryptography and steganography are introduced to overcome the weaknesses in order to provide a double layer of security and protection. This paper provides a general overview of steganography and cryptography as well as a comparison analysis of different crypto-steganographic schemes. A secure crypto-steganographic system for healthcare is then developed with the implementation and integration of the secure crypto-steganographic scheme proposed by Juneja and Sandhu. This healthcare system enables users to store and deliver message in a more secure way while achieving the main goals of both cryptography and steganography.**

Keywords—Steganography, cryptography, least significant bit (LSB), crypto-steganographic

I. Introduction

Cryptography and steganography are the two important techniques to deal with transmitting information over the insecure channel. Cryptography is different from steganography and the definition of cracking cryptography and steganography system is different. In steganography, the system is broken when the attacker knows that steganography has been utilised and he can detect the embedded message. In contrast, breaking of cryptographic system requires the attacker to decrypt the encrypted secret message. Past research has shown that it is probable to merge the techniques by encrypting the message and hiding the encrypted message with cryptography and steganography respectively [1]. This combination of crypto-steganographic can provide a higher level of security. This can be shown when cryptography converts the message into unreadable form but this encrypted message is able to be seen by everyone. Therefore, the intruders may try to decrypt the encrypted message in order to retrieve the original message. Steganography can deal with the imperfection of cryptography by concealing the encrypted message in other media such as pictures, audio or video [2].

A. Cryptography

Cryptography is the technique of protecting information from the unauthorised third party. The encryption process is the translation of the plaintext into unintelligible ciphertext. The reverse of the encryption process is called decryption which converting ciphertext back to plaintext. The purpose of cryptography is to provide a number of security goals which include integrity, authentication, access control, confidentiality and non-repudiation to avoid security issues. Cryptography can be categorised as asymmetric key cryptography and symmetric key cryptography [3].

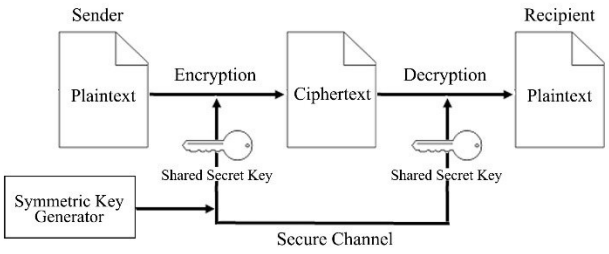

Fig. 1. Symmetric key encryption and decryption process.

Symmetric key cryptography is sometimes called private key cryptography. Identical cryptographic key is utilised for encryption and decryption in symmetric key cryptography. Symmetric key encryption can use block cipher or stream cipher. In the stream ciphers, plaintext is encrypted a bit or a byte at a time. On the other hand, block ciphers encrypt plaintext a block at a time and the fixed plaintext block size

Published by MMU PRESS. URL: https://journals.mmupress.com/index.php/jetap/index

can be 64 bits, 128 bits and 256 bits of data. The example of the symmetric key cryptography includes Blowfish, Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4) and Data Encryption Standard (DES). Fig. 1 illustrates the symmetric key encryption and decryption process.

Asymmetric key cryptography, or public key cryptography utilises two different keys for the encryption and decryption process which is public key and private key. The public key in the key pair can be shared with everyone to encrypt the plaintext while the private key which needs to be kept secret is used to decrypt the ciphertext. Asymmetric key cryptography, unlike symmetric key cryptography, requires a secure channel to exchange the secret key between the sender and receiver. The example for asymmetric key cryptography includes RSA, DSA, and ElGamal. Fig. 2 illustrates the asymmetric key encryption and decryption process.

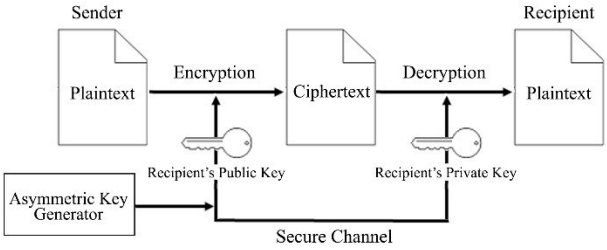

Fig. 2. Asymmetric key encryption and decryption process.

B. Steganography

Steganography is the technique of hiding the presence of the message from an observer. The process of steganography technique can be classified into four categories which are text, image, audio, and video [4]. In the text steganography, text file acts as cover media to hide the data, while image steganography uses the image; audio steganography uses audio and video steganography uses video to hide data. The common technique used by four of this steganography is LSB to achieve confidentiality.

Concealing information inside an image is a well-known technique nowadays. It is simple to spread an image that contains a secret message in a newsgroups or over the World Wide Web [5]. In image steganography, image files like BMP, PNG, JPEG, TIFF, GIF etc. are used to hide data. The technique used to achieve confidentiality is LSB, spread spectrum etc. Image steganography algorithms can be classified into two categories which are transform domain steganography and spatial domain steganography.

Transform domain is also known as frequency domain. The pixel value of the image is changed into coefficients utilising some mathematical transformation function and the message bits are embedded into the coefficients. The mathematical functions to change an image to frequency domain include Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Integer Wavelet Transform (IWT), Discrete Wavelet Transform (DWT), etc. However, DCT is the most famous transform function in the image among the transformation techniques due to the availability of DCT based image format in public domain [6].

The pixel value of the image is directly altered and substituted by the message bit in spatial domain. LSB substitution is the most common algorithm for concealing the secret message because it is the easiest technique with less algorithmic complexity. This algorithm makes use of the fact of LSB in an image could be treated as random noise and modifies to the least significant bit will not produce a conspicuous change on the image [7]. Due to Human Visual System (HVS) are not able to detect the slight changes in the image, it is less prone to HVS attack. Other than LSB substitution, there are various steganography techniques such as LSB matching, Adaptive LSB and Pixel Value Differencing (PVD), Edge detection filter based, etc. to insert data into the image.

Both transform domain and spatial domain have their strengths and weakness. Spatial domain algorithm is the simplest scheme in terms of embedding and extraction complexity. It has higher capacity compared to frequency domain algorithms. However, it is highly prone to cropping, compression and statistical attacks. On the other hand, transform domain has less capacity and complex way of hiding information in image but it is less exposed to cropping and compression [6].

C. Our Contributions

In this paper, we review the existing crypto-steganographic schemes in the literature. In particular, we focus on the feature of cryptographic and steganographic algorithms used by the existing crypto-steganographic schemes, and compare and discuss about their security properties, strengths and weaknesses.

We also developed a secure crypto-steganographic system for healthcare with the implementation and integration of the secure crypto-steganographic scheme proposed by Juneja and Sandhu [8]. Tools and techniques of the crypto-steganographic scheme that are used to develop the secure crypto-steganographic system will be described.

II. A Review on the Crypto-Steganographic Schemes

Juneja and Sandhu proposed a secure and robust approach by improving LSB based steganography techniques to conceal message in a 24-bit bitmap colour image [8]. Two-component based LSB methods utilised blue and green components of a random location in the edge area of images to embed secret data. While adaptive LSB based steganography randomly embedded data based on Most Significant Bit (MSB) of the blue, red, and green component of pixel in smooth areas. This method is more robust as it is combined with AES encryption algorithm [9, 10]. The authors used 128 bits key length which was more secure because no threats were found on 128 bits, but threaten found on 192 and 256 bits. The advantage of AES is robust against hacking and flexible and simple. The hybrid feature detection technique integrated Canny edge detection algorithm and enhanced Hough transform technique is used to extract edges and smooth areas from the cover image. The Canny edge detector is a standard edge detection algorithm due to its great localisation, great detection abilities, and insignificant measure of false edge detection rate. The Hough transform is utilised to refine the output of Canny edge detector by distinguishing the lines, circle, edge links, and peaks. The adaptive LSB substitution in this proposed scheme utilised the algorithm provided by Kekre and improved it to embed secret message bit and get smoother areas of a cover image.

Nurdiyanto *et al.* [11] proposed a method combining PVD steganography proposed by Wu and Tsai [12] with GOST encryption algorithm to provide higher security level in connection with data integrity as well as confidentiality. GOST encryption algorithm is a Soviet and Russian government standard symmetric key block cipher. It utilises 64-bit block ciphers and 256-bit keys with 32 round processes. The GOST method utilises eight permanent S-boxes to accept 4-bit input and produce a 4-bit output. Exclusive OR (XOR) operations and Rotate Left Shift also used in GOST method. PVD steganography divided image into non-overlapping blocks contain two consecutive pixels and the difference value between this two connecting pixels in the image is calculated. The computed difference value is to decide the number of bits to be embedded into the image. The embedding process in this technique is performed by comparing two neighbouring pixels until all of the message bits are inserted into the cover image.

Joshi *et al.* proposed a method which combines cryptography and spatial domain steganography on grey images [13]. Vernam cipher algorithm is used to encrypt the message at first to enhance the security. LSB with shifting (LSB-S) is utilised to embed encrypted message into an image. Vernam cipher is a symmetrical stream cipher which plaintext is integrated with identical length of random stream data to produce the ciphertext utilising XOR operation. The receiver and the sender need to share one-time pad key which is random and used only once for Vernam cipher. The four LSB of the image pixel is utilised and circular left shift operation and XOR operation is performed in LSB-S technique.

Juneja *et al.* proposed method which combines RSA algorithm and advanced LSB insertion [14]. This paper also suggested a method to rank the images in the user library according to the suitability of an image to be the cover image for the secret message. RSA encryption is an asymmetric cryptography uses a pair of public and private keys which are different but mathematically linked. Public key can be shared to sender for encrypting a message, whereas private key is utilised for decrypting the unintelligible message and must be kept covertly by the receiver. RSA modulus is the product of two huge prime numbers based on the difficulty of the factorisation. LSB insertion in this proposed method is to compare the encrypted message bits with the LSB of the colour pixel in the image. The first byte to the last byte in the cover image is compared in order to allow all the encrypted message bit to be embedded. The cycles through the pixel of the image is to search for the block of bytes that produce in least number of LSB changes. Next, the rank will be produced according to the matching percentage between encrypted message bits and the LSB of image bits. For instance, 10 bits of encrypted message to be embedded has a bit pattern 1000000001. If the block of bytes of the cover image with a bit pattern of 1000000011, the percentage of matching is ninety percent as 9 out of the 10 bits are exactly matched.

Kumar *et al.* proposed a technique by combining Hash-LSB and RSA algorithm [15]. RSA algorithm is an asymmetric key cryptography to enhance the secrecy of the message. The message is encrypted by public key and the meaningless encrypted message is decrypted by private key. Hash-LSB utilised a hash function to generate a model for embedding message bits into LSB of red, green and blue component of pixel value in the cover image. The hash function in this technique deals with the LSB bit position of the image pixel, the position of the image pixel and the number of bits of LSB [16]. Each 8 bits of the encrypted message are inserted into the LSB of the pixel value of image in the order of 3 bits in red colour component, 3 bits in green colour component and 2 bits in blue colour component. The embedding process is repeated until the entire message bits are embedded into the cover image.

Islam *et al.* used AES cryptography and improved LSB substitution method to provide better security [17]. AES cryptography is a symmetric key cryptographic algorithm that allows 128, 192 and 256 bits of key length. The message is encrypted with AES cryptography before embedding into cover image using LSB substitution. In this proposed technique, the author improved the LSB technique by using MSB bit to filter the cover image pixel. The MSB is used to analyse the darker area when the MSB of pixel has at least 2 bits of 0's and lighter area when the MSB of pixel has at least 2 bits of 1's. LSB substitution to embed message is performed depending on the darker and lighter area of the cover image [18]. This method used status checking for embedding and extracting messages. The comparison between the message bit and the LSB bit position of third byte is made and the LSB of 3rd byte will transform to "1" if matched and "0" if not matched.

Rashmi *et al.* proposed method which combines AES encryption and traditional Reversible Data Hiding techniques (RDH) [19]. Confidentiality will be provided by encrypting with AES encryption and the key. The ciphertext will be inserted to the cover image with RDH algorithms to form stego image. RDH algorithms embed messages into the cover image which is visually invariant, and the stego image can be losslessly restored after extracting the embedded messages. RDH algorithms generate a host sequence with the small entropy and reversibly embed message into the host sequence by modifying its histogram [20]. The proposed algorithm is secure as it uses dual level security with symmetric key sharing. It has a better invisibility feature when this crypto-steganographic method is applied on colour image compared to grey images as the quality of image does not degrade.

Harianto *et al.* proposed a method which combines bit matching steganography and AES to improve the security of the exchanged bit [21]. Bit matching steganography is able to find the location of matching pixels and creates a key to retrieve the encrypted message. AES is adopted to improve the security. The proposed method uses all colour channel of the cover image and locates message on the cover image follows the exact matches of colour value of image pixels and ASCII values of the secret message. This method will not generate the location for any duplicate character from the secret message. It will only use one pixel location and use it to regenerate the duplicate character. Next, it generates a secret key based on the message stored location and encrypts it with AES. The secret key is then sent to the receiver. This method overcomes the limitation of LSB that has less hiding capacity and improves the image quality.

Mohammad Obaidur Rahman *et al.* proposed a method which combines Blowfish algorithm and a new efficient embedded algorithm using Embedded Least Significant Bits (E-LSB), and used SHA-256 Hashing Algorithm for integrity checking [22]. The secret message is first encrypted with Blowfish encryption algorithm. Next, the encrypted message is embedded into cover image with E-LSB to create a stego

image. In E-LSB, the pixel of colour image is broken into frames of 8-bit for Red, Green and Blue plane respectively. The least significant 3, 2, 2-bit of Red, Green and Blue frame of a pixel will be utilised to embed the encrypted message. In order to check the data integrity, SHA-256 is used to calculate the hash value of stego image. Data detection attacks, for instance, visual attack and RS attack are applied to evaluate the security of this steganography system. These attacks are not able to detect any embedded data in the stego image.

III. Comparison Analysis

For ease of presentation, we summarise the crypto-steganographic schemes in terms of the cryptographic method and steganographic method employed, and image format during image compression in Table 1. The comparison of steganographic and cryptographic techniques are made in Table 2, Table 3 and Table 4 respectively.

A. Crypto-Steganographic Schemes

Table 1. Crypto-Steganographic Scheme.

Scheme	Crypto-graphic Method	Type of Crypto-graphy	Steganographic Method	Image Format
[8]	AES	Symmetric	2 component based LSB substitution, Adaptive LSB substitution	BMP
[11]	GOST	Symmetric	PVD	JPG
[13]	Vernam Cipher	Symmetric	LSB-S	-
[14]	RSA	Asymmetric	LSB insertion	BMP
[15]	RSA	Asymmetric	LSB insertion	TIFF
[17]	RSA	Symmetric	LSB substitution	BMP
[19]	AES	Symmetric	RDH	-
[21]	AES	Symmetric	Bit matching	-
[22]	Blowfish	Symmetric	E-LSB	-

We note that image compression is essential to reduce the storage space required and the bandwidth needed when transmitting over a network. Image compression methods can be categorised into lossless compression and lossy compression. The original image can be entirely restored after decompression in the lossless image compression. In contrast, lossy compression damages the image and only partial reconstruction are possible after decompression [23]. JPG files employ lossy compression which means some message bits get lost during the compression step. BMP files are uncompressed, and it is capable to hide a large message [24]. TIFF file is a flexible format that can be lossy or lossless compression [25].

B. Steganography

Among the prime security properties or characteristics of steganography are imperceptibility, robustness, and capacity of the hidden data [26]. Therefore, to evaluate the best crypto-steganographic scheme to be applied in the real life application, the scheme has to possess these essential properties. Table 2 shows the comparison of the properties achieved by LSB in the different schemes.

Table 2. Goal achieved by LSB.

Scheme	Imperceptibility	Robustness	Capacity
[8]	✓	✓	✓
[11]	✓		✓
[13]	✓		✓
[14]	✓	✓	
[15]	✓		
[17]	✓		
[19]	✓		
[21]	✓		✓
[22]	✓		

C. Cryptography

Cryptography is essential to keep data secure from unauthorised persons. Table 3 shows the brief comparison of symmetric and asymmetric key cryptography while Table 4 shows the comparison in terms of the specific encryption schemes employed in the respective crypto-steganographic schemes.

Table 3. Type of cryptography.

Type of Cryptography	Advantage	Disadvantage
Symmetric key	- Not consuming much computing power. - Work with high speed for encryption.	- Need secure channel for key distribution. - Cannot provide digital signature.
Asymmetric key	- Use different key for encryption and decryption. - Eliminates the need of secure channel to distribute public key. - Provide digital signatures.	- Speed of encryption is slower than symmetric key cryptography [3].

Table 4. Cryptographic method.

Cryptographic Method	Strength	Weakness
AES	- Fast and reliable. - A robust security protocol to implement in both software and hardware. - Strength of key length is sufficient to protect top secret information. - Difficult to hack as 128 bits of key length need 2^{128} attempts to break.	- Use simple algebraic structure. - Every block encrypted in the same way. - The long key length can cause complexity.
GOST	- Has faster speed than IDEA encryption algorithm.	- Can be broken by an algebraic attack and is a deeply flawed cipher. - Does not provide the security level required by ISO [27].
Vernam Cipher	- Encryption key is a random number and the key is used only once, so the cipher will be secured. - Unbreakable since there is no statistical relationship between ciphertext and plaintext.	- Amount of key bits are as large as the amount of plaintext. - Has problem of distributing key safely.
RSA	- Increased security because the private key does not need to be revealed to others. - Provide digital signature. - Hard to crack due to the difficulty of the factorisation of prime numbers.	- Has very slow speed in processing because encryption and decryption need a lot of calculation [28] - Complexity of key creation as this algorithm is limited by prime and efficiency of generating prime is low.
Blowfish	- Has fast encryption and decryption time [29]. - Consume less memory for unit operations. - Record the highest average entropy per byte of encryption [30].	- Not able to give confirmation and non-denial as two individuals have the same key. - Small block size of Blowfish is helpless against the attacks.

IV. Secure Crypto-Steganographic System for Healthcare

In this section, we provide a real-life application as a use case of crypto-steganographic in healthcare industry. This healthcare system is realised with the implementation of the crypto-steganographic scheme proposed by Juneja and Sandhu [8]. Juneja and Sandhu's scheme has been selected as it achieves the goal of imperceptibility with minimum mean square error, robustness tested and sustained the steganalysis attacks, and its capacity increases with the use of hybrid feature detection to detect more edge pixel to embed message. This scheme uses AES symmetric key encryption that consumes less computing power and it is fast and reliable. This healthcare system enables users to store and transmit confidential data securely with a double layer of security which the data is encrypted before hiding into a cover image. Therefore, the attackers are not able to perform cryptanalytic attack if they do not know the existence of encrypted message that appeared as an image. The use of this system can benefit the healthcare industry to secure the patient's sensitive information such as personally identifiable information and health data that must not be disclosed or accessed by any unauthorised party.

The minimum requirement of the application is to achieve the main goals of cryptography which protects the message confidentiality, integrity, and availability as well as basic requirements of steganography such as imperceptibility, robustness, and capacity of hidden message.

A. Tools and Techniques Used

Advanced Encryption Standard. A fast encryption technique to make the message unreadable. It consumes less computing power and it is fast and reliable. It is a robust security protocol to be implemented in a software and difficult to be hacked as the strength of key length is sufficient.

Hybrid Detection Method. It is used to extract pixel in the edges and smooth areas from an image. This technique combines the Canny edge detection technique [31] and Enhanced Hough transform techniques [32]. Canny edge detection technique. It is used to detect edges in images. It has great localisation, great detection abilities and insignificant measure of false edges detection rate. Enhanced Hough transform technique. It is utilised to improve the outcome of Canny edge detector which to discover the peaks, lines, circles and edge links from the output image processed by the Canny edge detector.

Two-Component LSB Substitution. This method is used to embed secret message into the edge pixels of the image. The 8-bit of the blue component would be utilised to embed encrypted message followed by embedding message into the 4 LSB of green component. The secret message is embedded more into the edge areas of image as human perception is less sensitive to changes in edge areas.

Adaptive LSB Substitution. This method is used to embed secret message into the smooth areas of the image. The embedding process across smooth areas in the image is employed according to the pixel value of each colour component. This method integrates maximum changes in blue, average changes in green component and least amount of changes in red. This is due to the visual perception of intensely red object is more distinct than the perception of green and blue [33].

B. Embedding Module and Extracting Module

The following Fig. 3 and Fig. 4 show the embedding module and extracting module respectively.

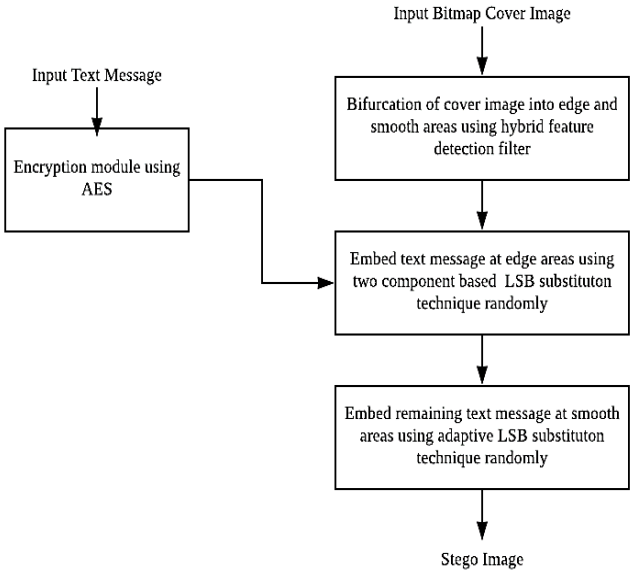

Fig. 3. Embedding module.

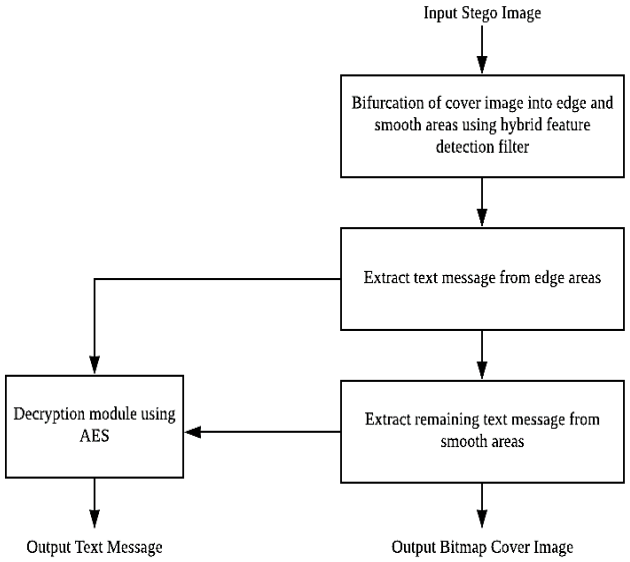

Fig. 4. Extracting module.

C. Result

The functionalities and the output will be illustrated along with the screenshots of the application.

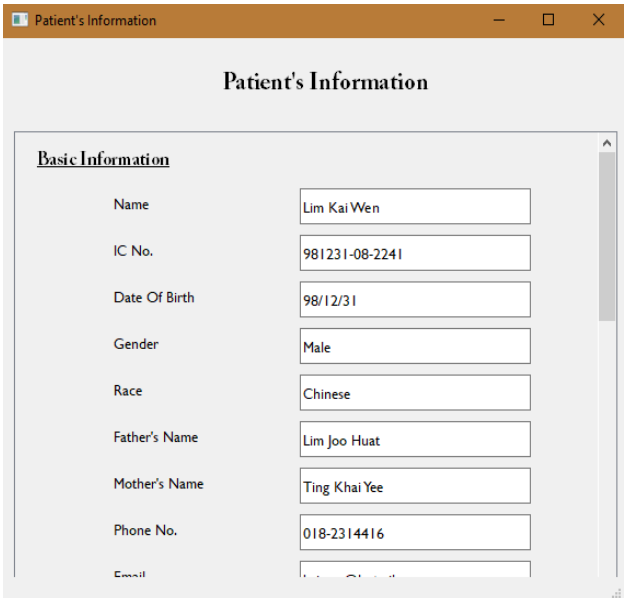

Fig. 5. Patient's information (Part 1).

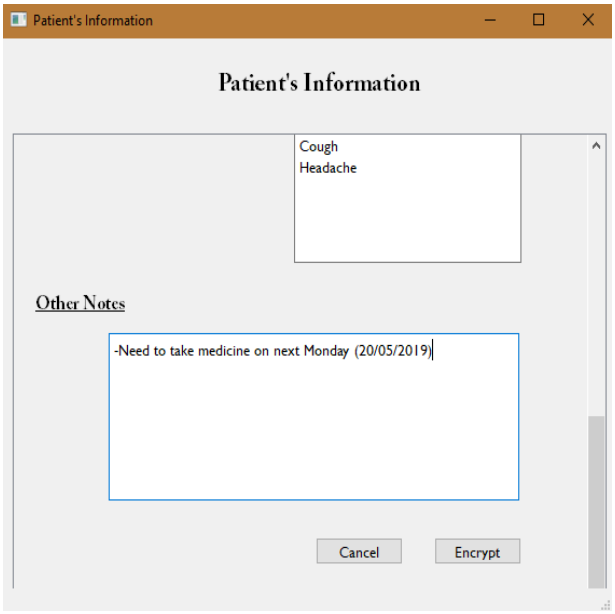

Fig. 6. Patient's information (Part 2).

To add a new patient in the application, the user inputs all the patient's information and the information will be encrypted once the "Encrypt" button is clicked. In this step, AES encryption function is called to encrypt the patient's information to protect data from unauthorised personnel. Fig. 5 shows the interface for user to key in the patient's information. Fig. 6 shows the "Encrypt" button to press after the data is keyed in.

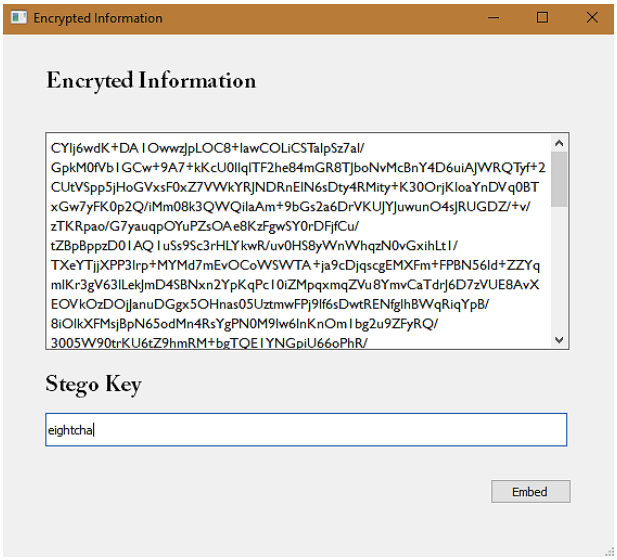

Fig. 7. Encrypted information.

Fig. 7 shows the patient's information is successfully encrypted. The user needs to input 8 characters stego key. Once the user presses the "Embed" button, the next page will be shown to user to select image to hide the encrypted data.

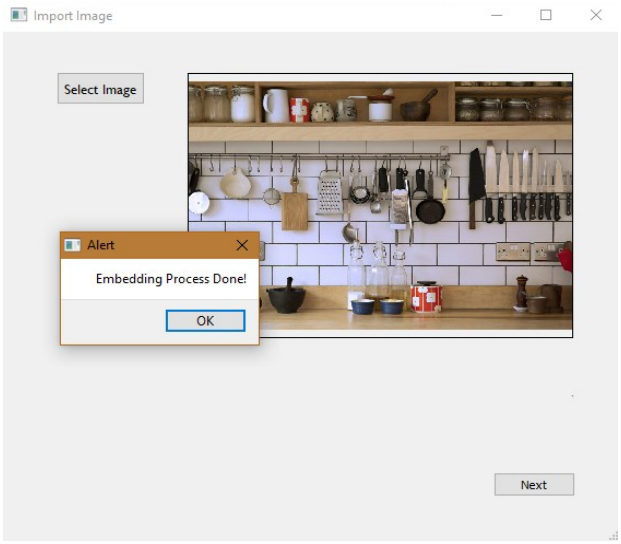

Fig. 8. Input image.

Fig. 8 shows the window for user to input image and for embedding process. In this step, Canny Edge Detection Technique and Enhanced Hough Transform Technique will be executed to detect the line and circle in the image to categorise edge and smooth pixel. After the detection of edge and smooth area, the embedding process for stego key is performed. Next, two component-based LSB substitution method is called to embed the encrypted data in the edge pixel until the end of the encrypted data character or the end of edge pixel. If there is remaining character to embed in the smooth area, adaptive based LSB substitution method is called.

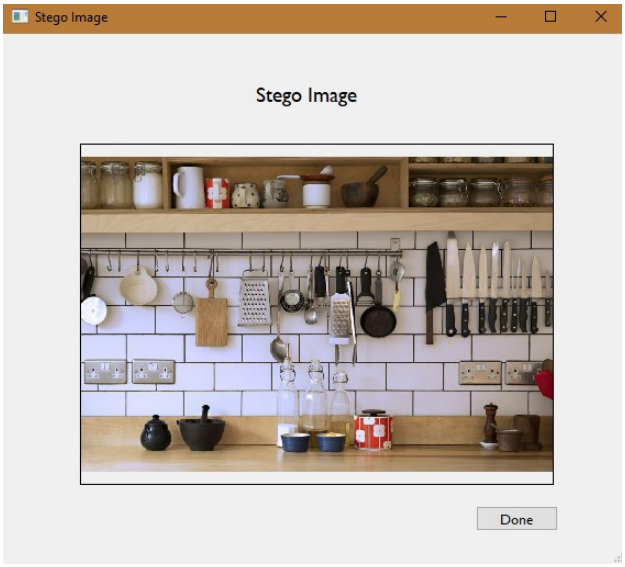

Fig. 9. Stego image.

Fig. 9 shows the stego image after the embedding process. The stego image is successfully formed with the implementation of crypto-steganographic scheme. The stego image is directly stored into the user's device.

V. Evaluation Analysis

The robustness of the selected solution was examined through several steganalysis attacks which include visual analysis and statistical analysis. Visual analysis and statistical analysis will be performed and explained with the result of crypto-steganographic technique.

A. Visual Analysis

The result of the selected crypto-steganographic scheme proposed by Juneja and Sandhu [8] is shown in Fig. 10. The result shows this technique effectively withstands visual attack as the visual difference between original image and stego image are not able to be detected with human perception. Fig. 11 shows the original image. Fig. 12 and Fig. 13 respectively show that the file size of original image and modified stego image are the same.

Fig. 10. Stego image (embedded.bmp).

Fig. 11. Original image (original.bmp) [34].

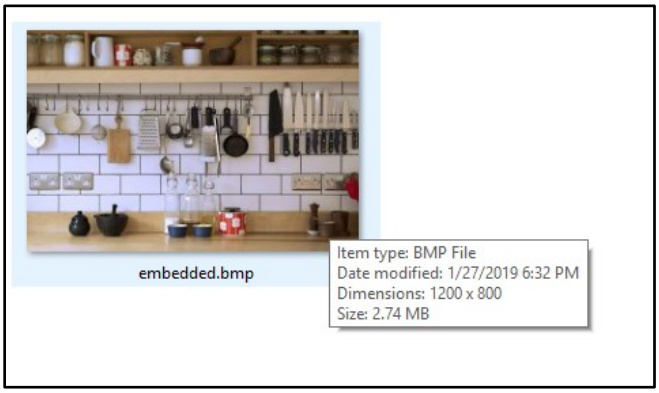

Fig. 12. Files size of stego image.

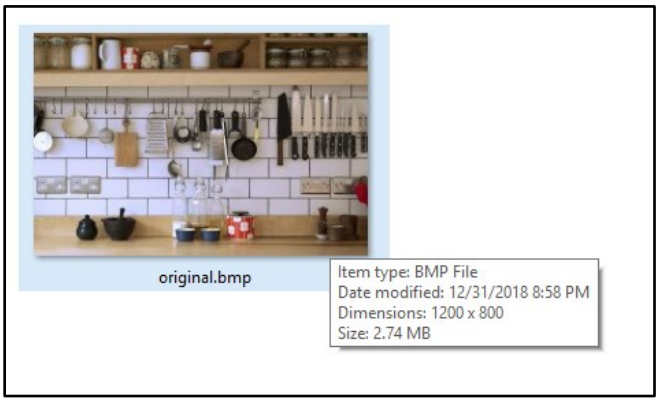

Fig. 13. File size of original image.

B. Statistical Analysis

Histogram analysis technique is used to compare the colour level of original image and stego image. This analysis is carried out with the use of online image histogram tool, PINETOOLS (https://pinetools.com/image-histogram). Fig. 14 and Fig. 15 respectively show the histogram analysis of the blue, red, green and luminosity of the modified stego image and original image (original.bmp). The result of histogram analysis technique shows the original and stego image are the same, therefore the attacker is not able to attack.

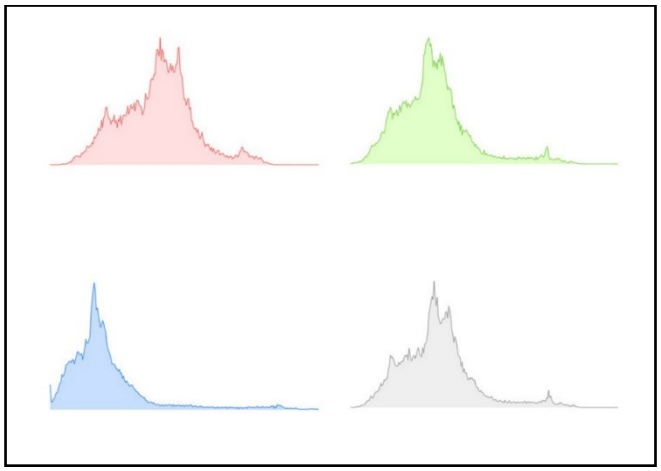

Fig. 14. Histogram analysis of the blue, red, green and luminosity of the stego image (embedded.bmp).

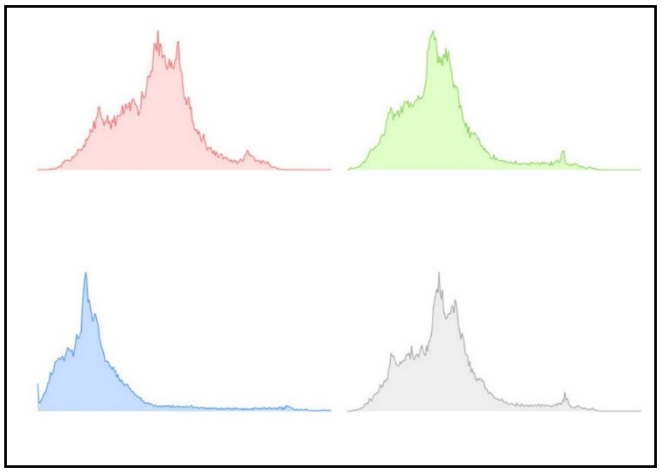

Fig. 15. Histogram analysis of the blue, red, green, and luminosity of the modified original image (original.bmp).

VI. CONCLUSION

We presented an overview of the existing crypto-steganographic schemes with their strengths and weaknesses. We also highlighted the similarities and differences between the crypto-steganographic schemes. A secure crypto-steganographic system for healthcare is then developed with the implementation of the selected scheme proposed by Juneja and Sandhu. In this system, a few techniques have been employed, namely, a secure and robust method using hybrid feature detection technique to extract edge and smooth areas from an image, two-component LSB substitution to embed secret message randomly in edge area, adaptive LSB substitution to embed secret message randomly in smooth area and standard encryption technique AES to encrypt message before the embedding process. We also showed that this system withstands two steganalysis attacks which are visual analysis and statistical analysis. Therefore, this crypto-steganographic system for healthcare managed to achieve the main goals of cryptography which protects the message confidentiality, integrity, and availability as well as basic requirements of steganography such as imperceptibility, robustness, and capacity of hidden message.

ACKNOWLEDGEMENT

The authors would like to acknowledge the Malaysia government's Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/MMU/01/01) for supporting this work.

REFERENCES

[1] H. Rout and B. Kishore Mishra, "Pros and Cons of Cryptography, Steganography and Perturbation techniques," *IOSR J. Electron. Commun. Eng.*, no. December, pp. 2278–2834, 2015.

[2] R. Mishra and P. Bhanodiya, "A Review on Steganography and Cryptography," *Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)*, pp. 119–122, 2015.

[3] R. Tripathi and S. Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography," *Int. J. Adv. Found. Res. Comput.*, vol. 1, no. 6, pp. 2348–4853, 2014.

[4] A. Febryan, T. W. Purboyo and R. E. Saputra, "Steganography Methods on Text , Audio , Image and Video: A Survey," *Int. J. Appl. Eng. Res.*, vol. 12, no. 21, pp. 10485–10490, 2017.

[5] J. R. Krenn, "Steganography and Steganalysis," https://www.krenn.nl/univ/cry/steg/article.pdf, no. January, 2004.

[6] M. Kalita, "A Comparative Study of Steganography Algorithms of Spatial and Transform Domain," *Int. J. Comp. App.*, pp. 9–14, 2015.

[7] J. Kour and D. Verma, "Steganography Techniques: A Review," *Int. J. Emerg. Res. Manag. & Technol.*, vol. 3, no. 5, pp. 132–135, 2014.

[8] M. Juneja and P. S. Sandhu, "A New Approach for Information Security using an Improved Steganography Technique," *J. Inf. Process. Syst.*, vol. 9, no. 3, pp. 405–424, 2013.

[9] S. C. Sumathi, T. Santanam and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," *Int. J. Comput. Sci. Eng. Surv.*, vol. 4, no. 6, pp. 9–25, 2013.

[10] P. S. Anju, B. Kuriakose and V. Paul, "A Survey on Steganographic Methods Used in Information Hiding," *Int. J. Sci. Eng. Comput. Technol.*, vol. 6, no. 1, pp. 27, 2016.

[11] H. Nurdiyanto and R. Rahim, "Enhanced Pixel Value Differencing Steganography with Government Standard Algorithm," *2017 3rd Int. Conf. on Sci. in Inf. Technol.*, pp. 366–371, 2017.

[12] H. Tseng and H. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," *J. Appl. Maths.*, vol. 2013, pp. 1–8, 2013.

[13] K. Joshi and R. Yadav, "A new LSB-S Image Steganography Method blend with Cryptography for Secret Communication," *Proc. 2015 3rd Int. Conf. Image Inf. Process (ICIIP)*, pp. 86–90, 2016.

[14] M. Juneja and P. S. Sandhu, "Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption," 2009 *Int. Conf. on Advances in Recent Technol. in Comm. and Comp.*, pp. 302–305, 2009.

[15] A. Kumar and R. Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique," *Int. J. of Adv. Res. in Comp. Sci. and Soft. Eng.*, vol. 3, no. 7, pp. 363–372, 2013.

[16] K. Dasgupta, J. K. Mandal and P. Dutta, "Hash Based Least Significant Bit Technique for Video Steganography (HLSB)," *Int. J. Secur. Priv. Trust Manag. (IJSPTM)*, vol. 1, no. 2, pp. 1–11, 2012.

[17] M. R. Islam, A. Siddiqa, M. P. Uddin, A. K. Mandal and M. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES cryptography," *2014 Int. Conf. Informatics, Electron. Vision (ICIEV)*, 2014.

[18] H. A. Prajapati and D. N. G. Chitaliya, "Secured and Robust Dual Image Steganography: A Survey," *Int. J. Innov. Res. Comput. Commun. Eng.*, vol. 3, no. 1, pp. 30–37, 2015.

[19] N. Rashmi and K. Jyothi, "An Improved Method for Reversible Data Hiding Steganography Combined with Cryptography," *Proc. 2nd Int. Conf. Inven. Syst. Control.(ICISC)*, no. Icisc, pp. 81–84, 2018.

[20] D. Hou, W. Zhang, J. Liu, S. Zhou, D. Chen and N. Yu, "Emerging Applications of Reversible Data Hiding," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1477, pp. 105–109, 2019.

[21] H. Antonio, P. W. C. Prasad and A. Alsadoon, "Implementation of Cryptography in Steganography for Enhanced Security," *Multimed. Tools Appl.*, 2019.

[22] M. O. Rahman, M. K. Hossen, G. Morsad and A. Chandra, "An Approach for Enhancing Security of Cloud Data using Cryptography and Steganography with E-LSB Encoding Technique," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 9, pp. 85–93, 2018.

[23] P. Miklós, "Comparison of Spatial and Frequency Domain Image Compression Methods," *4th Int. Conf. Work. Mechatronics Pract. Educ. – MECHEDU 2017*, pp. 57–60, 2017.

[24] E. Eltyeb, "Comparison of LSB Steganography in BMP and JPEG Images," *Int. J. Soft Comput. Eng.*, vol. 3, no. 5, pp. 91–95, 2013.

[25] R. R. Sindhu M, "Images and Its Compression Techniques – A Review," *Int. J. Recent Trends Eng. Technol.*, vol. 2, no. 4, pp. 71–75, 2009.

[26] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[27] N. T. Courtois, "Security Evaluation of GOST 28147-89 in View of International Standardisation," *Cryptologia*, vol. 36, no. 1, pp. 2–13, 2012.

[28] N. Qi , W. Wei, J. Zhang, W. Wang, J. Zhao, J. Li, P. Shen, X. Yin, X. Xiao and Jie Hu, "Analysis and Research of the RSA Algorithm," *Inf. Technol. J.*, vol. 12, pp. 1818-1824, 2013.

[29] M. Nazeh, A. Wahid, A. Ali and M. Marwan, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," *J. Comp. Sci. Appl. Inf. Technol.*, pp. 1–7, 2018.

[30] P. Patil, P. Narayankar, D. G. Narayan and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016.

[31] J. Canny, "A Computational Approach to Edge Detection.," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 8, no. 6, pp. 679–698, 1986.

[32] P. E. Queneau, "Method and Means for Recognizing Complex Patterns," U.S. Pat. 3.069.654, 1962.

[33] "The Rods and Cones of the Human Eye." [Online]. Available: http://hyperphysics.phy-astr.gsu.edu/hbase/vision/rodcone.html. [Accessed: 30-May-2019].

[34] R. T. Houzz, "How to Organize your Kitchen — and Enjoy Cooking in It | Valley Life | argusobserver.com." [Online]. Available: https://www.argusobserver.com/valley_life/how-to-organize-your-kitchen-and-enjoy-cooking-in-it/article_1959efd0-9fe3-11e8-a135-f3c020d54df5.html. [Accessed: 30-Jan-2019].