Multimedia Tools and Applications (2019) 78:32721–32734
https://doi.org/10.1007/s11042-019-7559-7

Implementation of cryptography in steganography for enhanced security

Harianto Antonio[1] · P. W. C. Prasad[1] · Abeer Alsadoon[1]

Received: 18 February 2018 / Revised: 1 March 2019 / Accepted: 2 April 2019 /
Published online: 10 May 2019

Abstract
The rapid development in technology has had a great influence on the exchange of information. In this modern era, maintaining security during informationexchanges is essential. There are many algorithms were used to ensure the exchanged data is confidential, with examples being cryptography and steganography. In this paper, we present a combined of bit matching steganography and Advanced Encryption System (AES) cryptography are used to improve the security of the exchanged data. Bit matching steganography has advantages in terms of payload capacity and image quality. The bit matching algorithm presented here is capable of finding the location of matching pixels and creates a key to retrieve the secret message. The AES algorithm is secure standard cryptographythatensures security of the generated key from attack. The proposed method utilizes the entire color channel to find the bit matching and then encrypts the key generated from the bit matching method before sending it to a receiver. Experimental results show that the proposed method has higher speed, an undistorted image, and unlimited payload capacity when compared with other popular steganography algorithms. Moreover, the proposed method also provides security against statistical steganalysis.

Keywords Steganography · Cryptography · Encryption · Advanced encryption system · Information hiding · Exact matching algorithm · Image,Secret message · LSB · And key-dependent data technique

1 Introduction

Alongside the development in communication technology, information exchange in public networks has increased. It is essential to secure private content and this issue has been considered has been the subject of a significant body of researcher over several decades.

✉ P. W. C. Prasad
cwithana@studygroup.com

[1] Charles Sturt University – Sydney Campus, 63, Level 1, Oxford Street, Darlinghurst, Sydney 2010, Australia

Cryptography is the process of encrypting sensitive information into scrambled messages [19]. However, the form of encrypted messages makes them conspicuous and attracts attacker into attempting to decrypt the message. Steganography is defined as the art of hiding confidential messages within media, in the form of images, text, video, audio, and protocols [1, 9, 11, 17]. This method provides protection in the form of confidentiality, information availability, and integrity.

The main difference between cryptography and steganalysis lies in the cryptography, where the confidential message is encrypted to prevent third partiesfromunderstanding it. By doing that, the existence of the secret message is recognized, but cannot be undertood without using decryption methods. In steganography, the existence of a secret message is concealed in the media container. The combination of steganography and cryptography can increase the data security [8, 9, 17]. According to the mechanism usedfor data embedding, steganography can be divided into spatial domain and frequency domain. According to Alsarayreh [5], the spatial domain provides more hiding capabilities and offers lower computational time.

A Steganography system consist of an embedding process and an extracting process. A stego image is produced in the embedding process while a cover image and secret message will be required as input. To hide the secret information, the pixel of the cover image will be secretely chosen with a stego key. After that, the secret message can be extracted as shown as in the Fig. 1.

According to Kanan and Nazeri [11], there are 3 main features in steganography that make it suitable for information hiding, which are:

1. Payload Capacity: Determined by the number of secret bits embedded in each cover image pixel. A higher number indicates more data can be embedded into a cover image.
2. Imperceptibility: usually calculates the stego image's quality by using a peak signal-to-noise ratio (PSNR). The number will be small if the image quality is poor and high if the image quality is good.
3. Robustness: Prevents the secret data from being stolen or manipulated.

The three main features of steganography is shown in Fig. 2.

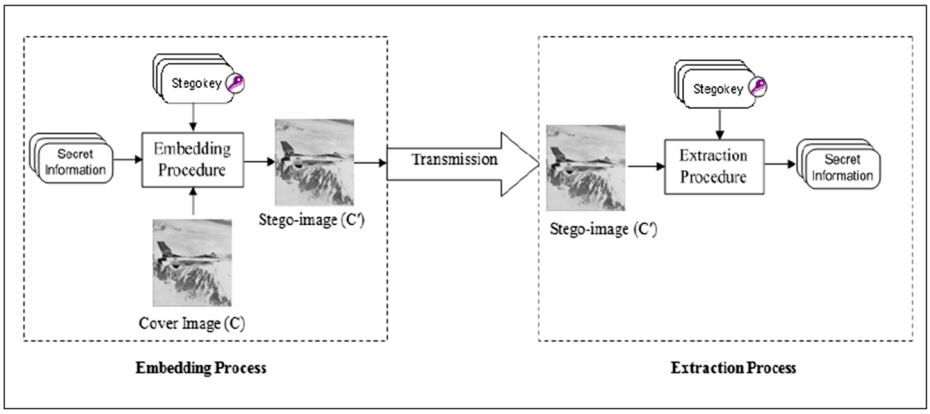


Fig. 1 General Steganography System

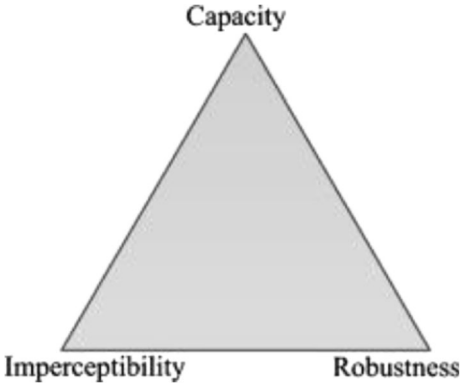


Fig. 2 Trade-off triangle of Steganography features

This paper is organized as follows: In Section 2, we provide brief information of the various techniques of steganography and examine their strength and weaknesses. In Section 3, we give the details of the proposed method. Section 4 shows the experimental results and analysis, and the conclusion is given in section 5.

2 Related work

2.1 Least significant bit (LSB)

The LSB method is the most popular technique used in spatial domain steganography. Muhammad, Ahmad, Rehman, Jan, and Sajjad [14] implemented two level encryption algorithms alongside a multi-level encryption to increase the security of the LSB method. Although this method increased the security of the secret message, the payload capacity and image quality are not increased; it is also needed longer computational time.

According to Sabeti, Samavi, and Shirani [18], calculated pixel complexity and setting the threshold value before using the LSB method to embed the secret message. This can be improved the produced stego-image. This method also secured againts analytical steganalysis attack. The drawback of this method is when the data embedding is high, the stego-image is weak againts visual attack. Similar results have also beenfound by Muhammad, Sajjad, Mehmood, Rho, and Baik [13].

2.2 Multi-bit embedding

Multi bit embedding is the improvement of the LSB method which in this method will use more than one bit for embedding instead of using only the last bit of image's pixel value. Chen, Chang, and Le [6] improved the payload capacity by combining Canny edge detection and Fuzzy edge detection to increase the accuracy for finding edge areas in the images. This method increased the payload capacity, but the disadvantage represented in the image quality, whichis reduced when embedding includes large data.

Furthermore, in recent years, multi-bit embedding has also been used to increase the payload capacity. Several uses of steganography based on multi-bit embedding have been reported [3, 4, 7, 10, 12, 19, 20]. Thismethod, which focused on increasing the payload capacity, generally has a problem with the quality of the produced image.

Table 1 Matched values from a sample secret message

X-axis value	Y-axis value	Character	Character position in the secret message
0	122	t	1
3	135	e	2
2	12	s	3
0	122	t	4
0	63	Space	5
8	152	s	6
5	33	a	7
5	62	m	8
0	45	p	9
0	12	l	10
0	135	e	11

2.3 Block-data hiding

The block-data hiding is a steganography method where, before embedding, the image is divided into blocks. Nguyen, Arch-int and Arch-int [15, 16] proposed a method to increase the payload capacity, image quality and security by using multi-bit plane block data hiding, adaptive region selection, and AES encryption. The stego image produced through this method is very good and secured against Human Visual Attack. The drawback is that the computational workload is very high.

According to Nguyen, Arch-int, and Arch-int [16], Cellular automata techniques and XOR encoding can be used to improve the security of the block-data hiding methods. This system has good security, but the computational workload is high.

2.4 Bit-matching

The bit-matching method works by finding the matching bit between the secret message bit value and image's pixel bit value to generate a key to point to the location of the pixel bit and the sequence of the secret message. According to Alamsyah, Muslim, and Prasetyo [2], to

Table 2 The Key Structure for Each Character

Character	Character location	Pixel location (x,y)	Key values for each character
t	1	0,122	0,122^1^4
e	2	3135	3135^2^11
s	3	2,12	2,12^3^6
t	4	0,122	–
Space	5	0,63	0,63^5
s	6	2,12	–
a	7	5,33	5,33^7
m	8	5,62	5,62^8
p	9	0,45	0,45^9
l	10	0,12	0,12^10
e	11	3135	–

0,122^1^4$3,135^2^11$2,12^3^6$0,63^5$5,33^7$5,62^8$0,12^10*0,45^9*

Fig. 3 Key generated from test sample before encryption

combine bit-matching and the DES method can increase the security of the bit-matching technique. This method has high image quality and security, but the drawback when it is vulnerable in to any direct image processing.

Alsarayreh, Alia, and Maria [5] worked on a the bit-matching method which focused on matching values between the ASCII value of the secret message and the pixel value from blue channel. This method provides an excellent good stego image, but security is lacking and weak when subjected to the image processing.

2.5 Current best solution

The current best solution is proposed by Alsarayreh [15]. This solution uses bit-matching methods to generate a key. In this solution the matching values between secret images and pixel's colour values location, a key was created and sent to the receiver to reconstruct the secret images from the key. In order to get the matching value, the secret message was converted into their ASCII value to find the matches with the pixel colour values of the blue channel.

The reason for choosing this approach as the best solution was because it needs low computational workload and simple to implement. The image quality was not reduced from the method so it's secure against any type of attacks.

This method doesn't consider securing the key generated from the exact matching. Any attacker who gets the key can reconstruct the secret message from the key and the image. The limitation also exists when the author only consider to use the blue channel to find the matches since it will reduce the possibilities to broaden the matching values, this method is also not secure against image processing.

3 Proposed method

In this section, the proposed method takes the advantages of the bit-matching algorithm which is presented in section 2.4. The proposed solution incorporates the advantages from the model with the exact matching algorithm to produce undistorted stego images with high embedding capacity. Furthermore, AES security features will also be adopted to improve the security.

The fundamental idea of the proposed system is to use all color channels from images and locate all the Exact Mathces (EM) between the ASCII values of the secret message and the color values of image pixels. A key dependent data will be created and encrypted as a part of the separating procedure. This method overcomes the LSB limitation of hiding capacity and also overcomes the high computational complexity of frequency domain steganography. The

A5cbi44LTyeBUQXmTpaN6TQE97jQC+bkbynlQjOEfL21RtAdJb9C9Af3pRFiEskaZLbMWqAelaYSukjpujx77q0EtvDKFwXW6qf
3XeUPnkPI-10sCnKeYerHUsOkNaFY

Fig. 4 Key generated from test sample after encryption

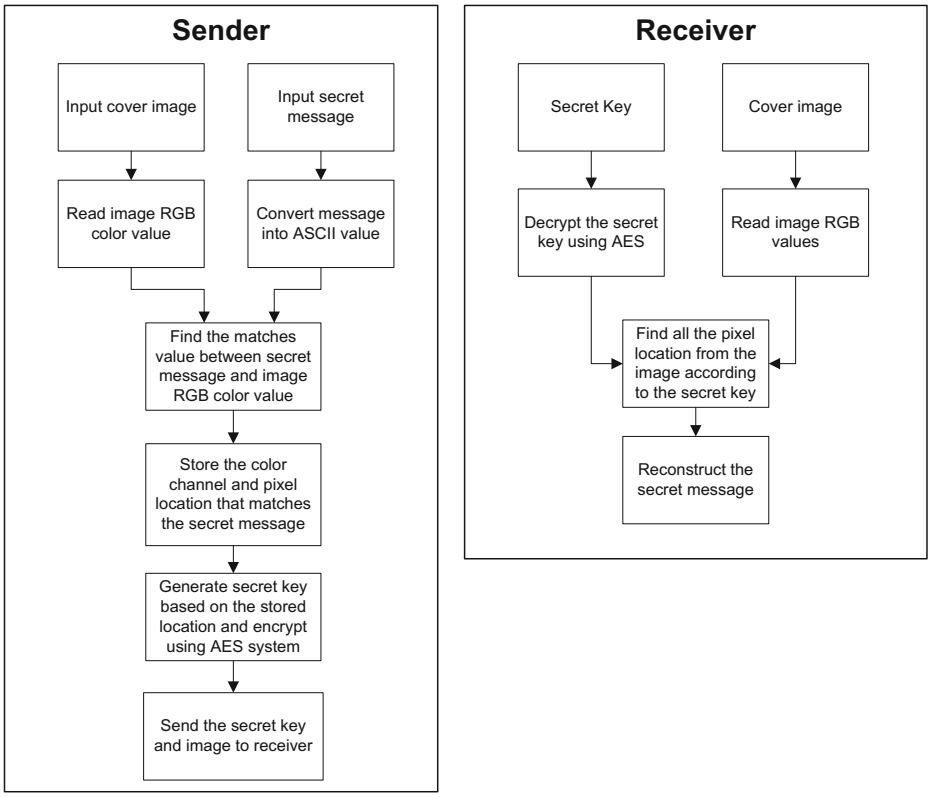


Fig. 5 Proposed system block diagram

process of finding the Exact Matching and the key dependent data will be shown in Section 3.1, and the key creation will be explained in Section 3.2. The extraction of the secret information will be demonstrated in Section 3.3.

3.1 Exact matching (EM) between images and secret message

This section will explain a method of getting the match between cover image and secret message. This method starts with converting the secret message into decimal ASCII value, after which it starts reading the cover image color starting from Blue channel, Green channel and finally to Red channel as decimal value. The system will try to discover the matches between image's pixel color and the secret message. This method will not regenerate the location of any duplicate character from the secret message. It will only use one pixel location and use it to regenerate the duplicate character. After finished all matching between secret messages and images, all locations (x,y) of the matching pixel will be saved and used to generate the key for sending to the receiver. Table 1 shows a sample of a secret message "test sample" that has been used to demonstrate how the system works. In the secret message, the characters (t) and (e) are both repeated twice, but the system will only use the first matched location value and use it for the construction of the key.

The algorithm below shows how the proposed method works to find the exact matches between the cover image and secret message:

Algorithm 1: Extraction exact matches pixel locations

Input: Cover image and secret message.
Output: Array of matches pixel locations and character position in secret message.
Begin:
Step 1: Convert the secret message into ASCII value and read the cover image color value.
Step 2: Store the pixel location that matches the cover image's color value and ASCII value from the secret message starting from the blue color channel, and then green color channel, and finally red color channel.
End

3.2 Key-dependent data creation process

The key is created from the location of the pixel in the cover image and the location of the character in the secret message. However, the key must have three values for each character. The first value from creating the key is the x-axis (row) and y-axis (column) value from the pixel. The second value is the location of the character in the secret message. The third value is the special character that will be used to reconstruct the secret message from the key. The (,) will be used for divide the row and column of the pixel location. The ($) character will be used to separate the pixel location and the character location in the secret message. The (^) character is used to divide each character from secret message from others, and the (*) character will be used to divide the color channels used. The system will only use one pixel location for any duplicate character from the secret message to maintain computational simplicity. Table 2 shows an example for the key creation for each character from the secret message "test sample".

After having found all matches and created the key, the last step is to combine all the key values from each character and encrypt it with an Advanced Encryption System with 128-bit key size to form the key that will be sent to the receiver. Figure 3 shows the key created from the secret message "test sample" before encryption. Notice that the character p cannot be found in the blue channel but it can be found in the green channel instead. So, during the key creation process, the key value of character p is after the special character (*) to show that the pixel value is from the next color channel, which is the green color channel. Figure 4 shows the key after AES encryption has been used.

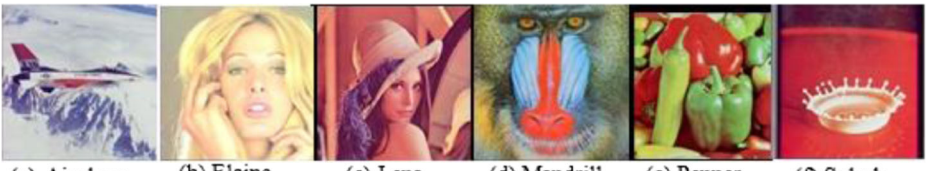


Fig. 6 dataset used for the experiment (Alsarayreh et al., 2017)

Table 3 Results of number of possible matches found

Table Dataset	Number of possible matches from current method	Number of possible matches from proposed method
Airplane	209	255
Lena	225	256
Elaine	189	242
Mandrill	256	256
Pepper	244	256
Splash	240	256

3.3 Extraction and secret message reconstruction process

The algorithm below shows the proposed method for reconstruct the secret message from the image and generated key received:

Algorithm 2: Extraction for pixel locations and reconstruction for the secret message
Input: Image and generated key.
Output: Secret message.
Step 1: Decrypt the generated key with AES method.
Step 2: Decode the generated key to get location of the pixel and character position in secret message.
Step 3: Read the color value from pixel location and color channel.
Step 4: Convert the color value into ASCII and reconstruct the secret message.
End

The proposed system block diagram is shown in Fig. 5. Both the sender and receiver will have the same system. From the sender, the system will require the cover image and the secret message as input for the user. The system will convert the secret message into ASCII value and find the matches with the cover image. After the matching process is completed, the AES method will be used to encrypt the key generated before sending itto the receiver along with the image to maintain the integrity

Table 4 Results of time consumption

Number of characters	Current method (ms)	Proposed Method (ms)
5	87	0.18
10	104	0.20
20	82	0.24
30	88	0.31
90	91	0.62
130	91	1.35
210	91	3.30
300	149	3.84
450	114	4.47
600	121	6.36
725	139	11.15
829	133	16.55
971	157	24.59

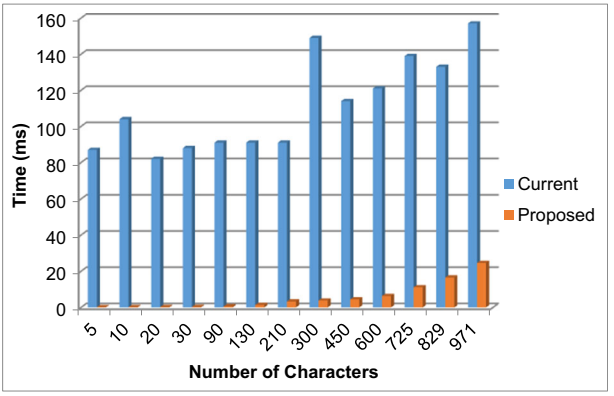


Fig. 7 Number of characters and searching time

of the message. The receiver will receive the key and the image, after which the system will use the AES method to decrypt the key and reconstruct the secret message from pixel coordinates and character location.

4 Experiment results and analysis

The implementation of the proposed model has been carried out by using NetBeans 8.2 with 6 sample images. The experiment has been carried out on a computer that is running with Windows 10 Operating System, Intel i7 2.5 GHz processor and 4 GB RAM. Fig. 6 shows the dataset that will be used for the experiment. The dataset used for the experiment is fromAlsarayreh [5]. The performance of the proposed system has been measured based on percentage of matching value and levels of security between the current method and the proposed method. The images used for the experiment are airplane, Lena, Elaine, mandrill, pepper, and splash.

Table 5 Results of generated key size

Number of characters	Current method (byte)	Proposed Method (byte)
5	20	88
10	27	152
20	50	216
30	230	236
90	405	704
130	648	920
210	900	1388
300	873	1880
450	744	2712
600	1024	3520
725	1350	4204
829	1550	4760
971	1830	5528

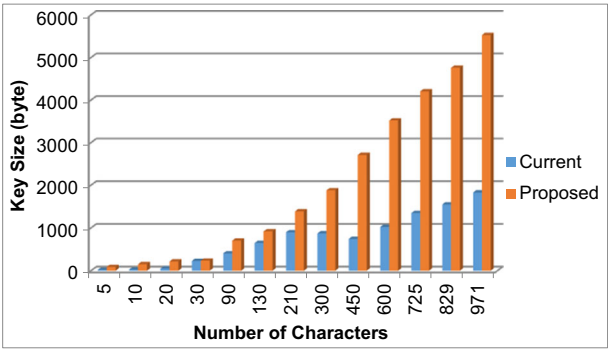


Fig. 8 Number of character and key size

The image quality and imperceptibility are strongly related. If there are any changes in the image quality, then the imperceptibility will be reduced. The image quality will be calculated by using PSNR as defined in Eq. 1.

4.1 Equation 1 PSNR calculation

$$PSNR = 10x\log_{10}\frac{255^2}{MSE}(dB) \tag{1}$$

Where MSE (Mean Square Error) will be calculated as defined in Eq. 2. Where W is image width and H is the height, with $I_{ij}$and I'_{ij} are the pixel values of the cover image and stego image, respectively.

4.2 Equation 2 MSE calculation

$$MSE = \frac{1}{WxH}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(I_{ij}-I'_{ij}\right)^2 \tag{2}$$

Table 3 shows the result of possible matches found from each dataset. It is shown that the proposed method can find more matches than the current method. The increase in the matches

Table 6 Comparison between proposed method and Existing Steganography Method

No	Author (s)	Steganography method	PSNR	MSE	Payload capacity
1	Muhammad et al. (2017)	Multi-Level encryption and LSB embedding	45.03	38.03	1 bpp
2	Sun (2016)	edge based image steganography with 2kcorrection	61.96	23.15	3bpp
3	Kanan and Nazeri (2014)	Chromosome representation and LSB embedding	54.25	32.92	1bpp
4	HayatAl-Dmour and AhmedAl-Ani (2016)	Edge identification and XOR	56.12	31.31	3bpp
5	Al-rahal, Sen, and Basuhil (2016)	LSB embedding and 3DES	64.42	21.96	1bpp
6	Alsarayreh et al. (2017)	Exact Matching and random key dependant	Infinite	Zero	Unlimited
7	Harianto Antonio (2017)	Exact Matching key dependant and AES encryption	Infinite	Zero	Unlimited

Table 7 Comparative results of Current Best Solution and Proposed Method

Features	Current Best Solution	Proposed Method
Payload capacity	Increase payload capacity	Increase payload capacity
Channel Values	Using only blue color	Using the three color values
Image quality	Not reduced	Not reduced
Key Security	Not secure	More power security because of using AES algorithm in encryption the generated keys
Key Size	Lesser size than the proposed method	Generate more keys
Matches locations	The current best solution can find less matches location than the proposed method because of using only blue channel in the matching process	The proposed method finds more matches location in three times because of using three channel values instead of using one channel value
Hidden data	Less data hidden because of using one channel value	More data can be hidden because of using three channel values means 3 times more than the current best value this means more data can be stored in the image by using the proposed method
Time	More consumed time	Less consumed time

is occurring when the entire color channels are used for finding the matches instead of only using one color channel. It also shows that the proposed method has more possible matches value than the current method.

From the Table 4, the results of the experiment are shown, based on search time in millisecond (ms). It shows that the proposed system higher speed in finding the matches compared to the current system. The proposed system does not require high computational power and can find the matches quickly. Figure 7 shows that there is a significant gap between the proposed method and the current system in terms of search time. The reason that the proposed system having faster speed is that in the current method, the process scans the pixels for the entire image for every character in the secret image and saves the pixel location in the array. Then, it will randomly choose one pixel location for key construction. By doing this, it consumes a lot of time if the secret message is long. Therefore, the proposed method will only use the first matching pixel location for key generation and in the matching process; after the match has been found, it will skip to the next character of the secret message instead. Thus, it reduces computational complexity and saves time.

From Table 5 and Fig. 8, it's shown that the proposed system produces a larger key size than the current system. It happens because in the proposed system the key will be encrypted with AES encryption, but it is a good trade off because it provides more security and also the proposed system has a large payload capacity.

Table 6 shows the comparison between the proposed method and other Steganography systems. It shows that the proposed method maintains the image quality and also has large payload capacity. The result is considered very promising, due to having a great payload capacity, high image quality, and low time consumption, and it also secures the key with encryption before sending it to the receiver. Furthermore the Table 7 shows the Comparative results of Current Best Solution and Proposed Method.

5 Conclusion

The result above shows the difference in the number of possible matching values according to the ASCII number between the current method and proposed method. The result shows that the proposed method improves the possible matching numbers as well as the security of the generated key.

In conclusion, by using the entire color channels to find the matching value, it improves the possibility of the match. The AES also helps secure the generated key to secure the integrity of the exchanged information from third-parties. The limitation of the proposed method is that the matching value is still limited to the color distribution of the cover image. If the matches cannot be found, then the system will not be able to produce the key.

Considering the limitations, future research should investigate the possibility to produce the key from the cover image when the matching value cannot be found. Future research can also increase the security, availability, and also robustness to improve the method.

The proposed method and the current method have been examined by using NetBeans 8.2 and it has been demonstrated that the proposed method is capable of more matching values than the current method. The key produced by the proposed method is also more secure from third parties than the current method.

Acknowledgements We are grateful to Miss. Rasha S. Ali for proof reading and making corrections to this article. Without her support, it would have not been possible to submit this in the current form.

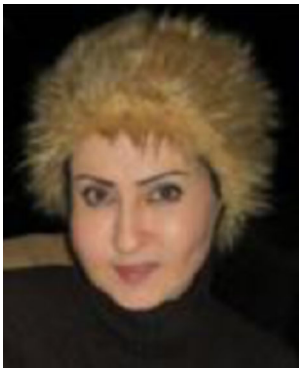
References

1. Abdelmgeid AA, Tarek AA, Al-HussienSeddik S, Shaimaa MH (2016) New image steganography method using zero order hold zooming. International Journal of Computer Applications 133:27–31
2. Alamsyah MMA, Prasetiyo B (2015) Data hiding security using bit matching-based steganography and cryptography without change the stego image quality. Journal of theoretical and applied information technology 106–112
3. Al-Dmour H, Al-Ani A (2016) A steganography embedding method based on edge identification and XOR coding. Expert systems with applications 293–306
4. Al-rahal M, Sen AA, Basuhil AA (2016) High level security based steganoraphy in image and audio files. Journal of theoretical and applied information technology 29–37
5. Alsarayreh MA, Alia MA, Maria KA (2017) A novel image steganographic system based onexact matching algorithm and key-dependent data technique. Journal of theoretical and applied information technology 1212–1224
6. Chen WJ, Chang CC, Le TH (2010) High payload steganography mechanism using hybrid edge detector. Expert Systems with Applications, 3292–3301
7. EL-Emam NN (2007) Hiding a large amount of data with high security using steganography algorithm. Journal of computer science 223–232
8. Eng PMKM, Abdulhameed Z (2014) High capacity steganography based on chaos and contourlet transform for hiding multimedia data. Int J Electron CommEngTechnol (IJECET) 5:26–42
9. Fakhredanesh M, Rahmati M, Safabakhsh R (2013) Adaptive image steganography using contourlettransform. J Electron Imaging 22:043007
10. Jung KH, Yoo KY (2014) Data hiding using edge detector for scalable images. Multimedia Tools and Application 1455–1468
11. Kanan HR, Nazeri B (2014) A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm. Expert Systems with Applications 6123–6130
12. Mohamed MH, Mohamed LM (2016) High capacity image steganography technique based on LSB substitution method, Applied Mathematics & Information Sciences. Appl Math Inf Sci 10(1):259–266

13. Muhammad K, Sajjad M, Mehmood I, Rho S, and Baik SW (2016) A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimedia Tools and Applications 14867–14893
14. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M (2017) CISSKA-LSB: color image steganography using stegokey-directed adaptive LSB substitution method. Multimed Tools Appl:8597–8626. https://doi.org/10.1007/s11042-016-3383-5
15. Nguyen TD, Arch-int S, Arch-int N (2015) A novel secure block data-hiding algorithm using cellular automata to enhance the performance of JPEG steganography. Multimedia tools and applications 5661–5682
16. Nguyen TD, Arch-int S, Arch-int N (2016) An adaptive multi bit-plane image steganography using block data-hiding. Multimedia tools and applications 8319–8345
17. Parah SA, Sheikh JA, Hafiz AM, Bhat G (2014) Data hiding in scrambled images: a new double layer security data hiding technique. Comput Electr Eng 40:70–82
18. Sabeti V, Samavi S, Shirani S (2013) An adaptive LSB matching steganography based on octonary complexity measure. Multimedia Tools and Application:777–793. https://doi.org/10.1007/s11042-011-0975-y
19. Sun S (2016) A novel edge based image steganography with 2kcorrection and Huffman encoding. Information Processing Letters 93–99
20. Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recognition 671–683

Harianto Antonio has received his master of information technology, majoring in Network Security from Charles Sturt University in 2017. His research interests are in the areas of network security, pattern recognition and artificial intelligent. He is working as a Systems administrator in one of the leading IT Company in Australia.

Dr. P.W.C. Prasad is an Associate Professor with the School of Computing and Mathematics at Charles Sturt University, Australia. Prior to this, he was a lecturer at the United Arab Emirates University in UAE, Multimedia University in Malaysia and also the Informatics Institute of Technology (IIT), Sri Lanka. He gained his undergraduate and postgraduate degrees from St Petersburg State Electrotechnical University in the early 90s and completed his PhD studies at the Multimedia University in Malaysia. He is an active researcher in the areas of computer architecture, digital systems, and modeling and simulation". He has published more than 130 research articles in computing and engineering journals and conferences proceedings. He has co-authored two books entitled 'Digital Systems Fundamentals' and 'Computer Systems Organization and Architecture' published by Prentice Hall. He is a senior member of the IEEE Computer Society.



Dr Abeer Alsadoon has academic experience includes working as an associate IT course coordinator and IT lecturer at Charles Sturt University (CSU), Sydney (2012 – up to now), Researcher in e-health research group in CSU, Bathurst. She gained her Post-Doctorate from University of Technology, Sydney (UTS). She received her Ph.D. and Master Studies from the University of Technology, Baghdad in Iraq. She is holding a Certified Associate Project Manager (CAPM) from Canada. Dr. Abeer's Biography is available in "Who's Who in the World" book that is published in America. It includes the recognized people Biographies in the world. She has significant passion in research and teaching. Dr. Alsadoon has published more than 65 IEEE Conferences and 7 Journal papers Level Q1 & Q2, mainly in Medical Engineering, e-Health, and Bioinformatics.