Australian Journal of Basic and Applied Sciences, 11(7) May 2017, Pages: 37-41

AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Block-based Image Steganography for Text Hiding Using YUV Color Model and Secret Key Cryptography Methods

[1]Suhaila Mohammed, [2]Shaymaa Ahmed, [3]Ghusoon Mohammed, and [4]Dhuha Abduljabbar

[1]Suhaila N. Mohammed, Assistant lecturer, Computer Science Department, College of Science, Baghdad, Iraq,
[2]Shaymaa D. Ahmed, Assistant lecturer, Computer Science Department, College of Science, Baghdad, Iraq,
[3]Ghusoon G. Mohammed, Assistant lecturer, Computer Science Department, College of Science, Baghdad, Iraq.
[4]Dhuha A. Abduljabbar, Assistant lecturer, Computer Science Department, College of Science, Baghdad, Iraq,

Address For Correspondence:
Suhaila Mohammed, Suhaila N. Mohammed, Assistant lecturer, Computer Science Department, College of Science, Baghdad, Iraq,
E-mail: suhaila.najam@yahoo.com

ARTICLE INFO

Article history:
Received 18 February 2017
Accepted 5 May 2017
Available online 10 May 2017

Keywords:
steganography, text hiding, YUV color transform, image blocking, symmetric key encryption, multiplicative cipher, Least Significant Bit (LSB)

ABSTRACT

Due to malicious changes and abolition of secret data, the current trend in information protection is not only based on using encryption methods for securing the data and storing or transmitting it. The trend is towards the use of steganography methods to hide the encrypted data which are in turn increase the security provided for it. In this paper a new method for secret text hiding in color image is proposed. The method based on using image transformation to decrease the error that may be resulted in the secret image due to hiding process. Blocking idea is also used for hiding the secret data in more scrambling way. Hybrid secret key ciphering algorithm is used for encrypting the data before hiding. For evaluation purpose, standard images have been used as test material and various sizes of data are stored in the images and the PSNR (Peak signal-to-noise ratio) and MSE (Mean Square Error) are also calculated for each of the images tested. The proposed steganography method gives MSE around 1.82 and PSNR value equal to 45.6 with the number of blocks equal to 6x4. Based on the PSNR and MSE values of each image, the results are considered good when compared with the results of other newly published works.

INTRODUCTION

From the time that humans became able to communicate, developing a secret connection was one of the main demands. In the past, despite having minute means, people had tried to hide data to not be discovered easily (Tavoli *et al.*, 2016). Steganography has been progressively becoming one of a popular technique to be used for secret communication between two parties or more (Satar *et al.*, 2015).

Steganography is defined as "secure hiding information technique within a noise; a way to supplement encryption, to prevent the existence of encrypted data from being detected" (Bhagat and Dhembhare, 2015). The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists (Jayaram *et al*. 2011) .

However, there are many types of steganography methods. The methods in which data is hidden in sound files using properties of the Human Auditory System (HAS) are called as audio steganography. Some of the methods use image data as a container of the secret information. This technique is called as image steganography. Since the video comprised of image and audio, video steganography enables to hide data in image as well as in audio and generate stego-video. Finally, hiding secret information in the text is also one of

To Cite This Article: Suhaila Mohammed, Shaymaa Ahmed, Ghusoon Mohammed and Dhuha Abduljabbar., Block-based Image Steganography for Text Hiding Using YUV Color Model and Secret Key Cryptography Methods. ***Aust. J. Basic & Appl. Sci.,*** *11(7): 37-41, 2017*

the important methods of steganography. Text steganography method proposes to hide a secret message in every (m^{th}) letter of every word of a text message (Swetha and Prajith, 2015).

The most popular files for hiding data are the images. Image steganography refers to the process of passing secret or confidential data in an image (Bharti and Kumar, 2014). In image steganography, the image is referred to as "cover image", the text to be hidden is called "secret message". After embedding the secret message it is referred to as "stego-image" (Jassim, 2013).

There are numerous stenographic algorithms that can be used to embed secret information in an image. The algorithms can be categorized into: spatial domain and frequency domain techniques (Bharti and Kumar, 2014) .

Spatial domain method uses encoding in Least Significant Bits (LSB). There are numerous versions of this method; all these techniques reliably alter some of the bits in the values of image pixels for hiding data, such as LSB replacement, LSB matching, and matrix embedding (Sravanthi, 2012).

Transform domain techniques conceal data in the specific areas of the original image. Here the data is generally set into altered coefficients of an image, giving much more capacity for information hiding and robustness against attacks. Transformation techniques are used to convert the image from spatial domain into frequency domain like discrete wavelet transform (DWT), discrete cosine transformation (DCT), discrete Fourier transformation, etc. (Borse and Patil, 2015) .

Cryptography is one method that helps in encrypting the data to be transferred. Then the encrypted text generally known as cipher text can be sent over the network to the receiver who can decrypt the data using the private key. But the cipher text may lead to suspicion no matter how strong the algorithm is. So data may become prone to interception as the intruder may alter it to give a fake thought of any individual. The combination of cryptography and steganography help in increasing the security level of the data being transmitted (Ekatpure and Benkar, 2013). A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data (Bharti and Kumar, 2014).

Numerous studies Muhammad *et al*. (2015), Karim *et al*. (2011), Narayana1and Prasad (2010), Ibrahim and Kuan (2011) and Thanikaiselvan and Arulmozhivarman (2013) have attempted to hide secret data inside an image. Three famous techniques can be used to hide data in an image. They are watermarking, steganography and cryptography (Muhammad, 2015). Therefore, previous studies that the proposed approaches similar to the model introduced in this work should be reviewed.

Narayana1and Prasad (2010) introduced two new methods wherein cryptography and steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. So in the first method, the payload image is converted into text and this text is hidden in another image. The secret key used in S-DES algorithm may be a character or number. In the second method, the payload image is encrypted directly and this encrypted data is hidden in another image. The secret key used for S-DES algorithm here is an image. The proposed method provides a higher similarity between the cover and stego pictures is achieved that also yields a better imperceptibility and prevents the possibilities of steganalysis (Narayana and Prasad, 2010).

Karim *et al*. (2011) proposed a new approach to place hidden information in either LSB of Green or Blue matrix of a specific pixel in carrier image which is decided by the secret key and efficient LSB of Red matrix. So anyone cannot exactly make a decision that the bit of hidden information is placed in either LSB of Green or Blue matrix. This approach improves security of existing LSB method by utilization of the secret key. The proposed approach has the same payload, more robustness and provides good security issue and PSNR value than general LSB. However the secure key exchange of the secret key is an open challenge and is an extra overhead of the proposed method (Karim *et al*. 2011).

Ibrahim and Kuan (2011) had applying a system called SIS (Steganography Imaging System) in which uses binary codes and pixels inside an image to improve the security of the proposed algorithm. The authors have used zipped file before it is converted to binary codes in order to increase the storage of data inside the image. The zip file is then converted into binary codes and secreted in the cover image. The proposed system is only for BMP format images, but has extra overload capacity and it is very efficient to hide the data inside the image (Ibrahim and Kuan, 2011).

Thanikaiselvan and Arulmozhivarman (2013) have produced a high robust method for color images in transform domain on the base of Reversible Integer Haar Wavelet Transform (RIHWT) and Graph Theory (GT). The proposed approach RIHWT is applied to the R, G and B planes separately and selects random wavelet coefficients based on GT for scattering the secret data in wavelet coefficients. Three different unique keys are used for encoding and decoding of secret data in the proposed method. Key1 is sub band selection key for selecting one of the sub bands i.e. LL, LH, HL and HH; Key2 is for selecting coefficients inside the selected sub band randomly on the basis of GG; Key3 is for deciding the number of bits to be stored in selected coefficients. This method showed good imperceptibility, High capacity and Robustness (Thanikaiselvan and Arulmozhivarman, 2013).

Muhammad *et al*. (2015) proposed a novel image steganography Least Significant Bit (LSB) based technique for RGB images using color space exchanging from RGB to Hue-Saturation-Intensity (HIS). The secret data are embedded in Intensity Plane (I-Plane) of HSI color model using LSB method. Finally the resultant image is transformed to RGB color model after embedding. Experimentally, the proposed method had larger Peak Signal-to Noise Ratio (PSNR) values, good imperceptibility and multiple security levels which shows its superiority as compared to several existing methods (Muhammad, 2015).

MATERIALS AND METHODS

The proposed method consists of two important schemes which are: secret message hiding scheme (sender side) and secret message extraction scheme (receiver side) as shown in Figure (1).

Sender side implies secret text encryption and hiding steps which are:

a. Cover image loading: in which the cover image where the message will be hidden is loaded.

b. Secret message loading: the secret message is loaded in this step.

c. Secret message encryption: through using private key multiplicative cipher with key=K_1 and direct standard alphabets with key=K_2. These keys are known only by the sender and receiver.

d. Cover image color model transformation: by converting the RGB model of the cover image into YUV color model.

e. U and V bands blocking: these bands then portioned into NxM blocks.

f. Secret message hiding using LSB method in each block of U and V bands in reversing order fashion.

g. 7. YUV to RGB color conversion: finally, YUV bands are converted back into RGB bands to get secret image.

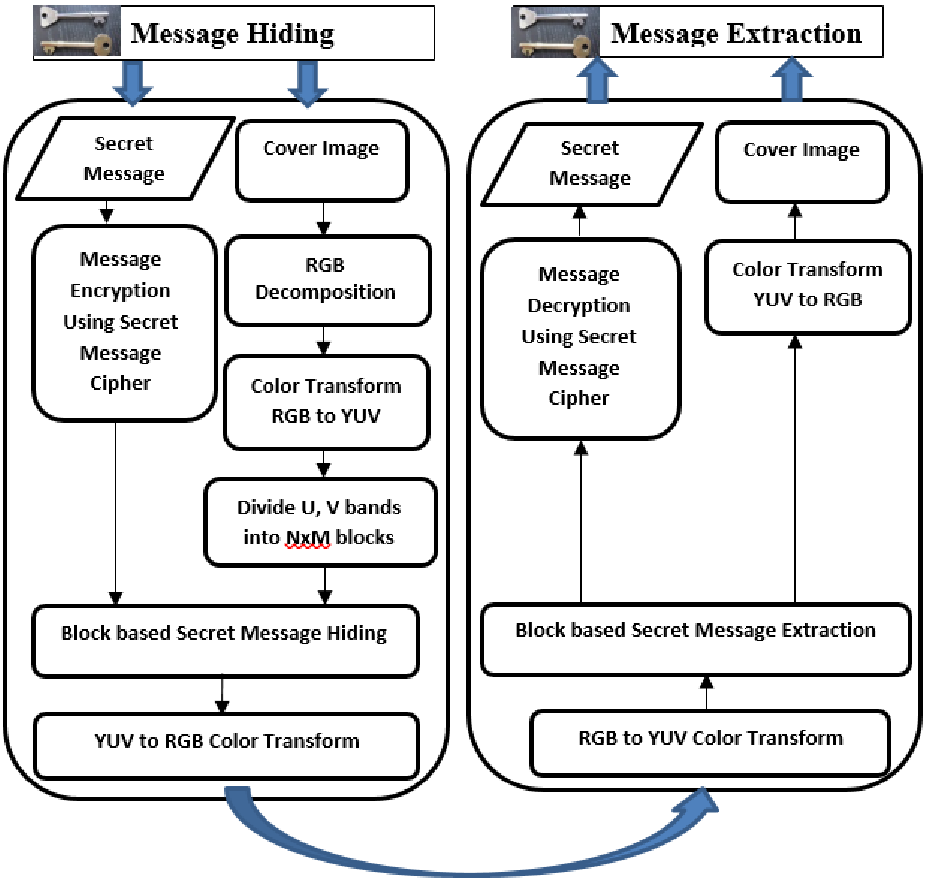


Fig. 1: Block diagram for the proposed steganography method

On the other hand, the receiver side will extract the hidden message as follows:

a. Secret image loading: here the secret image that contains the secret message is loaded.

b. Secret image color model transformation: since the secret message is hidden in U and V bands the secret image need to be converted from RGB into YUV color model.

c. U and V bands blocking: these bands are portioned into NxM blocks in order to access the actual hiding locations.

d. Secret message extraction using LSB method from each block of U and V bands in reversing order fashion.

Two schemes are described in details within the next subsections.

A. *Secret Message Hiding Scheme (Sender Side):*

In this part, the steps needed for protection secret message and hiding it in the cover image are done. This part implies following steps:

i. RGB to YUV Color Model Conversion Step:

The main goal of color models (also known as color systems or color spaces) is to represent all colors in a standard way. A color model is a way of representing a set of colors mathematically. The most popular color spaces are RGB, YCbCr (Luminance Component, Chroma Blue difference, Chroma Red difference) and CMYK (Cyan, Magenta, Yellow and Black), HSI (Hue, Saturation and Intensity), YUV.

YUV color space separate RGB into luminance and chrominance information and are useful in compression applications. By separating the luminance and chrominance information, most of the important information can be saved in a separate channel (Y channel) while the two other channels (U and V) will contain the fewer information of the image. By exploiting these properties, the secret message can be hidden in a location with less effect on the cover image (i.e. with fewer hidden error). For this reason the first step in the proposed steganography system is converting the cover image from RGB bands into YUV bands.

The following formulas define the conversion from RGB to YUV (MSDN, 2004) :

$$Y = ((66 * \mathrm{R} + 129 * \mathrm{G} + 25 * \mathrm{B} + 128) >> 8) + 16 \quad (1)$$

$$U = \left((-38 * \mathrm{R} - 74 * \mathrm{G} + 112 * \mathrm{B} + 128) >> 8\right) + 128 \quad (2)$$

$$V = ((112 * \mathrm{R} - 94 * \mathrm{G} - 18 * \mathrm{B} + 128) >> 8) + 128 \quad (3)$$

Figure (2) shows the results of applying this step on the cover image.

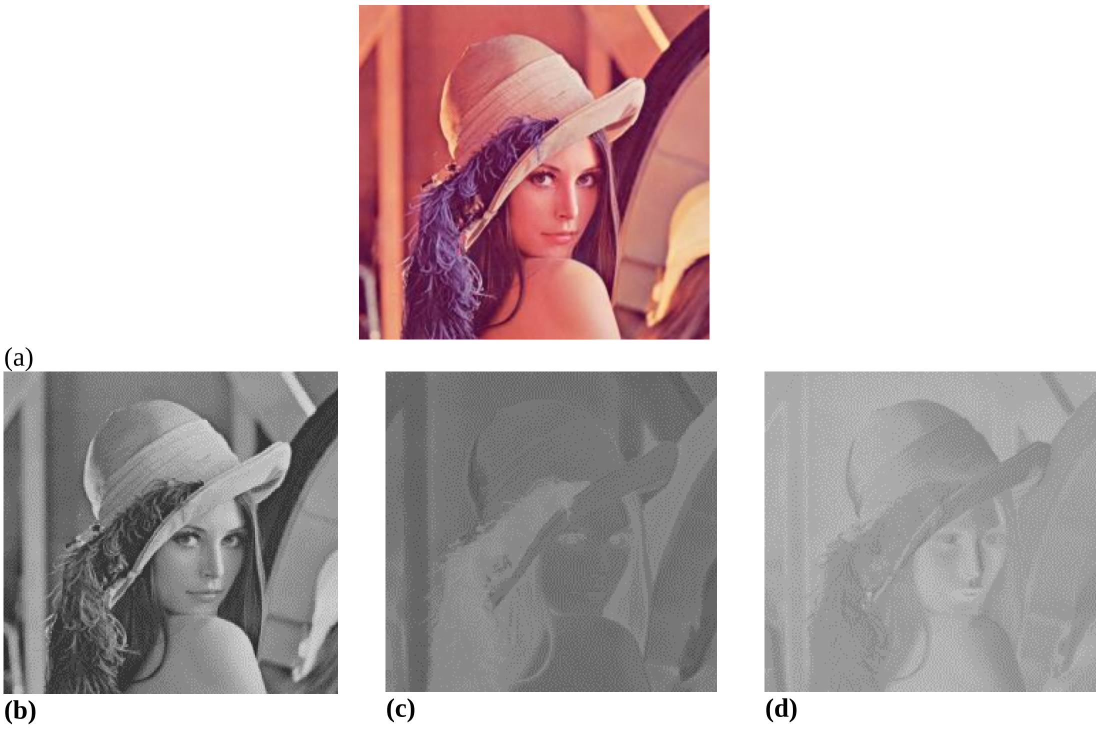


Fig. 2: RGB to YUV color space conversion results: (a) Original true color image, (b) Y band, (c) U band, (d) V band

ii. Secret Message Encryption Step:

Cryptography is the science or study of techniques of secret writing and message hiding. Cryptography is as broad as formal linguistics which obscures the meaning from those without formal training.

Encryption is one specific element of cryptography in which one hides data or information by transforming it into an indecipherable code. Encryption typically uses a specified parameter or key to perform the data transformation. Every method of encryption requires a special secret key to be previously and securely established. This is the nature of symmetric key encryption. A symmetric key, sometimes called private-key, encryption cipher is any algorithm in which the key for encryption is trivially related to the key used for decryption. There are many methods for symmetric encryption, such as DES, RC4, play fair... etc.

Australian Journal of Basic and Applied Sciences, 11(7) May 2017, Pages: 37-41

In the proposed method the secret message is encrypted using a combined encryption methods by combining direct standard alphabets (DES) and multiplicative encryption methods. Two private keys (K_1, K_2) are used for these methods, respectively, as in the following equation:

$$C = \left((P * K1) Mode\ N\right) + K2) Mode\ N \quad (4)$$

Where N is the number of characters in plain space, and since the characters of the secret message in our experiments are in ASSCII coding so N is 256

In multiplicative cipher the greatest common divisor between the key and the number of characters must be 1 (GCD (K_1, N) = 1) to ensure there is no duplicate encrypted characters for the same plain one.

The main reason of selecting these ciphering methods is both are easy, fast and the order of the cipher text alphabet is scrambled in which the multiplicative cipher does not preserve the pattern of frequency peaks and valleys that we have with the plaintext alphabet and is, hence, harder to recognize. In other hand direct standard method shifts the alphabets with K_2 positions and then increasing encryption power. Figure (3) shows the block diagram of encryption scheme.

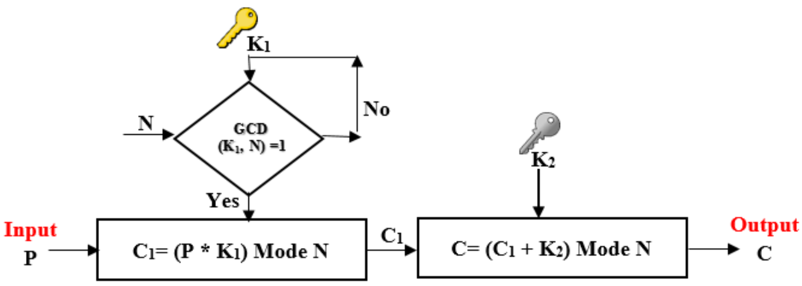


Fig. 3: Encryption block diagram

Table (1) shows an example for encrypting the message "Secret Message" with with K1=5 and K2=4 along with ASCII value for both plain and encrypted characters.

Table 1: An example for encrypting the message "Secret Message" with K_1=5 and K_2=4

Plain character	S	e	c	r	e	t	space	M	e	s	s	a	g	e
ASCII of plain character	83	101	99	114	101	116	1	77	101	115	115	97	103	101
ASCII of encrypted character	163	253	243	62	253	72	9	133	253	67	67	233	7	253
Encrypted character	£	*	ó	>	*	H	\t	"	ý	C	C	é	\a	ý

iii. Block based Secret Message Hiding:

As shown in figure (2) most of the energy of the image is stored in Y band while U and V bands contains few details. So, we have exploded this property in hiding a secret message in away with less error through hiding it in bands (U and V) those contain the low details of the image. First, these bands are portioned into NxM blocks as in Figure (4) in which U band image portioned into 4x5 blocks.

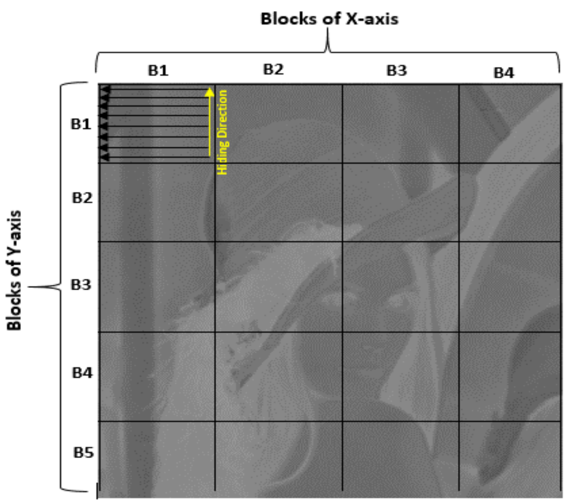


Fig. 4: Blocking Idea (with 4x5 blocks) upon Y band image

The characters of the message are stored in the U and V blocks one after another in reverse sequence (from the end of the block to the beginning as shown in figure (3)). The first pixel of these bands is used for storing the number of characters (CharCount) in the message by portioning the number that represents character count into two parts (because this number is 2bytes long and U and V bands can store only one byte) and storing them in the pixel at location (0,0) for U and V bands respectively as following:

$$Ustego(0,0) = CharCount \ \& \ 255 \quad (5)$$
$$Vstego(0,0) = (CharCount \gg 8) \ \& \ 255 \quad (6)$$

LSB method is used for hiding the encrypted secret message characters as in following steps:

a- The ASSCII number of each character (Ch) is converted into binary form.

b- The first 4- LSB bits of Y and V pixels' values are cleared by masking them with mask equal to 240 as follows:

$$Unew = U \ \& \ 240 \quad (7)$$
$$Vnew = V \ \& \ 240 \quad (8)$$

c- The binary number of the character is divided into two parts through applying following two equations:

$$P_1 = Ch \ \& \ 240 \quad (9)$$
$$P_2 = Ch \ \& \ 15 \quad (10)$$

d- The first part of the character is shifted left for four positions. This shift is needed to put character bits in the first LSB of the byte.

e- Finally, P_1 is Oring with Unew and p2 is Oring with Vnew

$$Ustego = Unew \ | \ P_1 \quad (11)$$
$$Vstego = Vnew \ | \ P_2 \quad (12)$$

Figure (5) shows a numeric example for applying this step.

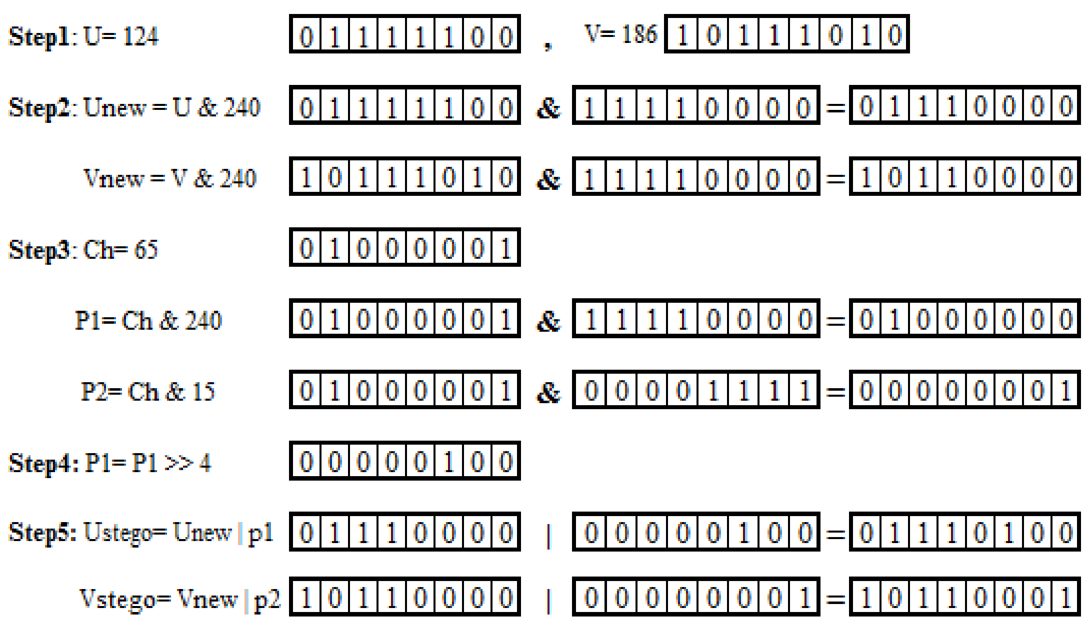


Fig. 5: A numerical example for applying hiding steps

iv. YUV to RGB Color Model Conversion Step:

Finally, the YUV bands which currently include the encrypted secret message converted back into RGB bands. The following coefficients are used in conversion process (MSDN, 2004):

$$C = Y - 16 \quad (13)$$
$$D = U - 128 \quad (14)$$
$$E = V - 128 \quad (15)$$

Using the previous coefficients, the following formulas provide the conversion from YUV to RGB (MSDN, 2004):

$$R = (298 * C + 409 * E + 128) >> 8 \quad (16)$$
$$G = (298 * C - 100 * D - 208 * E + 128) >> 8 \quad (17)$$
$$B = (298 * C + 516 * D + 128) >> 8 \quad (18)$$

B. Secret Message Extraction Scheme (Receiver Side):

After receiving stego-image from receiver side, the steps needed for extraction secret message and decryption it must be done. This part implies following steps:

i. RGB to YUV Color Model Conversion Step:

Again, the stego-image is converted from RGB bands into YUV bands, which are contain secret message within 4- LSB bits of U and V channels.

ii. Block-Based Secret Message Extraction:

As shown in sender part, the characters of the secret message are stored in the U and V blocks one after another in reverse sequence from the end of the block to the beginning. After extracting the characters of the secret message, the number of its characters is retrieved from the first pixel of U and V bands as follows:

$$P_1 = U(0,0) \quad (19)$$

$$P_2 = V(0,0) \quad (20)$$

$$CharCount = P_1 | (P_2 << 8) \quad (21)$$

After that, the characters of the secret message are extracted as follows:

a-The numbers those represent the number of blocks in stego-image (NxM) are retrieved from the first two pixels (Y (0, 0), Y(0,1)) of Y band .

b- The characters of the secret message are extracted from the first 4- LSB bits of U and V pixels of each block in reverse order as following:

$$P_1 = U \,\&\, 15 \quad (22)$$

$$P_2 = V \,\&\, 15 \quad (23)$$

$$Ch = (P_1 \ll 4) \mid P_2 \quad (24)$$

Figure (6) shows a numeric example for applying this step.

iii. The Extracted Secret Message Decryption:

In decryption step, the secret message is firstly decrypted with direct standard alphabets (with K2) after that the result is decrypted with multiplicative cipher using the inverted key of K1 as following equation:

$$P = \big((C - K2) Mod\ N\big) * K1inv) Mode\ N \quad (25)$$

The block diagram of decryption step is shown in Figure (7).

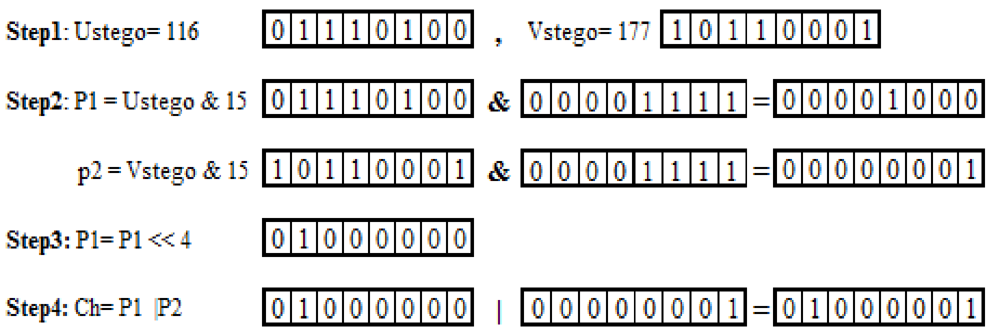


Fig. 6: A numerical example for extracting hiding text

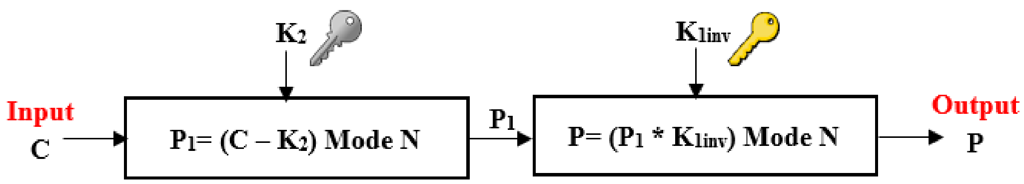
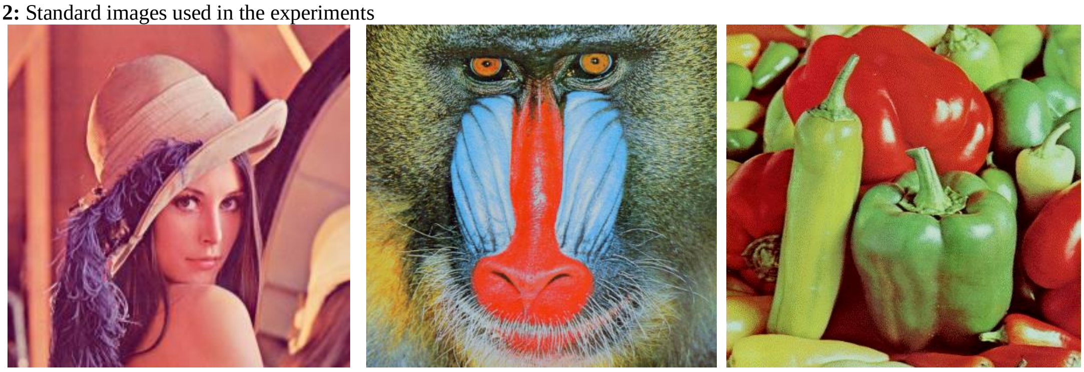


Fig. 7: Encryption block diagram

Results:

The proposed method is tested using standard test images of size 256x256 or 512x512 which are all colored images (the used images are shown in Table(2)). Three types of experiments are made by measuring the standard metrics: Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and the histogram based testing. Also the elapsed time is measured.

Table 2: Standard images used in the experiments



(a) **(b)** **(c)**

A. MSE Results:

The mean-squared error (MSE) between two images $I_1(i; j)$ and $I_2(i; j)$ - cover image and stego image ,respectively, is:

$$MSE = \frac{1}{WxH}\sqrt{\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}(I_1(i,j) - I_2(i,j))^2} \quad (26)$$

Where W and H are the number of rows and columns of the cover image.

Tables (3-5) show the MSE resulted when hiding secret messages of size (1K), (2K) and (3K), respectively, on the tested cover images.

Table 3: MSE resulted when hiding secret message of size (1K) in the tested cover images.

Images	MSE_R	MSE_G	MSE_B	MSE_{Av}
a	2.75	0.71	2.72	2.06
b	0.58	0.17	0.97	0.58
c	0.63	0.16	0.94	0.58

Table 4: MSE resulted when hiding secret message of size (2K) in the tested cover images.

Images	MSE_R	MSE_G	MSE_B	MSE_{Av}
a	4.08	1.34	4.65	3.36
b	0.93	0.36	1.7	0.99
c	0.89	0.33	1.66	0.96

Table 5: MSE resulted when hiding secret message of size (3K) in the tested cover images.

Images	MSE_R	MSE_G	MSE_B	MSE_{Av}
a	5.87	1.992	7.227	5.029
b	1.383	0.529	2.488	1.467
c	1.33	0.367	2.361	1.353

Figure (8) shows flow chart for the average MSE value when saving data of the three different sizes for the three different testing images.

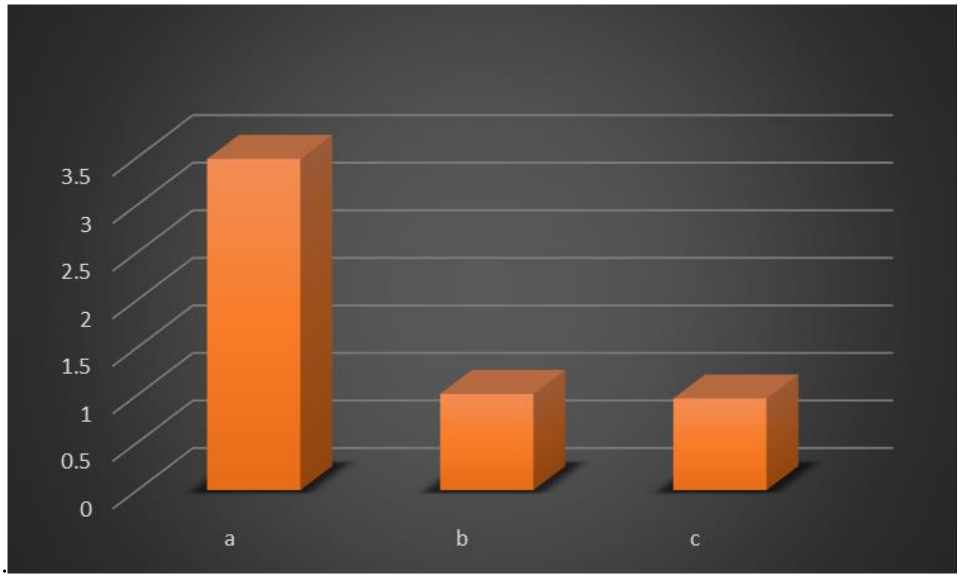


Fig. 8: Flow chart for the average MSE value when saving data of the three different sizes

B. PSNR Results:

Peak Signal-to-Noise Ratio (PSNR) measures the distortion in the stego-image. In fact, the PSNR measures the deviation between the stego-image and the cover image and it is expressed in terms of the logarithmic decibel (dB) as:

$$PSNR = 10\ log_{10}(\frac{MAX^2}{MSE}) \qquad (27)$$

Where MAX is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255. For color images with three RGB values per pixel. Typical values for the PSNR in lossy image and video compression are between 30 and 60 dB, where higher is better. Tables (6-8) show the PSNR resulted when hiding secret messages of size (1K), (2K) and (3K), respectively, on the tested cover images.

Table 6: PSNR resulted when hiding secret message of size (1K) in the tested cover images.

Images	$PSNR_R$	$PSNR_G$	$PSNR_B$	$PSNR_{Av}$
a	39.8	47.61	43.2	43.54
b	48.53	51.55	46.33	48.8
c	48.72	51.62	46.49	48.94

Table 7: PSNR resulted when hiding secret message of size (2K) in the tested cover images.

Images	$PSNR_R$	$PSNR_G$	$PSNR_B$	$PSNR_{Av}$
a	38.85	45.89	40.96	41.9
b	46.82	50.17	44.54	47.18
c	46.96	50.26	44.67	47.3

Table 8: PSNR resulted when hiding secret message of size (3K) in the tested cover images.

Images	$PSNR_R$	$PSNR_G$	$PSNR_B$	$PSNR_{Av}$
a	38.02	44.46	39.22	40.57
b	45.57	49.11	43.26	45.98
c	45.72	49.2	43.48	46.13

Figure (9) shows bar chart for the average MSE value when saving data of the three different sizes for the three different testing images.

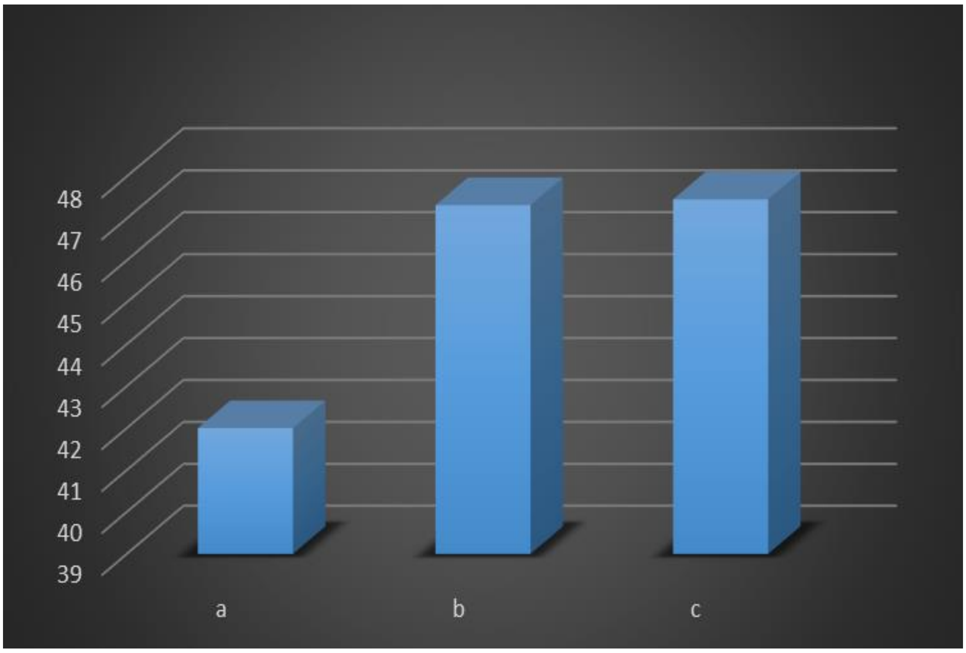


Fig. 9: Flow chart for the average PSNR value when saving data of the three different sizes for the three different testing images

C. Elapsed Time:

The consumed time is also calculated because it can give an indication for the efficiency of the system. Table (9) shows the consumed time for hiding and extraction steps with three different secret message sizes.

Table 9: The consumed time for hiding and extraction steps with three different secret message sizes

Cover Images	File size=1K		File size=2K		File size=3K	
	Hiding Time (msec)	Extraction Time (msec)	Hiding Time (msec)	Extraction Time (msec)	Hiding Time (msec)	Extraction Time (msec)
A	00.667	02.185	00.669	02.155	00.903	02.049
B	03.539	03.078	03.542	02.914	02.606	03.193
C	02.606	02.841	03.533	02.732	02.619	02.924

Conclusion:

In the era of fast information interchange using World Wide Web and internet, steganography has become a necessary tool for information security. Steganography can be categorized based on numerous criteria and one among them is based on the type of cover media. In this paper a new method for hiding a secret message in the cover image (image steganography) has been proposed. Several researchers have been described different techniques, but all the methods suffer with the image quality problem. So, in order to achieve good quality, hybrid secret key encryption methods have been used to encrypt secret messages by combining multiplicative and direct standard alphabets ciphering methods using two different secret keys (K1 and K2). Color transform has been used to convert cover image into YUV color model which is more suitable for hiding purpose that do not have a noticeable distortion on it by the human eye. The secret message characters are hidden in U and V bands (those contain the low details of the image) using LSB method in blocking manner. The stego colored images with different size were tested using MSE and PSNR measures. The proposed method gave an average MSE equal to 1.82 and average PSNR equal to 45.6 with block numbers 6x4, the average hiding and extraction time for different cover images and stored data size are equal to 2.29 msec and 2.67 msec respectively. As a future work the proposed system can be improved by converting the cover image into frequency domain using wavelets transform to decompose the cover image to get the four frequency bands (LL, LH, HL, and HH) where in the high frequency band maximum data are embedded. This gives maximum data embedding capacity and security used in steganography, and the secret message can be hidden in low energy coefficients, also blocks based Secret Message can be applied with another different block size.

REFERENCES

Bhagat, A.R and A.B. Dhembhare, 2015. An Efficient and Secure Data Hiding Technique – Steganography. International Journal of Innovative Research in Computer and Communication Engineering, 3(2): 941-949.

Bharti, D and A. Kumar, 2014. An improved mechanism of secret data hiding in an image and enhanced security by minimized detection .International Journal For Research In Applied Science and Engineering Technology (IJRAS ET), 2(VI): 176-179.

Borse, D and S. Patil, 2015. Review on Transform Domain Steganographic Techniques (DCT & DWT). International Journal of Innovative Research in Computer and Communication Engineering, 3(12): 12466 – 12473.

Ekatpure, P.R and R.N. Benkar, 2013. A Comparative Study of Steganography & Cryptography. International Journal of Science and Research (IJSR), 4(7): 670- 672.

Ibrahim, R and T.S. Kuan, 2011. Steganography algorithm to hide secret message inside an image. arXiv preprint arXiv:1112.2809.

Jassim, F.A., 2013. A novel steganography algorithm for hiding text in image using five modulus method. arXiv preprint arXiv:1307.0642.

Jayaram, P., H.R. Ranganatha and H.S. Anupama, 2011. Information Hiding Using Audio Steganography– A Survey. The International Journal of Multimedia & Its Applications (IJMA), 3: 86-96.

Karim, S.M., M.S. Rahman and M.I. Hossain, 2011. December. A new approach for LSB based image steganography using secret key. In Computer and Information Technology (ICCIT), 2011 14th International Conference, pp: 286-291.

MSD04, 2004. April. http://msdn.microsoft.com/en-us/library/ms893078.aspx.

Muhammad, K., J. Ahmad, H Farman and M. Zubair, 2015. A novel image steganographic approach for hiding text in color images using HSI color model. arXiv preprint arXiv:1503.00388.

Narayana, S and G. Prasad, 2010. Two new approaches for secured image steganography using cryptographic techniques and type conversions. Signal & Image Processing: An International Journal (SIPIJ), 1(2): 60-73.

Satar, S.D.M., N.A. Hamid, F. Ghazali, R. Muda and M. Mamat, 2015. A New Model for Hiding Text in an Image Using Logical Connective. International Journal of Multimedia and Ubiquitous Engineering, 10(6): 195-202.

Sravanthi, G.S., B.S. Devi, S.M. Riyazoddin and M.J. Reddy, 2012. A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method. Global Journal of Computer Science and Technology Graphics & Vision, 12(15): 176-179.

Swetha, V and V. Prajith, 2015. Data Hiding Using Video Steganography -A Survey. International Journal of Computer Science Engineering and Technology (IJCSET), 5(6): 206-213.

Tavoli, R., M. Bakhshi and F. Salehian. 2016. A New Method for Text Hiding in the Image by Using LSB. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 7(4): 126-132.

Thanikaiselvan, V and P. Arulmozhivarman, 2013. October. High security image steganography using IWT and graph theory. In Signal and Image Processing Applications (ICSIPA), 2013 IEEE International Conference, pp: 337-342.