IJCTA, 9(30), 2016, pp. 175-184
© International Science Press

A Combined Crypto-Stego System Using Dynamic Encryption Assisted Intensity Color Steganography

Hayfaa A. Atee* Robiah Ahmad Norliza Mohd Noor** and Abidulkarim K. Ilijan*****

Abstract : Developing a robust crypto-stegosystemforcompactciphering or embedding ofvital data to securely transfer over the open channels is ever-demanding. Present encryption and concealment algorithms suffer from various limitations and often get attacked by the unauthorized users. Thus,it is pertinentto develop new algorithms for greatly secureddata transmission.By combining the notable advantages of existing cryptography and steganography,we propose a new crypto-stegosystem called Dynamic Encryption Assisted Intensity Color Steganography (DEAICS) with extra security.In this system, the dynamic encryption scheme is used for encrypting the data before embedding in the specific intensity color of an image. The results obtained using the proposed techniqueare compared with simple Least Significant Bit (LSB)embedding data (without encryption) in terms of embedding capacity, mean square error (MSE), peak signal to noise ratio (PSNR). Presentcrypto-stego systemis demonstrated to achieve good capacity,imperceptibility, and robustness.The Capacity of the newly proposed DEAICS system is increased by 40% as compared to LSB algorithm without encryption.

Keywords : Cryptography, Steganography, Data Hiding, Spatial Domain, Intensity Color Embedding, Dynamic Encryption.

1. INTRODUCTION

In the present information communication technology (ICT) era, safe mining of sensitive information (data) over the internet and its subsequent conversion appears the major concern worldwide. With the ever escalating demand of the privacy preserved data mining (information transfer) via the Internet, the process of exchanging vast amount of information secretly through open channels become inevitable. Thus, the data confidentiality and integrity requires an absolute protection from unauthorized access and wanton uses. This led to the tremendous growth of developing data hiding algorithm so called robust encryption decryption scheme. Gamut research activities are prompted to invent or develop different methods for encryptingor hiding information. Existing simple techniques are limited because they are easily detectable by steganalysis, thereby defeats the purpose of robust steganogrphic technique.Despite intensive efforts for developing new encrypting and concealment schemes/algorithms a robust technique is far from being achieved.

Cryptography and steganography are widely used techniques that handle information for ciphering or hiding their existence. Steganography is the art and science of communicating the information in a hidden manner[1] so thatthe message remains invisible to the adversaries[2].Conversely, cryptography is the enciphering and deciphering of data and information with a secret code to make the unauthorized users incomprehensible[3]. Figure 1 depicts the combined notions of cryptography and steganography.

* Foundation of Technical Education, Higher Education and Scientific Research, Baghdad, Iraq

** Department of Engineering, UTM Razak School of Engineering and Advanced Technology, UTM Kuala Lumpur, 54100 Jalan Sultan Yahya Petra, Kuala Lumpur, Malaysia

*** College of Engineering, Almuthanna University, Samawa, Iraq

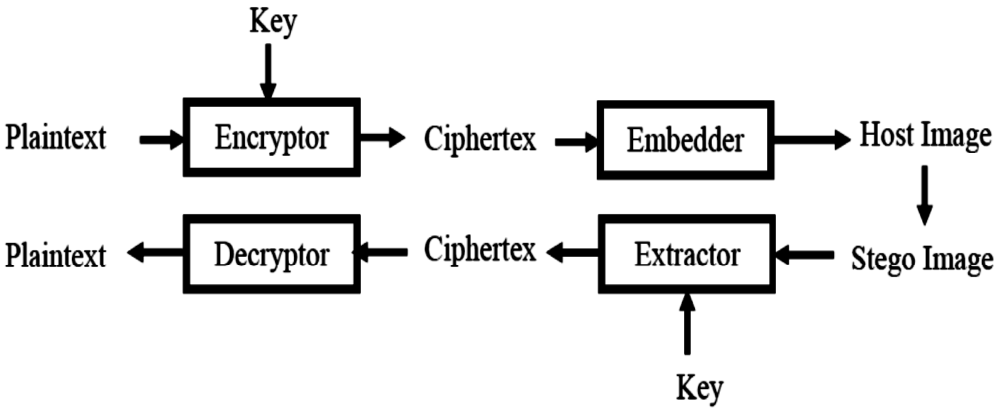


Fig. 1. Architecture of a typicalcrypto-stego system.

Digital information (data)including image, audio, and video files are used as a cover in a technical steganography. Hiding information in an image called image steganography. It is the most popular type because of the large exchange on the Internet. Moreover, it appears common and unsuspicious after the embedding process. In data steganography, the spatial and frequency domain are the two categories used for hiding the information intoan image. The most common approach of hiding in the spatial domain is Least Significant Bit (LSB) method, which is easiest with high capacity. Mean while, discrete wavelet transform (DWT), discrete cosine transform (DCT), and discrete Fourier transform (DFT) are the most common techniques in the frequency domain which are used for hiding the data intoan image.

2. RELATED WORKS

Presently, with the rapid advancement of internet communications network the security appeared a major concern, whereabsolute cyberspace protection against internet phishing is prerequisite. The threat imposed via ever increasing massive phishing or adversaries' attacks with advanced deceptions demanded the development of robust cryptography and steganography systems. The mitigation of internet threats and its significant impacts on global security and economy remains challenging. Strengthening the protection performance against such attacks and unauthorized users interference by reducing the computational costs is the main issue. Cryptography and steganography being the most widely employed techniques to overcome such threat have received focused attention in recent time.These techniques are useful for encrypting and hiding the data. It is realized that by integrating cryptography with steganography it is possible to achieve higher levels of security[4]with safer data transfer capacity [5].

Image steganography uses both the spatial domain and frequency domain for concealing the data into an image. Depending on the demands of high capacity, elevated robustness, and enhanced performance criteria the researcher decided to employthe steganographic technique. The spatial domain is used for gaining high capacity whereas the frequency domain is used for achieving high robustness.Over the years, spatial domain steganography is intensively used for embedding the secret message [6][7][8][9][10][11][12][13]. Nevertheless, frequency domain steganography is also employed for hiding the secret message[1][14][15].Different techniques are used for encrypting the data before embedding it into the spatial and frequency domain as explained hereunder.

Spatial domain Data Encryption Algorithm (DEA)is used[6]to encrypt the data, where the modified bit encoding technique is applied to hide the encrypted data for further security level enhancement. A combined cryptography and steganography technique of is also proposed [7]. In order to raise the security level,the message is encrypted using Playfair cipher and AES algorithm. Then, LSB method is used for embedding the encrypted data.A secure algorithm that provided the best approach for LSB based steganography is obtained by combining the Genetic Algorithm (GA) with Visual Cryptography (VC). It is designed and implemented to ensure the improved security and reliability[8]. Meanwhile, the security features of the steganographic system are highly optimized using a GA.

A hybrid cryptographic algorithm is built by combining Date Encryption Standard(DES) and Rivest Shamir Adleman(RSA) algorithms[9]. The modified Bit Plane Complexity Segmentation(BPCS) steganography technique is used to hide the data.To achieve double level of security, the Vernam cipher is used for encrypting the data and the new LSB-S algorithm is used for embedding the encrypted data into an image[10].The data size is first reduced by compressing and then the compressed data is encrypted using AES algorithm[11]. Finally, the encrypted data is hidden in the image. GA is used for pixel assortment of image where data is to be concealed so that detection of clandestine information becomes multifarious. To increase the security, the AES algorithm is applied for encrypting the data before being hidden using LSB steganographic method[12].The secret message is encrypted by using a new cipher which is extended from Hill cipher[13]. Then, the encrypted message is embedded in the image using LSB, LSB minus 1, and LSB minus 2 bit locations of the darkest and brightest pixels. It is acknowledged that LSB method intend to raise the security level due to its susceptibility against statistical analysis.

The AES algorithm is used in the frequency domain to encrypt a message and a part of the message is hidden in the DCT of an image[1]. To raise the level of security, the remaining part of the message is used to generate two secret keys for achieving strong encryption. The secret message is encoded using Quick Response Code (QR) and DWT is used for embedding the encrypted message into an image[14]. Furthermore, the embedding process is protected by AES to achieve higher level of security. A public-key encryption algorithm (RSA) is used to encrypt the plain text and the DCT is utilized for transferring the image from spatial domain to frequency domain[15]. Despite many efforts, a robust crypto-stego system for accurate ciphering or embedding of central data (information)to securely transfer over the open channels is still to be achieved.

In this view, we proposed a new method by combiningthe security benefits of both cryptography and steganography as one system to achieve high capacity, imperceptibility, and enhanced robustness. Earlier, most researchers combinedthe cryptography and steganography either using the traditional approach or relied on the enhancement or development of anew one. Undoubtedly, enhancing or developing a new technique is always better than using the traditional methods with known functional mechanism and obvious exposures. The proposed integrated system calledDynamic Encryption Assisted Intensity Color Steganography(DEAICS). In this system, data is first encrypted following the earlier scheme [16]. Second, the encrypted data are embedded using the method suggested by Samidha and Agrawal [17]without implementation.The concealment process in DEAICSis performed randomly via specificintensity color of a whole image for hiding the encrypted plaintext into the image. Thus, the changes affected only the selected intensity color so that human eyes are unable to recognize such trivial changes.

This paper is organized as follows. Section 3is explains the detailed methodology of the work. Section 4 outlines the performance measurements. Section 5 presents the results and discusses them. Section 6 concludes the paper.

3. METHODOLOGY

As aforementioned, in the proposed system the data are encrypted using dynamic encryption scheme[16]. Then, the cipher-text are embedded into an image using the steganographic method of Samidha and Agrawa[17]. The encrypted data (cipher-text) is further embedded into a specific intensity color of an image. The DEAICS processes are comprised of three main stages such as encryption, embedment, and extraction. Figure 2 schematically illustrates the basic architecture of the DEAICS algorithm.

One of the major advantages of the proposed system is that if the attacker detects the steganography techniqueit still needsto decode the encrypted message and vice versa, thus make the system robust.The DEAICS is compared together with the embedding the message without encrypting into an image using simple LSB. The scheme of LSB Without Encryption is termed as LSBWE. The following subsections depict the three stages of DEAICS.

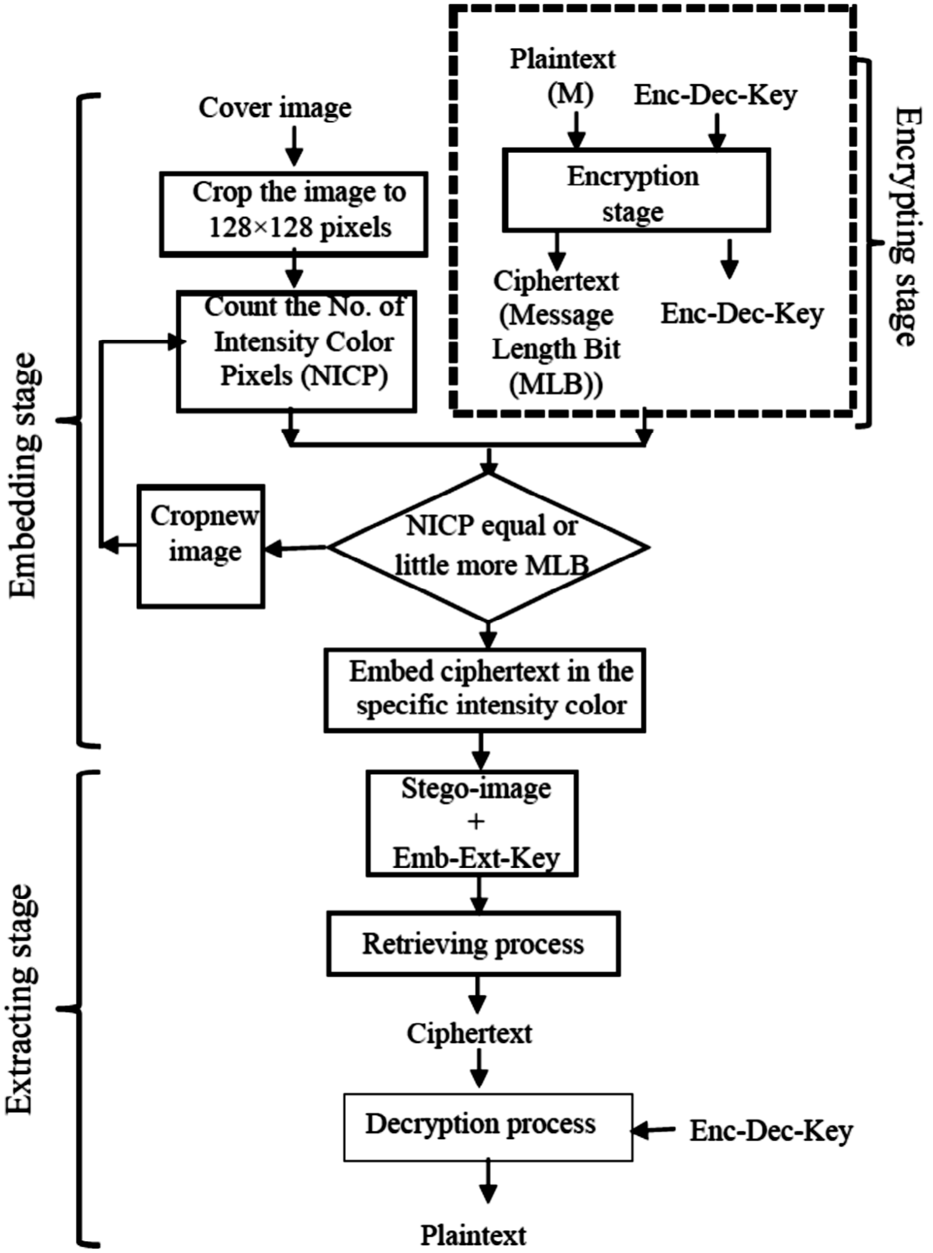

Embedding stage
Cover image
Crop the image to 128×128 pixels
Count the No. of Intensity Color Pixels (NICP)
Plaintext (M)
Enc-Dec-Key
Encryption stage
Ciphertext (Message Length Bit (MLB))
Enc-Dec-Key
Encrypting stage
Cropnew image
NICP equal or little more MLB
Embed ciphertext in the specific intensity color
Extracting stage
Stego-image + Emb-Ext-Key
Retrieving process
Ciphertext
Decryption process
Enc-Dec-Key
Plaintext

Fig. 2. Flowchart for DEAICS algorithm.

3.1. Encrypting Stage

Following the earlier cryptographic method[16], the proposed DEAICS encrypted the plain text.It is worth to mention that DEAICS being a symmetric algorithm used the same key for encryption and decryption operation. The Encryption-Decryption-Key (Enc-Dec-Key) and the plaintext are used to produce the ciphertext.The encryption process begins by assigning a code number for each plaintext character in the message as summarized in Table 1.

The Enc-Dec-Key(Table 1) corresponds to the code number of the first character in the plaintext. Then, it creates the dynamic table (Table 2) which is the first row and column start with the first character in the message and continues alphabetically for other rows and columns. The number of the rows are equal to the number of the plaintext. Afterwards, Table 2is employed to obtain a decimal code values using column numbers that corresponds to each character in the message. Next, each decimal code value is converted to 5 binary bits' code.Finally, the encryption process produced a cipher-text as a stream of binary bits and the Enc-Dec-Key[16].

Table 1. The code numbers andcharacters with English alphabets.

Code Number	*Character*	*Code Number*	*Character*	*Code Number*	*Character*	*Code Number*	*Character*
A	U	21	N	14	G	07	
01	A	08	H	15	O	22	V
02	B	09	I	16	P	23	W
03	C	10	J	17	Q	24	X
04	D	11	K	18	R	25	Y
05	E	12	L	19	S	26	Z
06	F	13	M	20	T	27	SPACE
07	G	14	N	21	U		

Table 2. The dynamic encryption table.

Char. code *Char. code*	*Char. 1*	*Char. 2*	.	.	.	.	.	.	.	.	.	*No. of message char.*
01	.	.	.	.	K	L	M	N	O	.	.	.
02	.	.	.	.	L	M	N	O	P		.	.
03	.	.	.	.	M	N	O	P	Q		.	.
04	.	.	.	.	N	O	P	Q	R		.	.
05	.	.	.	.	O	P	Q	R	S		.	.
06	.	.	.	.	P	Q	R	S	T		.	.
07	.	.	.	.	Q	R	S	T	U		.	.
08	.	.	.	.	R	S	T	U	V		.	.
09	.	.	.	.	S	T	U	V	W		.	.
10	.	.	.	.	T	U	V	W	X		.	.
11	.	.	.	.	U	V	W	X	Y		.	.
12	.	.	.	.	V	W	X	Y	Z		.	.
13	.	.	.	.	W	X	Y	Z			.	.
14	.	.	.	.	X	Y	Z		A		.	.
15	.	.	.	.	Y	Z		A	B		.	..
16	.	.	.	.	Z		A	B	C		.	.
17	.	.	.	.		A	B	C	D		.	.
18	.	.	.	.	A	B	C	D	E		.	.
19	.	.	.	.	B	C	D	E	F		.	.
20	.	.	.	.	C	D	E	F	G		.	.
21	.	.	.	.	D	E	F	G	H		.	.
22	.	.	.	.	E	F	G	H	I		.	.
23	.	.	.	.	F	G	H	I	J		.	.
24	.	.	.	.	G	H	I	J	K		.	.
25	.	.	.	.	H	I	J	K	L		.	.
26	.	.	.	.	I	J	K	L	M		.	.
27	.	.	.	.	J	K	L	M	N		.	.

3.2. Embedding Stage

The embedding process is performed using the following steps:

1. Read the ciphertext and the cover image.
2. Crop the image to size128´128 pixels.
3. Count the number of all intensity color valuesin the cropped image.
4. Choose the pixels that the number of the intensity color value it equal to or little more than the number of message bits.If there is no number of intensity color value pixels satisfy the condition, then make new crop for cover image and continue from step 3.
5. Embed the plaintext into the cropped image in the specific intensity color valuepixels(random embedding).
6. Keep the specific intensity color value and the first index store position of the storing array of the image as theEmbedding-Extracting-Key(Emb-Ext-Key).
7. The stego-image and the Emb-Ext-Keyare achieved.

3.2. Extracting Stage

Extractionphase consisted of two processes including retrieving and decrypting. In the retrieving process, the Emb-Ext-Key and the stego-image is used for retrieving the ciphertext from the image.Then, the Enc-Dec-Key is used for decipheringthe ciphertext via the dynamic encryption schemefollowing decrypting process. Extraction is carried outusing the following steps:

1. Read the stego-image.
2. Usethe Emb-Ext-Key to retrieve the embedding ciphertext.Retrieve the eighth bit from the image pixel according to the specific intensity color value and the first indexstore positions array. The number of retrieved bits must be equal to the number of the number of plaintext character.
3. Split the retrieved stream bits into groups of 5 bits and then convert each 5 bits to decimal value.
4. Use Table 1 to retrieve the first plaintext character that corresponds to the code value of the Enc-Dec-Key.
5. Use the retrieved first plaintext character to create the dynamic table(Table 2).
6. Using Table 2, perform the extraction operation for retrieving each character corresponding to the identical decimal value code from one row of Table 2 and continue sequentially until all plaintext characters are obtained.

4. PERFORMANCE EVALUATION

4.1. Imperceptibility and Robustness Criteria

Peak Signal to Noise Ratio (PSNR) is calculated to determine the quality of stego image with respect to the original image. The PSNR is considered to be the most accurate evaluator index for imperceptibility, which measures the similarity between stego image and original image [18]. A stego image having higher PSNR value indicated better image quality. In other words, it signifies higher imperceptibility of the hidden message behind the pixels of an image. The expression for PSNR yields:

$$\text{PSNR} = 10 \times \log\left(\frac{255^2}{\text{MSE}}\right) \tag{1}$$

where the metric MSE is the Mean Square Error that calculates the magnitude of average error between the original image and stego image. MSE is used to estimate the robustness of the stenographic method, where the differences between the original and stego image are squared and then averaged[19]. MSE is calculated via:

$$\text{MSE} = \sum_{i=1}^{x} \sum_{j=1}^{y} \frac{(|\,\text{A}_{ij} - \text{B}_{ij}\,|)^2}{x * y} \tag{2}$$

where A and B represent the data matrix with *x* and *y* as the number of rows and columns for the original and the cover image, respectively.

4.2. Capacity

By definition, the concealment capacity represents the possible number of bits that can be embedded in an image where only one bit of the ciphertextisused for embedding each pixel into the image. In the LSBW Eembedding method, the plaintext is embedded into the image without encryption. In this technique, the eighth bit (LSB) of the pixel is used to hide the binary stream bits of the plaintext and7 bits are used to represent each character. To determine the maximum capacity the value of LSBWE is calculated using:

$$\text{C}_{\max} = (\text{L} \times \text{W})/7 \tag{3}$$

where L and W are the length and width of the image.

In the proposed DEACIS system, the plaintext is encrypted using dynamic encryption scheme. Then, the ciphertext is embedded in the image, where 5bits are used for presenting each ciphertext character in the image. The maximum capacity is calculated using:

$$\text{C}_{\max} = (\text{L} \times \text{W})/5 \tag{4}$$

5. RESULTS AND DISCUSSION

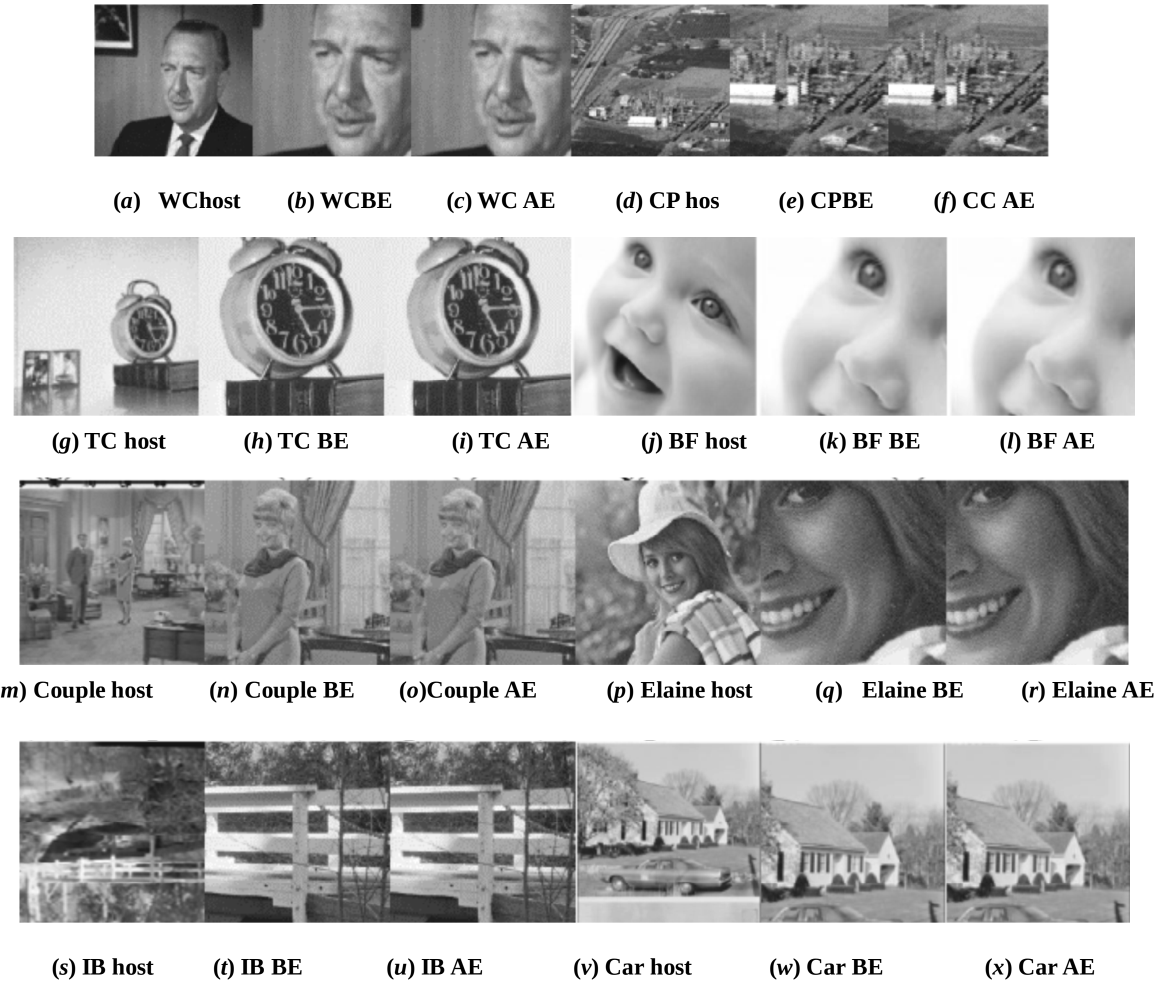
The performance of DEAICS is compared with LSBWE in terms of capacity, imperceptibility, and robustness.Table 3enlists the maximum capacity for different image sizes for the DEAICS including grayscale and color one. In all images, the capacity for DEAICSalgorithms is found to be higher than the capacity of LSBWE method for both grayscale and color one. The observed enhanced capacity achieved by the proposed method is attributed to the usage of5 bits that represented each character. Conversely, LSBWE used 7bits to represent each character.

Table 3. Image pixel size dependent capacity achieved by DEBICS and LSBWE algorithm for gray scale and color host images

Image	*Grayscale*		*Color Images*	
Dimension	*LSBWE*	*DEAICS*	*LSBWE*	*DEAICS*
128 × 128	2341	3277	7022	9830
256 × 256	9362	13107	28087	39322
512 × 512	37449	52429	112347	157286
1024 × 1024	149797	209715	449390	629146

The imperceptibility and robustness performance (PSNR and MSE) of the proposed crypto-stego system (DEAICS) are evaluated using different grayscale as well as color host images and compared with LSBWE algorithm.Figures 3 and 4 show the DEBICS system generated images before embedding (BE) and after embedding (AE) together withthe host images.In all tests, images of size (256 × 256) and (512 × 512) are used with cropped size (128 × 128) to keep the image features.

Eight grayscale images such as Walter Cronkite (WC), Chemical Plant (CP),Table Clock (TC), Couple, Elaine, Iron Bridge (IB), Baby Face (BF), and Car, are used. Likewise, eight color images including Tree, House, Jellybeans, Baboon, Lena and Pepper are used.



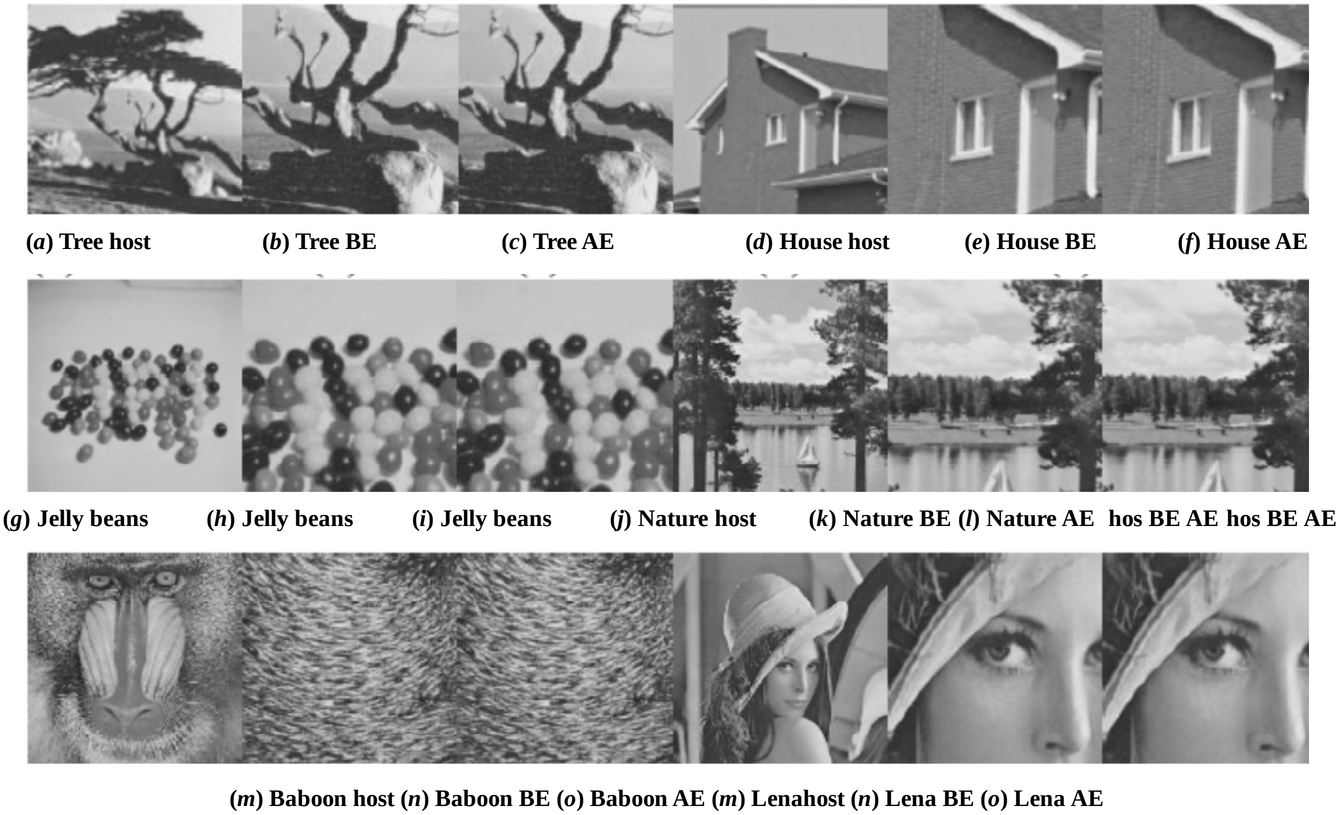
(*a*) WChost (*b*) WCBE (*c*) WC AE (*d*) CP hos (*e*) CPBE (*f*) CC AE

(*g*) TC host (*h*) TC BE (*i*) TC AE (*j*) BF host (*k*) BF BE (*l*) BF AE

(*m*) Couple host (*n*) Couple BE (*o*)Couple AE (*p*) Elaine host (*q*) Elaine BE (*r*) Elaine AE

(*s*) IB host (*t*) IB BE (*u*) IB AE (*v*) Car host (*w*) Car BE (*x*) Car AE

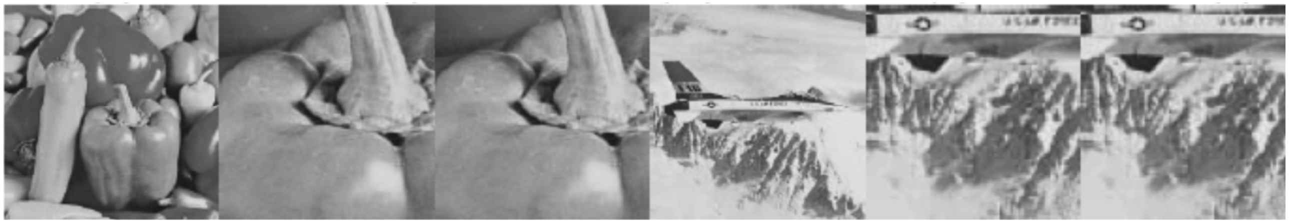
Fig. 3. The eight grayscale images host and, beforeand after embedding using DEBICS.



(*a*) Tree host (*b*) Tree BE (*c*) Tree AE (*d*) House host (*e*) House BE (*f*) House AE

(*g*) Jelly beans (*h*) Jelly beans (*i*) Jelly beans (*j*) Nature host (*k*) Nature BE (*l*) Nature AE hos BE AE hos BE AE

(*m*) Baboon host (*n*) Baboon BE (*o*) Baboon AE (*m*) Lenahost (*n*) Lena BE (*o*) Lena AE



(*p*) Pepper host **(*q*) Pepper BE** **(*r*) PepperAE** **(*v*) F16 host** **(*w*) F16 BE** **(*w*) F16 AE**

Fig. 4. The eight color imageshost and, before and after embedding using DEBICS.

Tables 4 and 5 enlist the PSNR and MSE values for grayscale and color images that are cropped to size (128 × 128). From the results it is evident that the proposed algorithms achieved higher PSNR and lower MSE values for all tested images when than that of LSBWE system.In terms of PSNR and MSE,the proposed algorithm out performed the LSBWE due to its superior hiding characteristics which is represented by 5 bits as opposed to 7 bits in LSBWE algorithm.

Table 4. Comparison of the PSNR and MSE values obtained using DEAICSand LSBWE algorithm for grayscale host images.

Image size	*Host images*	*LSBWE*		*DEAICS*	
		PSNR	*MSE*	*PSNR*	*MSE*
256 × 256	Walter Cronkite	70.9199	0.0038	73.2313	0.0023
	Chemical Plant	72.4935	0.0037	74.5930	0.0023
	Table Clock	71.0548	0.0046	74.2809	0.0023
	Baby Face	71.5336	0.0042	73.8266	0.0023
512 × 512	Smiling Lady	71.1018	0.0034	71.2627	0.0032
	Elaine Face	71.5904	0.0035	73.4671	0.0023
	Iron Bridge	72.2844	0.0037	74.4557	0.0023
	Car	71.9557	0.0036	73.8733	0.0023

Table 5. Comparison of the PSNR and MSE values obtained using DEAICSand LSBWE algorithm for color host images.

Image size	*Host images*	*LSBWE*		*DEAICS*	
		PSNR	*MSE*	*PSNR*	*MSE*
256 × 256	Tree	72.5094	0.0035	72.8254	0.0032
	House	71.4503	0.0043	72.7201	0.0032
	Jelly beans	70.9309	0.0039	71.7499	0.0032
	Nature	71.8335	0.0040	72.8863	0.0032
512 × 512	Baboon	71.3790	0.0038	72.0601	0.0032
	Lena	71.8606	0.0038	74.1025	0.0023
	Pepper	71.5674	0.0038	72.2486	0.0032
	Car	71.2577	0.0036	72.5916	0.0032

6. CONCLUSION

We combined the features of cryptography and steganography to develop a robust crypto-stego system called DEAICS for precise ciphering or embedding of sensitive data information. The aim wasto securely transfer the private data over the open internet channels without being getting attacked by adversaries or unauthorized users. The proposed crypto-stegosystemrevealed better performance when compared withLSBWE algorithm. This achieved higher performance byDEAICS system is attributed to the use of random concealment procedure to hide the secret message into the specific intensity color pixels of the image as opposed tosequential hiding schemeused by LSBWE method. The proposed algorithmis demonstrates to achieve high level of capacity, higher PSNR for security, and lower MSE for robustness against attacks.

7. REFERENCES

1. D. K. Sarmah and N. Bajpai, "Proposed System for data hiding using Cryptography and Steganography," Int. J. Comput. Appl., vol. 8, no. 9, pp. 7-10, Oct. 2010.
2. K. Challita, H. Farhat, and N. Dame, "Combining Steganography and Cryptography?: New Directions," Int. J. New Comput. Archit. Their Appl., vol. 1, no. 1, pp. 199-208, 2011.
3. C. Lv and Q. Zhao, "Integration of data compression and cryptography: Another way to increase the information security," in Proceedings - 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINAW'07, 2007, vol. 1, pp. 543-547.
4. S. S. Sherekar, V. M. Thakare, and S. Jain, "Critical review of perceptual models for data authentication," 2nd Int. Conf. Emerg. Trends Eng. Technol. ICETET 2009, pp. 323-329, 2009.
5. A. Dhamija and V. Dhaka, "A novel cryptographic and steganographic approach for secure cloud data migration," in Green Computing and Internet of Things (ICGCIoT), 2015 International Conference on, 2015, pp. 346-351.
6. P. Marwaha and P. Marwaha, "Visual Cryptographic Steganography in Images," in Second International conference on Computing, Communication and Networking Technologies, 2010, pp. 1-6.
7. S. Usha, G. A. S. Kumar, and K. Boopathybagan, "A secure triple level encryption method using cryptography and steganography," Proc. 2011 Int. Conf. Comput. Sci. Netw. Technol. ICCSNT 2011, vol. 2, pp. 1017-1020, 2011.
8. G. Prema and S. Natarajan, "Steganography using Genetic Algorithm along with Visual Cryptography for wireless network application," 2013 Int. Conf. Inf. Commun. Embed. Syst., pp. 727-730, 2013.
9. S. P. Bansod, V. M. Mane, and R. Ragha, "Modified BPCS steganography using Hybrid cryptography for improving data embedding capacity," in Proceedings - 2012 International Conference on Communication, Information and Computing Technology, ICCICT 2012, 2012, pp. 1-6.
10. K. Joshi and R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication," 2015, pp. 86-90.
11. P. Sethi and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by Using Genetic Algorithm and Cryptography," in Procedia Computer Science, 2016, vol. 87, pp. 61-66.
12. 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," in 2014 International Conference on Informatics, Electronics and Vision, ICIEV 2014, 2014, pp. 1-6.
13. G. Swain and S. K. Lenka, "A Hybrid Approach to Steganography Embedding at Darkest and Brightest Pixels," in Proceedings of the International Conference on Communication and Computational Intelligence, 2010, pp. 529-534.
14. S. Republic, "Image steganography with using QR code and cryptography," 2016, no. 1, pp. 350-353.
15. Shahana T, "An Enhanced Security Technique for Steganography Using DCT and RSA," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 3, no. 7, pp. 2277-128, 2013.
16. H. A. Atee, R. Ahmad, and N. M. Noor, "Combining Cryptography and Steganography for Data Hiding in Images," in conference of Applied Computer and Applied Computational Science (ACACOS), 2014, pp. 128-134.
17. D. Samidha and D. Agrawa, "Random Image Steganography in Spatial Domain 1 2," Conf. Nano Electron. Telecommun. Syst. (ICEVENT). IEEE. Tiruvannamalai, pp. 1-3, 2013.
18. K.-H. Jung and K.-Y. Yoo, "Data hiding method using image interpolation," Comput. Stand. Interfaces, vol. 31, no. 2, pp. 465-470, 2009.
19. M. Aziz, M. H. Tayarani-N, and M. Afsar, "A cycling chaos-based cryptic-free algorithm for image steganography," Nonlinear Dyn., vol. 80, no. 3, pp. 1271-1290, 2015.