Image Anal Stereol 2017;36:15-23 doi: 105566/ias.1482
Original Research Paper

CLSM: COUPLE LAYERED SECURITY MODEL A HIGH-CAPACITY DATA HIDING SCHEME USING WITH STEGANOGRAPHY

CEMAL KOÇAK
Gazi University, Faculty of Technology, Department of Computer Engineering, 06500, ANKARA
e-mail: ccckocak@gazi.edu.tr
(Received February 12, 2016; revised December 21, 2016; accepted February 1, 2017)

ABSTRACT

Cryptography and steganography are the two significant techniques used in secrecy of communications and in safe message transfer. In this study CLSM – Couple Layered Security Model is suggested which has a hybrid structure enhancing information security using features of cryptography and steganography. In CLSM system; the information which has been initially cryptographically encrypted is steganographically embedded in an image at the next step. The information is encrypted by means of a Text Keyword consisting of maximum 16 digits determined by the user in cryptography method. Similarly, the encrypted information is processed, during the embedding stage, using a 16 digit pin (I-PIN) which is determined again by the user. The carrier images utilized in the study have been determined as 24 bit/pixel colour. Utilization of images in .jpeg, .tiff, .pnp format has also been provided. The performance of the CLSM method has been evaluated according to the objective quality measurement criteria of PSNR-dB (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index). In the study, 12 different sized information between 1000 and 609,129 bits were embedded into images. Between 34.14 and 65.8 dB PSNR values and between 0.989 and 0.999 SSIM values were obtained. CLSM showed better results compared to Pixel Value Differencing (PVD) method, Simulated Annealing (SA) Algorithm and Mix column transform based on irreducible polynomial mathematics methods.

Keywords: cryptography, decryption, encryption, high-capacity data hiding scheme, image processing, steganography.

INTRODUCTION

Cryptography is the science of making changes in the data which is intended to be embedded in mathematical techniques in order to protect it against attacks and make it safe. Cryptography originates from the Greek words “κρυπτός, Kryptos, "Hidden / Secret" and γράφειν, graphein, "writing". The original message to be encoded is called the “Plain Text”, the message obtained at the end of the *conversion* is called the “Cipher Text”, the coding of the message during the *conversion* is called the “encryption” and the reversal process of this is called the “decryption” (Menezes *et al*., 1996; Seth *et al*., 2010; Stallings, 2010; Narayana and Prasad, 2010; Nivedhitha and Meyyappan, 2012). The AES – Advanced Encryption Standard method is the one used most in cryptography method. AES is the symmetric key block encryption which has a higher performance in terms of safety and speed, known as standard Rijndael algorithm (Lie and Chang, 1999; Lee and Chen, 2000; Lou and Liu, 2002; Chan and Cheng, 2004; Wu *et al*., 2005; Yang *et al*., 2008; Seth *et al*., 2010; Sarmah and Bajpai, 2010). One of the most significant issues with the modern cryptography is the distribution of the keys. In order to provide the communication of two users physically too far away from each other and who are willing to establish a safe communication over a common and secret key known by the two only; key distribution protocols are used. There are two different encryption methods in obtaining the key;

- Symmetric Key Encryption
- Asymmetric Key Encryption

Symmetric key algorithms use a common key for encryption and decryption processes, whereas two keys are used in asymmetric key algorithms: one of the keys is used to encrypt the plain text and the other is used to decrypt the encrypted message body. One of these keys is published, the other is hidden. This technique has significantly slower information flow

rate comparing to the symmetric key technique (Petitcolas *et al*., 1999; Piyush and Paresh, 2010; Phad *et al*., 2012; Sreelatha *et al*., 2012).

Steganography however is an art and science of hiding the message and writing a hidden text where nobody, apart from the sender and the receiver, knows that there is a hidden message. Steganography originnates from the Greek words "στεγανός" steganos, "covered or protected", and "γραφή", graphei, "writing or graph" and means hidden writing. Covered writing is also used as the full meaning of the steganography. In this context, the medium in which the information is hidden is called *cover-data*, the medium formed *stego-text* or *stego-object*. The aim of the steganography is to hide the existence of a message and form a covert channel, and it can be seen as a part of the cryptology which aims to hide the contents of the message. The most common of the practical methods of steganography is to use the LSB – *Least significant Bit* method to hide the message and is known as LSB adding. In this method, the bits of the data that is intended to be hidden are placed in order on the least significant bits of each byte of each pixel forming the cover object (image, video, etc.). Here, as maximum one bit of the eight bits is changed and the bit that is changed, if any change is made, is the least significant bit, the changes formed in the steganogram (= Cover data + Embedded data) will be undistinguishable in human eye. In order to embed hidden data on the limited cover-image of large data, more than one LSB should be used. Recently, many suggestions have been made using two or more LSBs to embed the hidden information (Petitcolas *et al*., 1999; Provos and Honeyman, 2003; Seth *et al*., 2010; Narayana and Prasad, 2010; Usha *et al*., 2011). On the studies made where cryptography and steganography are used in connection; DES – Data Encryption Standard algorithm is used in encryption, 3-bit LSB method for steganography (Seth *et al*., 2010), and AES algorithm is used to encrypt the message, and in a study in which multimedia stegano-cryptic method is used, however, the information which has been encrypted using an asymmetric key encryption is hidden in a image file (Piyush and Paresh, 2010). On these studies made using different encryption methods, Peak Signal-to-Noise Ratio (PSNR-dB) and Structural Similarity Index – SSIM were not used in the performance evaluation methods. On the steganography application where edge masking effect is not good enough despite advanced LSB algorithm being used and image was used as the hidden data, PSNR values of 33 dB – 43 dB were obtained (Lie and Chang, 1999). On the study where a randomly chosen 16-digit encryption algorithm was used (Nath and Nath, 2011), however, the size of the image hidden was given but performance evaluation (PSNR – SSIM etc.) was not performed. On the study in which 128-bit encryption Pixel Value Differencing (PVD) using AES algorithm and LSB methods were used, PSNR values of 38.25 dB – 43.96 dB were obtained and lesser data in various volumes were embedded in RGB channels (Phad *et al*., 2012). On the study where variable size LSB was suggested however, PSNR values of 31.75 dB – 32.57 dB (Lee and Chen, 2000) were obtained using grey-scale images and on another study where 775,220-bit data on average were embedded PSNR values of 39.12 dB were obtained (Yang *et al*., 2009).

On the experimental studies information varying in size between 1000-609,129 bits were encrypted and embedded in the colour carrier images. Yet again, in contradistinction to the said studies, the PSNR and the SSIM values belonging to the G and B channels of the images were given in a graph. On the next parts of the study, these subjects will be handled in order: information on suggested materials and method. Experimental results are provided in section Results, followed by discussion of the results in section Discussion and conclusions being drawn in section Conclusions.

MATERIALS AND METHODS

On this study detailed below, high security CLSM – Couple Layered Security Model was suggested which combines cryptography and steganography for secret data and the application was performed. The main parameter used for the storage of the information and adjustment of the security level in modern cryptography is the keys and length of the keys. For the first security model, text encryption was performed using AES algorithm with an encryption coded to be maximum 128-bit long. On the encrypted text embedding stage, as the second security layer, embedding in the image was performed with an encryption maximum 128-bit long which would again be determined by the user (Fig.1).

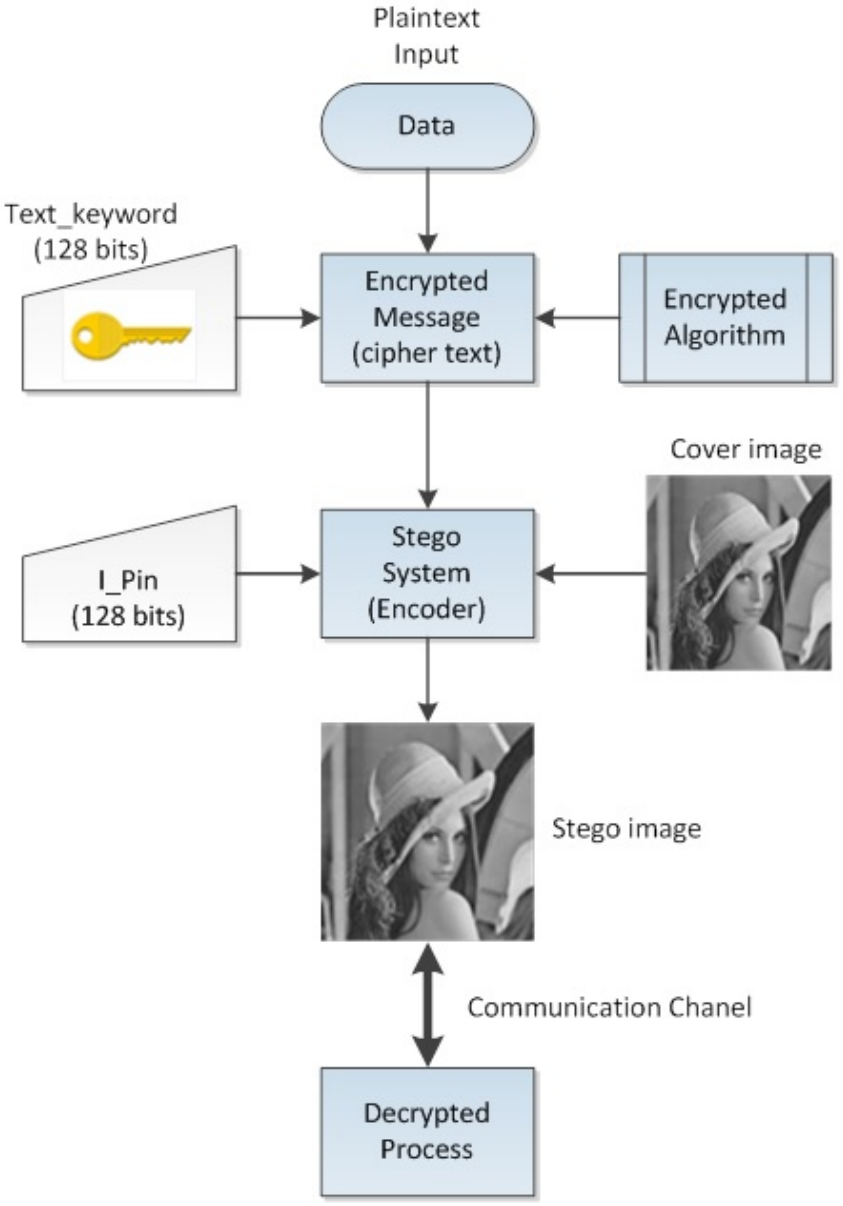

Fig. 1. Proposed *CLSM – Couple Layered Security Model Procedure.*

In order to embed more encrypted data and obtain lesser degeneration in the image, embedding was performed by changing 2 least significant bits (4 in total) of the Green and Blue (G and B) channels of the cover-image RGB channels through a K-bit LSB algorithm. Sensing of the colours is related to the amount of light in a given wave length. The human eye detects light whose wave length is between 370-770 nm. The linear order of the wave lengths forms the colour spectrum. The colour sense which these wave lengths form in the visual system are red - 620 nm, green - 530 nm and blue - 470 nm of the spectral colours. The detection of the spectrum is called spectral sense (Griffin, 2009). In addition, the number of color sensors (cones) is different from the number of luminance sensors (rods) in the human eye (rods > cones). Thus, the light sensitivity and color sensitivity of the human vision system (HVS) are different from each other (Yalman and Erturk., 2013; Koçak, 2015). In consideration of the spectral sensitivity of the eye, the Green (G) and the Blue (B) bits of the image, which are low, are used and by reasons of the sensitivity in the red colour, the R channel was not used.

With the Couple Layered Security Model (CLSM), it is aimed to prevent problems such as unauthorized access and invasion of the information and to provide top level information security. The graphical interface of the application carried out using Visual Studio.Net® is shown in Fig.2.

Fig. 2. *Selection of the text to be encrypted and cover image in which the encrypted text to be embedded.*

Initially, the message is encrypted using Symmetric Key Encryption method which is a well-known concept of encryption. In symmetric key encryption a key is needed for the encryption and the same key is used to decrypt the encrypted text. In order to provide a strong and reliable encryption, level encryption is used. The text is first encrypted using a maximum 128-bit keyword. In the encryption algorithm the user is asked to enter the text to be encrypted and a key. The key can be 16-digit (128 bits), variable length, any number, and letters of the alphabet or special characters. In the plain text to be encrypted, every character of the text, depending on the keyword entered, is replaced by another character. This replacement is performed through the numerical values (ASCII) of the characters. ASCII is a coding standard used to show data on the computer network systems. The encrypted text is formed by means of performing an XOR process in the codes (ASCII) of every character of the text and next character code (ASCII) of the keyword.

Used in the One-Time Pad (OTP) encryption method, encryption is done using a randomly generated sequence of characters. In order to make a strong encryption there should be letters, numbers and special characters in the 16-character keyword. To encrypt plain text data, an equal length key sequence is used. The key is used by mixing (XOR-ing) bit by bit, always adding one bit of the key with one bit of the plain text to create one bit of cipher text (Fig.3). This cipher text is then sent to the receiver. At the receiver's end, the encoded message is mixed (XOR-ed) with the duplicate copy of the One Time Key and the plain text is restored. The security of OTP encryption method depends on randomly generated sequence. This system provides excellent privacy. OTP is used to encrypt the information since it offers provides high security compared to other methods. Key to provide excellent privacy series must be used once only (Menezes *et al*., 1996; Bruce, 2007; Alavi-Milani *et al*., 2012; Widiasari, 2012).

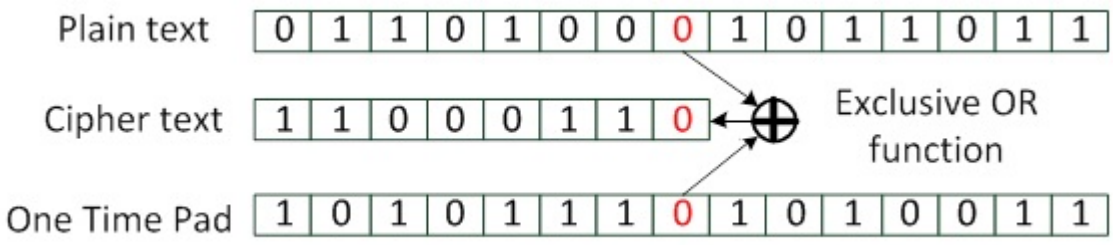

Fig. 3. *One Time Pad (OTP) encryption algorithm method.*

This system can be interpreted as follows:

$c_i = p_i \oplus k_i$

pi = *(i)th binary equivalent of the plain text*

ki = *(i)th binary equivalent of the keyword*

ci = *(i)th binary equivalent of the chipper text*

$\oplus$ = *exclusive-or (XOR) process.*

In this way, as a result of the XOR process of the values of the plain text and the key, the cipher text is formed. For the decryption purposes, XOR process is again applied on the same bits.

$$c_i = p_i \oplus k_i$$

The reasons for selecting XOR process in encrypting characters;

- In order to obtain the original character using again the XOR process on the encrypted character with the same key
- There is no overflow during the encryption

That is, when an ASCII value of a character is XORed with an ACSII value of another character, the resultant value is between 0-255, that is an ASCII value of another character. After performing data encryption, the encrypted message will have been embedded into the cover-image using again a 128-bit encryption on a K-bit LSB substitution method. Therefore, the text encrypted with the keyword will have been embedded into the image using another encryption. One of the most used techniques in steganography is the LSB method. In this study a 4-bit substitution has been made using only the 2 least significant bits of the G and B channels of the RGB channels.

*MaxBytes =[{image (height(…)*width(…)*2*2}/8],*

786,432 bits of information, at the most, can be embedded into a 24-bits, 512*512 pixel image using LSB (3-bits). Through the LSB (GB-4 bits) used in the CLSM method, **1,048,576** bits can be embedded into the same image. The difference in between is **262,144** bits (32,768 bytes). This method has increased the capacity of the secret information in the cover-object. As the colour spectrum in the 24-bit colour images is wider, the substitutions are not big enough to be sensed by human eye. Even though the 128-bits encryption is decrypted using the steganographic techniques to take the message out of the stego-object, there is still a need for the 128-bit encryption (I_PIN) key to decrypt the encrypted message.

RESULTS

With the CLSM data hiding system, the text is encrypted and embedded in images in real colour RGB images and tested. In the experimental studies 512*512pixel, 24-bit colour cover images have been used and two of these are shown in Figs. 4a-b and stego-images obtained using the CLSM method are shown in Figs. 4c-d. Images used; Baboon, Tiffany, Airplane, House, San Diego, the cover images are in Microsoft bitmap (.bmp) file format.

In measuring of the image quality, the results should be compared to the original images. The PSNR has been used in the past as a reference criterion. The measurement unit of the PSNR is decibel (dB). Larger PSNR values mean better signal restoration. The SSIM is an alternative, newer criterion used in the measurement of image quality. The PSNR and the SSIM measurements will be used in the measurement of the visual differences between the original image and the stego image. On the comparisons, a SSIM value of 1 means that both images are the same (Wu *et al*., 2005; Chen *et al*., 2008; Lusson *et al*., 2013). On the other hand, PSNR-HVS and PSNR-HVS-M metrics taking into account some of important characteristics of human visual system (HVS) are the recently introduced criteria that measures the quality of the images (Wang *et al*., 2004; Ponomarenko *et al*., 2011; Rubel *et al*., 2015; Fu and Wang, 2016). The varieties of research showed that the HVS was more sensitive for high frequency distortions than conventional approaches (Wang *et al*., 2004; Egiazarian *et al*., 2006; Ponomarenko *et al*., 2007; Ponomarenko *et al*., 2011; Zhang *et al*., 2011; Rubel *et al*., 2015). The HVS is basically modified version of PSNR and could be stated as follows:

$PSNRHVS = 10 \log_{10} (255^2/MSE_{HVS})$ and

$PSNRHVSM= 10 \log_{10} (255^2/MSE_{HVS\text{-}M})$

(PSNRHVS-M 2006; Egiazarian *et al*., 2006; Ponomarenko *et al*., 2007; Ponomarenko *et al*., 2011).

The MSE_{HVS} and $MSE_{HVS\text{-}M}$ are mean square errors (MSE) reproduced by considering characteristic of HVS (Egiazarian *et al*., 2006; Ponomarenko *et al*., 2011).

(a) (b)

(c) (d)

Fig. 4. *Cover Images: (a) Lena and (b) Peppers. Two stego images Created by CLSM approach: (c) Lena (embedded data are 500,000 bits, PSNR_G 33.33dB, PSNR_B 33.37dB; P-HVS-M 37.71dB, P-HVS 33.67dB; SSIM_G channel 0.9945, SSIM_B channel 0.9875); (d) Peppers (embedded data are 500,000 bits, PSNR_G 30.85dB, PSNR_B 33.34 dB; P-HVS-M 33.87dB, P-HVS 30.65dB; SSIM_G channel 0.9951, SSIM_B channel 0.9923).*

In graphs in Fig. 5, the PSNR (a), the HVS (b) and the SSIM (c) values which were obtained against the information encrypted in various sizes and embedded in Lena are shown. As it can be easily seen that there are magnificent the SSIM values and good the HVS values.

When embedded bits are increase from 1,000 bits 500,000 bits, the PSNR in Green Blue channel have decrease from 63.33–65.80 dB to 33.37–33.33 dB. So that means overall performance have decreased 47.3%–49.3% percent Fig. 5a. On the other hand, distortions in HVS Lena is 1.84% percent (from 38.58 to 37.87 dB). Consequently, HVS measure confirm that proposed method is quite robust to number of bits embedded in to image. As could be seen in Fig. 5b.

For Lena, it is seen that the PSNR and HVS values have decreased based on the increase in the information embedded (Figs. 5a-b). While this value is 0.99 for SSIM_G channel, even though this value decreases to 0.98 levels for SSIM_B channel after 500,000 bits good quality the SSIM values have been obtained Fig. 5c.

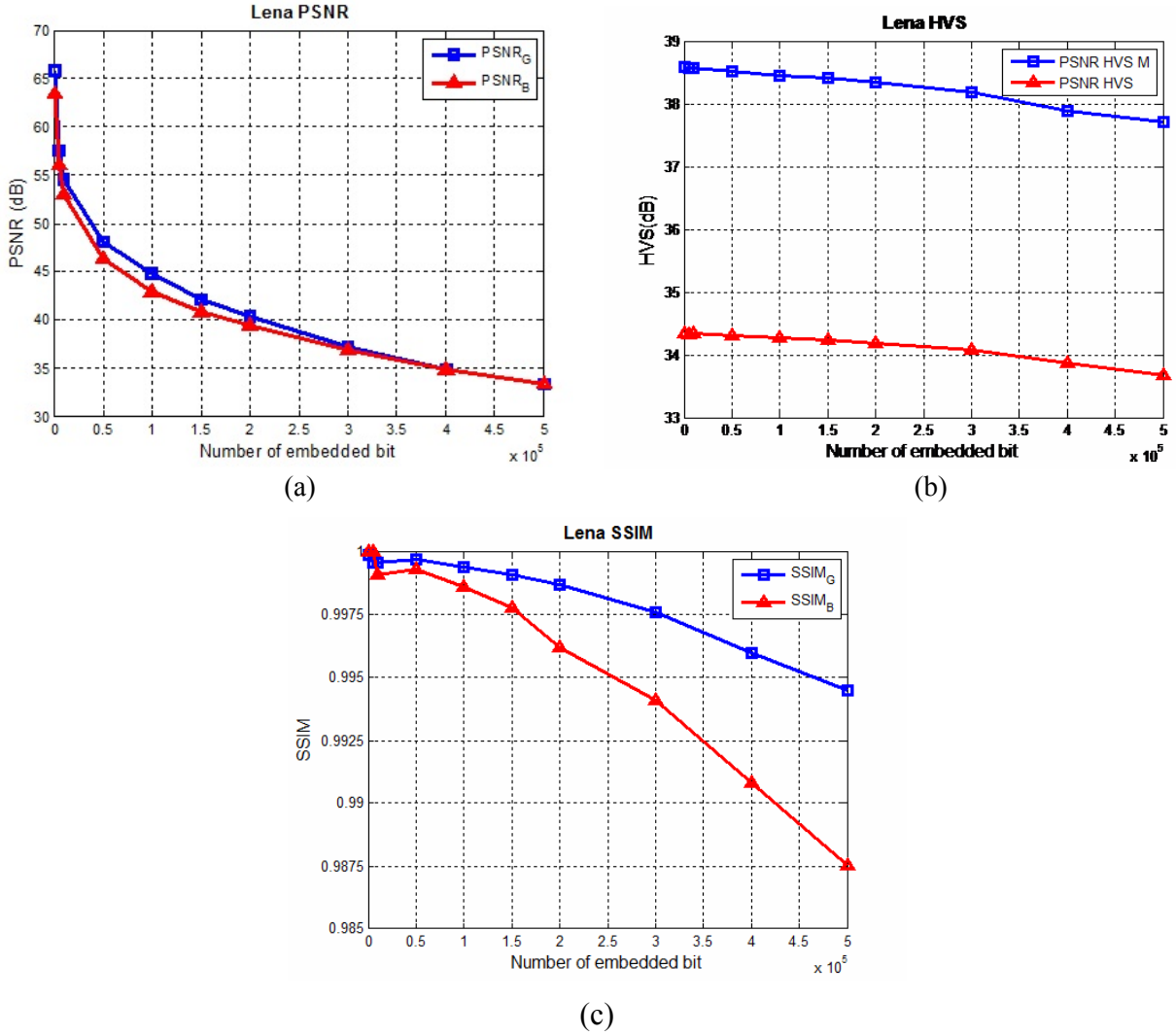

Fig. 5. *Results of the PSNR (a), the PHVS, PHVSM (b) and the SSIM (c) against different embedding capacity for Lena.*

DISCUSSION

In Steganography one of the main objectives to increase the capacity of the data to be hidden into stego-images and the value of PSNR, PHVSM, PHVS. However, a balance between "high capacity" and "high PSNRM" must be provided. PSNR/PHVSM/PHVS/ SSIM comparison between the proposed CLSM and the other studies is shown in Table 1. As seen in Table 1, two different PSNR values 42.26 dB (Mandal and Das, 2012) and 43,624 dB (Koçak, 2015) were obtained in studies with 145,787 bits of embedded data. A higher rate of PSNR value 44.883 dB and of PHVSM value 37.76 dB, PHVS value 33.90 dB were obtained in proposed CLSM. In raw 2, PSNR values 27.03 dB (Lin *et al*., 2010) and 31.982 dB (Koçak, 2015) were obtained in studies with 53,248 bits of embedded data. A higher rate of PSNR value 39.844 dB and of PHVSM value 42.36 dB, PHVS value 35.02 dB were obtained in proposed CLSM.

Similarly, better HVS and similarity performance were obtained by the proposed CLSM method compared to other methods given in Table 1. In this study, for embedded hidden message of maximum 1,043,608 bits PSNR(G) 28.642 dB, PSNR(B) 29.111 dB, and PHVSM 36.57 dB, PHVS value 32.49 dB and SSIM(G) 0.984, SSIM(B) 0.966 were obtained. As seen in row 4 in Table 1, 58% more capacity in terms of hidden data and a good SSIM was obtained via slightly lower PSNR, PHVSM and PHVS value. Comparisons show that, proposed CLSM method has better PSNR, HVS and SSIM values. At the same time capacity increase was achieved with a little deterioration in the stego images.

Table 1. *PSNR/HVS/SSIM comparison between the proposed CLSM and the other studies.*

	Test image	Embedded Data (Bits)	PSNR (dB)	Proposed CLSM					
				PSNR (dB)		PSNRHVS (dB)		SSIM	
				G	B	PHVSM	PHVS	G	B
Mandal and Das Koçak	Lena	145,787	42.26 43.62	44.88	42.27	37.76	33.90	0.99	1.00
Lin *et al.*'s Koçak	Barbara	53,248	27.03 31.98	39.84	39.83	42.36	35.02	0.99	0.99
Abduallah *et al.*'s Koçak	Lena	609,129	32.70 33.13	34.15	34.14	37.42	33.38	0.99	0.98
In the study	Lena	1,043,608		28.64	29.11	36.57	32.49	0.98	0.96

CONCLUSION

On the applications where the steganographic techniques would be insufficient, utilizing of cryptographic techniques as well will enhance the security. On the suggested CLSM method the data embedding has been taken up to top level by means of combining cryptographic and steganographic techniques. Encryption was made using a 16 character (128-bit) keyword which provides a higher security for secret information and embedding was performed with a 16-character (128-bit) I_PIN. In order to embed encrypted secret message in a cover image, more information has been embedded using a 2-bit LSB substitution method for G and B channels. Out of the experimental results, better image quality has been obtained with the suggested approach, in terms of similarities in the original image and the stego-images in return for the higher capacity secret information.

ACKNOWLEDGMENTS

Author would like to thank Prof. Dr. Recep DEMIRCI for his image processing software called MedPic which was used in this study and Sercan ALTAS for study supports.

REFERENCES

Abduallah WM, Rahma AMS, Pathan ASK (2014). Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach. Comput Electr Eng 40:1390–404.

Alavi-Milani MMR, Pehlivan H, Hosein-Pour S (2012). OTP (One Time Pad) tabanlı DNA şifreleme yöntemi. Akademik Bilişim'12, XIV. Akademik Bilişim Konferansı Bildirileri 1–3 Şubat 2012 Uşak Üniversitesi.

Bruce S (2007). Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, Inc.

Chan CK, Cheng LM (2004). Hiding data in images by simple LSB substitution. Pattern Recogn 37:469–74.

Chen YY, Chang YW, Yen WC (2008). Design a deblocking filter with three separate modes in DCT-based coding. J Vis Commun Image R 19:231–44.

Egiazarian K, Astola J, Ponomarenko N, Lukin V, Battisti F, Carli M (2006). New full-reference quality metrics based on HVS. In CD-ROM proceedings of the second international workshop on video processing and quality metrics, Scottsdale, USA, 2006, 4 p.

Fu Y, Wang S. (2016). No-reference image quality assessment based on HVS. International symposium on computer, consumer and control (IS3C), 2016 Xi'an, China July 4-6, 1093–6.

Griffin AL (2009). Color, mapping. International encyclopedia of human geography, Elsevier UK, 195–201.

Koçak C (2015). High-capacity data hiding scheme together using cryptography and steganography. Erciyes U J Inst of Sci Technol 31:115–23.

Lee YK, Chen LH (2000). High capacity steganographic model. P IEE Vision, Image and Signal Process 147: 288–94.

Lie WN, Chang LC (1999). Data hiding in images with adaptive numbers of least significant bits based on the human visual system. Image Process, ICIP 99. Proc Intern Conf, Kobe, Japan Oct. 24-28, 286–90.

Lin GS, Chang YT, Lie WN (2010). A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm. Multimedia, IEEE Trans 12:345–57.

Lou DC, Liu JL (2002). Stenographic method for secure communications. Comput Secur 21:449–60.

Lusson F, Bailey FK, Leeney M, Curran K (2013). A novel approach to digital watermarking, exploiting colour spaces. Signal Process 93:1268–94.

Mandal JK, Das D (2012). Colour image steganography based on pixel value differencing in spatial domain. Int J Inform Sci Tech 2:83–93.

Menezes AJ, Van Oorschot PC, Vanstone SA (1996). Handbook of applied cryptography. CRC press.

Narayana S, Prasad G (2010). Two new approaches for secured image steganography using cryptographic

techniques and type conversions. Signal Image Process: An Int J (SIPIJ) 1:60–73.

Nath J, Nath A (2011). Advanced steganography algorithm using encrypted secret message. Int J Adv Comp Sci Appl 2:19–24.

Nivedhitha R, Meyyappan T (2012). Image security using steganography and cryptographic techniques. Int J Eng Trends Technol 3:366–71.

Petitcolas FA, Anderson RJ, Kuhn MG (1999). Information hiding a survey. IEEE P, special issue on protection of multimedia content 8:1062–78.

Phad VS, Bhosale RS, Panhalkar AR (2012). A novel security scheme for secret data using cryptography and steganography. Int J of Comput Network Inform Secur 4:36–42.

Piyush M, Paresh M (2010). Visual cryptographic steganography in images. Computing communication and networking technologies (ICCCNT), Karur, India, July 29-31, 1–6.

Ponomarenko N, Lukin V, Egiazarian K (2011). HVS-metric-based performance analysis of image denoising algorithms. In Vis Inform Process, 3rd European Workshop on IEEE, Paris, July 4-6, 156–61.

Ponomarenko N, Silvestri F, Egiazarian K, Carli M, Astola J, Lukin V (2007). On between-coefficient contrast masking of DCT basis functions. In proceedings of the third international workshop on video processing and quality metrics, Scottsdale, Arizona, U.S.A, Jan. 13–15.

Provos N, Honeyman P (2003). Hide and seek: An introduction to steganography. IEEE Secur Privacy 1:32–44.

PSNR-HVS-M page: http://ponomarenko.info/psnrhvsm.htm 2006.

Rubel O, Ponomarenko N, Lukin V, Astola J, Egiazarian K (2015). HVS-based local analysis of denoising efficiency for DCT-based filters. Problems of infocommunications science and technology (PIC S&T), 2015 second international scientific-practical conference. IEEE, Kharkiv, Ukraine, Dec. 14, 189–92.

Sarmah DK, Bajpai N (2010). Proposed system for data hiding using cryptography and steganography. Int J Comput Appl, 8:7–10.

Seth D, Ramanathan L, Pandey A (2010). Security enhancement: combining cryptography and steganography. Int J Comput Appl 9:3–6.

Sreelatha M, Ramana KV, Sunitha Ch, Sushma V (2012). Two level data hiding scheme: using shape based cryptography and MIB steganography technique. International conference on computer science and engineering, Vizag, April, 73–7.

Stallings W (2010). Cryptography and network security: Principles and Practices. Pearson Education, Inc., 5th Edn., publishing as Prentice Hall, 2010.

Usha S, Kumal GAS, Boopathybagan K (2011). A secure triple level encryption method using cryptography and steganography. Computer Science and Network Technology (ICCSNT), International Conference on, Harbin, China, 2:1017–20.

Wang, Z, Bovik, AC, Sheikh, HR, Simoncelli, EP (2004). Image quality assessment: from error visibility to structural similarity. IEEE T Image Process 13:600–12.

Widiasari IR (2012). Combining advanced encryption standard (AES) and one time pad (OTP) encryption for data security. Int J Comput Appl, 57:1–8.

Wu HC, Wu NI, Tsai CS (2005). Image steganographic scheme based on pixel-value differencing and LSB replacement methods. IEE P-Vi Image Sign 152: 611–15.

Yang CH, Wang CY, Wang SJ (2008). Adaptive data hiding in edge areas of images with spatial LSB domain systems. IEEE Inform T Forensics Secur 3:488–97.

Yang H, Sun X, Sun G (2009). A high-capacity image data hiding scheme using adaptive LSB substitution. Radio Eng 18:509–16.

Yalman Y, Erturk I (2013). A new color image quality measure based on YUV transformation and PSNR for human vision system. Turkish J Electr Eng Comput Sci 21:603–12.

Zhang, L, Zhang, L, Mou, X, Zhang, D (2011). FSIM: a feature similarity index for image quality assessment. IEEE T Image Process 20:2378–86.