Journal of Engineering and Applied Sciences 13 (11): 4235-4244, 2018
ISSN: 1816-949X

Image Steganography Technique Based on Extracted Chains from the Secret Key

Mohammed Abbas Fadhil Al-Husainy and Diaa Mohammed Uliyan
Department of Computer Science, Faculty of Information Technology,
Middle East University, Amman, Jordan

Abstract: Image stegangoraphy is considered as an active research topic where secret information is embedded in digital images while preserving their visual quality. Recently, various image steganography techniques focused on payload capacity, robustness and imperceptibility. However, there is a state of art between of these three metrics and keeping a balance between them is still a challenge problem. In addition, some existing techniques failed to gain better security caused by direct embedding of secret data inside images without encryption or random placement consideration. This issue could make image styganalysis quite easy for an adversary. Therefore, in this study, Least Significant Bit (LSB) is used to replace the least significant bits of image pixels with the bits of secret data. We propose a secure image steganography method based on stego-key. Secret data is embedded randomly in LSB of the image pixels based on chain of secret keys. The common pipeline of our method starts by dividing the image into a group of two-dimensional blocks and uses a set of two-dimensional stego-key. Then, the secret data is hidden in the pixels of each image block, based on the extracted chains from the stego-key. The quantitative and qualitative experimental results show that, the proposed method can achieve a good balance between visual image quality and its security, providing a high capacity for hiding data with relatively less time complexity. A relatively large size stego-key is also employed in order to increase the level of security for the proposed method and makes it hard to detect by the brute force attacks.

Key words: Chains of pixels, hiding capacity, image steganography, information hiding, information security, secret key

INTRODUCTION

The origin of steganography is from the Greek word "steganos" which means concealed "writing" (Sharma and Srivastava, 2017). With the rapid development of clouds in networks and digital image processing tools, there are a lot of images are distributed in the cloud recently. Steganography techniques were developed to hide messages into a cover image without showing any visual differences on the image itself (Luo *et al*., 2010). The performance of a steganography technique is mainly evaluated by its capacity, robustness and statistical imperceptibility criteria (Hamid *et al*., 2012). Consequently, a steganography method should have a high capacity and better imperceptibility where the human eyes fail to detect it. However, these criteria are often mutually exclusive to each other. It is difficult to balance all these criteria concurrently. High embedding capacity and undetectability are two main properties which demanded to be carefully regarded in the practical applications (Fridrich *et al*., 2007).

In the era of Information Technology (IT), protecting information against unauthorized access in the cloud or modification became essential to maintain the security in storing and sharing digital information. The importance of information security has stimulated the IT experts to develop innovative methods for protecting information.

However, a higher level of protection could be achieved by hiding the information in a way that no one can suspect its existence, detect and retrieve it. The authorized persons can do steganalysis based on secret key to read hidden information. Mainly, steganography techniques are developed to hide secret information inside four types of digital carrier files such as image, text, audio or video files (Lu, 2004). Recently, images are commonly used as a carrier to hide information (Fridrich *et al*., 2001; Kaur *et al*., 2014). According to type embedding information in the image content, steganography methods can be categorized into: spatial Domain techniques (Cheddad *et al*., 2010; Gul and Kurugollu, 2010), frequency domain techniques (Chen and

Corresponding Author: Mohammed Abbas Fadhil Al-Husainy, Department of Computer Science, Faculty of Information Technology, Middle East University, Amman, Jordan

Lin, 2006, Saidi *et al*., 2017). While, the spatial domain techniques apply direct manipulation over the pixels of the image, the transform domain techniques transform the image into frequency domain and then hide the secret message. It is important to notice that the hiding capacity of secret messages in spatial domain technique is relatively larger than frequency domain techniques (Cheddad *et al*., 2010).

Steganography techniques that use stego key for hiding information are classified into three classes (Sumathi *et al*., 2014).

Pure steganography: Where there is no stego key used. It supposes that no other parties know about communication (Han *et al*., 2017).

Secret key steganography: Where the stego key is exchanged before the communication. It assumed that the communication might be intercepted (Saqer and Barhoom, 2016).

Public key steganography: Where two stego keys (public and private) are used for elastic and secure communication (Manjula and Shivakumar, 2016).

This research proposes a secret key steganography technique where it uses a secret key of size (256×8 = 2048 bits).

A large number of images transmitted via. the internet have encouraged researchers to use these images as a cover media in developing the steganography methods for protecting data in the field of information security (Rana and Singh, 2010). Image steganography methods concentrate on the techniques of hiding a secret data in a cover image and generate a stego image which is carrying a hidden secret message (Kaur *et al*., 2014). An image steganography model consists of three elements: secret data, cover image and key. Where stego image is the cover image that contains the secret data and stego key is the key that is used to embed the secret data in the cover image (Subhedar and Mankar, 2014).

The success of the image steganography methods depends on exploiting the weak point in detecting minor changes happen in the stego-image pixels by the Human Visual System (HVS). There are some major properties that determine the strength and weaknesses of the image steganography techniques (Purohit and Sridhar, 2014; Tiwari *et al*., 2014).

Capacity: It is the indicator of the amount of data that is embedded in the cover image. It is measured in bits per pixel (bpp) (Sarreshtedari and Ghaemmaghami, 2010).

Robustness: The novelty and the solidity of the way that is used to embed information without causing damage the cover image itself (Subhedar and Mankar, 2014).

Undetectability: The ability to detect the embedded information in the cover image using visual or statistical means (Wu and Tsai, 2003; Roy *et al*., 2013).

These goals are hard to achieve in the same time. Hiding long message makes it more vulnerable to detect by attackers (i.e., it becomes less secure) and vice versa. One of the common techniques to do steganography is hiding secret messages in the Least Significant Bit (LSB) of the image plane. LSB techniques in terms of the competing major properties are considered as a practical way to conceal messages in the spatial domain of image plane. Furthermore, it can hide large quantities of data, for instance, high payload capacity (Hamid *et al*., 2012).

Least Significant Bit (LSB) is the traditional method of embedding secret information in a digital image (Yadav *et al*., 2014). This traditional method uses the LSB of the pixels in the cover image to hide the bits of the secret message. This usually causes distortion in the stego image and the ratio of distortion depends mainly on the number of changes that occur in the LSB of pixels. This distortion must keep at the minimum to drive away any doubt about the presence of the secret message in the stego-image. This will make the image steganography based on LSB method is efficient.

The proposed method will present a secure and full capacity LSB steganography technique. This is done by using all the pixels of the cover image to hide the secret message and random selection of the pixels based on a large stego key of size (2048 bits).

In the field of information security, many researchers focused on innovation of strong steganography techniques. Several efficient algorithms are developed to attack image steganography techniques, some of these algorithms focused on steganalyze the LSB techniques through implementing two stages on specific types of images: features extraction and classification as shown in Table 1 (Desai and Patel, 2014). Therefore, the designing of secure steganography technique is day by day becoming critical. If the attacker observed that there is a secret data hidden in the stego image, it should be difficult to extract the secret data from the stego image. Thus, the major task of designing the secure image steganography technique is the selection of strong stego key.

Table 1: Set of steganalysis algorithms on the LSB steganography techniques (Desai and Patel, 2014)

Algorithm	Features	Classifier	Image type
Avcibas *et al.* (2001)	IQM	Multivariate	BMP
		Regression analysis	JPEG
Zou *et al.* (2006)	Markov	SVM with Linear and	BMP
		Nonlinear kernel	JPEG
Farid (2002)	Wavelet	FLD	BMP
			JPEG
Xuan *et al.* (2005)	Wavelet	Bayes	BMP
			JPEG
Sun *et al.* (2009)	Wavelet	Back propagation	BMP
			JPEG
Avcibas *et al.* (2005)	BSM	SVM	BMP
			JPEG
Qian-Lan (2010)	Histogram	SVM	BMP
			JPEG
Yan *et al.* (2013)	Merge	SVM	BMP

While the frequency domain image steganography methods try to convert the colored image and extract features from the whole image to hide data, the time complexity of these methods (Xuan *et al.*, 2005; Sun *et al.*, 2009; Al-Asmari *et al.*, 2011) will arise. Hence, the main focus in this study is on spatial domain techniques based on LSB due to its robustenss and easy to implement. Various LSB techniques for image steganography have been covered (Trivedi *et al.*, 2016).

One of the major goals of steganography techniques is to increase the amount of data hidden in the cover image; this certainly needs to use a large number of bits of pixels of the cover image. But this results to raise the distortion ratio in the stego image and affect negatively on the quality of the stego image (Tiwari *et al.*, 2014).

Husainy (2012) proposed a steganography technique reduces the distortion that occurs in the stego image pixels through dividing the secret message into a set of blocks of the same length and finding the best similarity between LSBs of pixels and the blocks.

Abhiram *et al.* (2009) proposed a randomization technique that used the three channels of image colors to improve the hiding of secret information. The embedding capacity in two channels is determined by the two LSBs of the third channel. The indicator channel is selected by the user if the two LSBs of the indicator channel are (where the channels of image colors are Red, Green and Blue (RGB)):

- 00 Both channels 1 and 2 do not contain hidden data
- 01 Only channel 2 contains hidden data
- 10 Only channel 1 contains hidden data
- 11 Both channels 1 and 2 contain hidden data

Gutub *et al.* (2010) presented a similar implementation of the pixel indicator technique to hide a secret message inside the image.

An image steganography technique based on dynamic pattern has been proposed by Thiyagarajan *et al.* (2010). Through generating a dynamic pattern in the selection of indicator sequence, this technique aims to strengthen the security of hidden data. To minimize the distortion in the pixels, data should embed in the insignificant color channel of pixels and exclude the significant color channel.

Rana and Singh (2010) suggested LSB image steganography technique by using a pre-determined random selection of pixels, dividing the cover image to a set of segments and dividing the secret message into four blocks after encrypted it using Data Encryption Standard (DES) method. A predetermined method is used to select a pixel in each block, each pixel represents the stego key. Three levels of security used in this technique through a combination of odd and even rows and columns, respectively.

Novel steganography technique for the RGB format images has been presented by Amir and Nilchi (2013). It embeds a secret text in the blue layer of certain blocks. At the first, each block chooses a unique t1×t2 matrix of pixels as a "pattern", using the bit difference of neighborhood pixels for each keyboard character. Then, a secret message is hidden in the remaining part of the block. Blocks are chosen randomly using a random generator for increasing the security.

Singh *et al.* (2014) proposed an image steganography method that hides a secret message using the N-Queen matrix (pattern) as the stego key. The value of N in the N-Queen matrix reflects the level of security in the steganography method. The numbers of solutions increase with the increase of N.

All the above-mentioned image steganography techniques which are based on random selection of LSB of pixels did not use a full capacity of the cover image like the traditional LSB techniques. But on the other hand, the traditional LSB techniques are more vulnerable to penetrate by attackers through reading the LSB of pixels in the stego image sequentially whereas the random based selection of LSB provides more security. The proposed technique in this research is based on the random selection for LSB of pixels and using the full capacity of the cover image.

MATERIALS AND METHODS

To achieve the three strength properties (i.e., capacity, robustness and undetectability) in the proposed

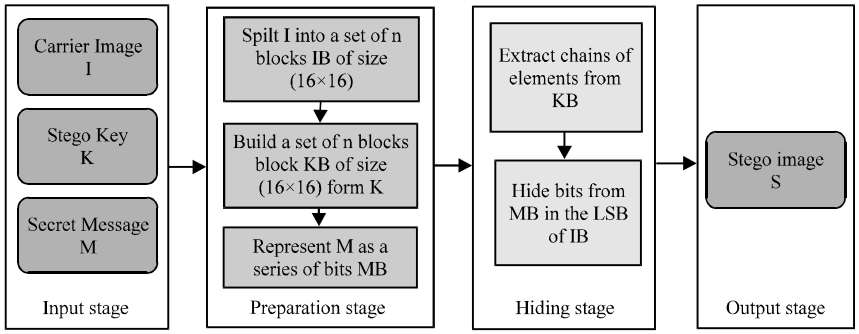

Fig. 1: The model of the proposed image steganography technique

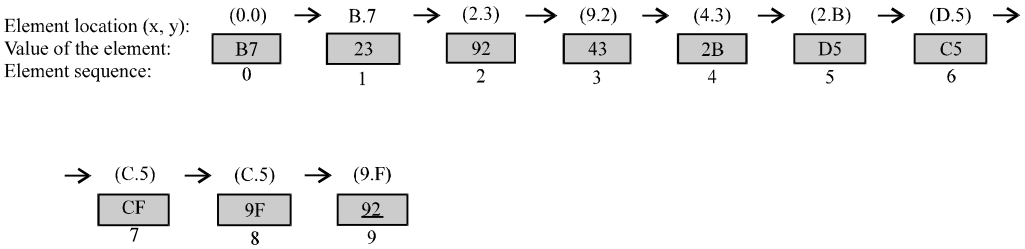

Fig. 2: The first chain of elements (yellow elements) started at (0, 0) contains the series of elements

image steganography technique. The proposed technique uses the full capacity of the cover image by exploiting the LSB of all pixels in the cover image to hide the bits of the secret data. And the random selection of pixels in the cover image using the extracted chains of elements from the key, leads to strengthen the security of the technique and increase the protection for the secret data against attackers.

The model that depicts the main stages of the hiding phase of the proposed image steganography technique is shown in Fig. 1. The details of the processes in each stage that are applied to hide the secret data in the cover image are illustrated below:

Input stage: Getting the following inputs from the user:

- Step 1: Cover Image I of size I_{Size} bytes
- Step 2: Stego key K of size K_{size} byte. Where K_{size} must be ≥256 bytes
- Step 3: Secret message M of size M_{size} bytes. Where (M_{Size}×8) must be ≤I_{size}

Preparation stage: Put the entered data in an appropriate structure to use it in the hiding stage:

- Step 1: Split the cover Image I into a set of n blocks of size (16×16) from IB(0) to IB(n-1). Where n = I_{size}/(16×16)
- Step 2: Taking the first 256 bytes of the stego Key K and put them in a block KB of size (16×16). The indices of rows and columns in KB are represented as Hexadecimal numbers (Fig. 2-5)
- Step 3: Represent the secret message bytes in the form of a series of bits MB

Hiding stage: The secret Message Bits MB are embedded in the LSB of the pixels in the cover image blocks IB where the pixels are randomly selected based on the stego key Block (KB):

- Step 1: For each image data Block IB(b) from b = 0 to n-1, do steps 2-4
- Step 2: Extract the chains of elements from the stego Key Block (KB) (this operation will be explained in detail later)
- Step 3: Generate a new stego Key Block (KB) (this operation will be explained in detail later)
- Step 4: If there are More Bits in (MB), read bits from MB and hide them in the LSB of the pixels in the cover Image Block (IB(b)). The sequence of elements in the extracted chains in step 2, determines the sequence of the pixels that are used in the hiding operation

Output stage: Construct the stego image S. In the proposed image steganography technique, to extract the secret message from the stego image, similar stages of the embedding operation are followed.

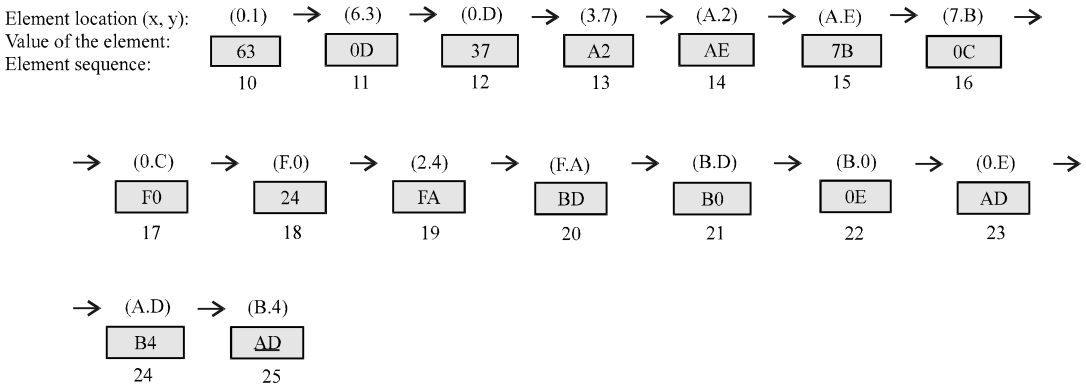

Fig. 3: The second chain of elements (green elements) started at (0, 1) contains the series of elements

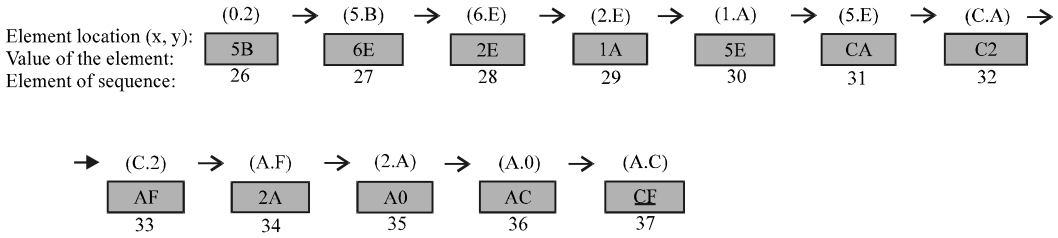

Fig. 4: The third chain of elements (red elements) started at (0, 2) contains the series of elements

To give more explanation about the generation of the new stego key and the extraction of the chains used in the hiding stage. Given below a simple numerical example:

Suppose the source block of the stego key that is obtained from the user is KB as shown in Fig. 5. The row number, the column number and the bytes in the stego Key Block (KB) are represented using the hexadecimal number system.

The extracted chain of elements from the above stego key block is a series of all elements in KB and this series starts from the first element at top-left corner of the KB (which is (0, 0)), the next element of an element (x, y) is the element that achieves one of the following two cases (Fig. 5 and 6):

Case 1: It is the element (r, c) which did not visit before and the row number and the column number (i.e., r and c) are calculated from the following formulas:

- r = (the most significant digit of the value of (x, y)+ the most significant digit of the value of the first element in the sub-chain) modulus 16
- c = (the least significant digit of the value of (x, y)+ the least significant digit of the value of the first element in the sub-chain) modulus 16

Case 2: When we reach in Case 1, to an element had been visited previously. The next element is the element which unvisited before and comes sequentially when we pass through the elements of the stego Key Block KB in a row-after-row manner. For examples: in the Key Block (KB) shown in Fig. 2-5.

For each Image data Block (IB(b)), a new stego key block is generated from the old key. The generation process of the new key is based on the extracted chain of elements mentioned above. The new value of an element (x, y) in the new stego key block is calculated using Eq. 1. If the chain of elements is: $(x, y)_0, (x, y)_1, (x, y)_2, \ldots, (x, y)_{255}$ then:

$$NewKey((x, y)_n) = [(OldKey((x, y)_n)+ NewKey((x, y)_{n-1})] \text{ modulus } 256 \quad (1)$$

Where:

n = 0, 2, 3, …, 255

x and y = The row and column numbers in the key block

Certainly, for each IB(b), the stego key block and the chains of elements, that are extracted from the stego key block are completely different. This achieves a maximum randomization in the sequence of pixels used to hide the secret message bits and will raise the level of protection for the secret message against the attackers (Fig. 5 and 6).

The first chain of elements (yellow elements) started at (0, 0)
The second chain of elements (green elements) started at (0, 1)
The third chain of elements (red elements) started at (0, 2)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B7	63	5B	40	52	8F	A3	21	B5	34	11	20	F0	37	AD	5A
1	85	D0	AE	4B	90	14	C0	CF	94	EB	5E	76	34	79	2A	B1
2	EE	C5	66	92	FA	07	5A	FB	B8	8D	A0	D5	6E	8B	1A	32
3	FD	E4	4E	BF	4A	1A	6B	A2	A2	8B	AB	66	31	2D	EC	3B
4	0A	60	31	2B	D0	1B	60	7E	76	B2	93	02	74	EA	61	08
5	D1	2B	79	50	2B	6B	66	D4	59	C4	F0	6E	5B	F3	CA	8B
6	A1	64	CB	0D	5A	EE	61	E2	84	CF	48	97	86	68	2E	B7
7	2A	A3	95	05	B3	9B	10	9E	F9	5C	D1	0C	2A	F1	23	83
8	E8	08	61	0F	1F	53	AE	E2	CA	96	CC	5B	22	CF	4D	F1
9	95	38	43	B7	5E	C4	D7	05	54	2C	13	FD	1D	54	B7	92
A	AC	C5	AE	7E	07	1F	98	D6	F5	B2	3A	1D	CF	B4	7B	2A
B	0E	E0	77	F2	AD	6C	25	23	31	5B	BB	F2	40	B0	C4	76
C	DE	39	AF	5D	20	CF	E9	76	9F	6D	C2	AB	89	B9	36	9F
D	B1	E9	EE	3D	DD	C5	E5	3F	A0	8A	4D	AC	64	A6	96	44
E	EE	C4	3E	96	04	1E	09	3F	F6	00	53	40	AA	7A	9A	77
F	24	1B	41	56	C2	87	98	19	53	70	BD	95	81	3C	12	F8

Fig. 5: Example of (16×16) stego Key Block (KB)

The first chain of elements (yellow elements) started at (0, 0)
The second chain of elements (green elements) started at (0, 1)
The third chain of elements (red elements) started at (0, 2)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	10	26	38	49	53	64	67	69	73	40	77	17	12	23	79
1	58	41	81	47	82	86	87	97	98	100	30	56	102	103	104	105
2	78	68	106	2	19	107	108	109	111	115	35	5	117	118	29	120
3	123	113	121	126	74	128	129	13	132	133	134	93	125	136	137	92
4	39	140	143	4	144	145	146	147	148	149	75	48	153	157	122	159
5	61	160	50	60	161	162	163	164	169	170	80	27	52	171	31	173
6	141	95	174	11	96	176	94	177	179	181	182	130	71	183	28	184
7	185	186	187	188	154	189	57	151	191	51	193	16	194	195	66	196
8	198	201	202	197	180	59	72	203	204	205	206	119	208	116	209	54
9	83	210	3	76	99	84	90	131	168	211	46	190	212	213	152	9
A	36	142	14	65	214	215	167	216	219	221	139	135	37	24	15	34
B	22	43	150	155	25	70	222	1	112	223	224	225	226	21	227	127
C	88	228	33	229	85	7	230	231	232	233	32	175	207	234	235	8
D	42	62	236	237	165	6	217	91	238	239	240	241	242	166	89	243
E	44	244	178	245	114	218	246	247	199	63	158	101	138	248	45	249
F	18	55	156	172	250	220	200	251	252	192	20	110	253	124	254	255

Fig. 6: The series of elements based on the extracted chains from the stego key block in Fig. 5

RESULTS AND DISCUSSION

The proposed image steganography technique has been implemented using a C# programming language in Visual Studio 2011. And using a computer system has Intel (Core-i3) 2.40 GHz processor and 4.0 GB memory. The proposed method has been tested on a set of standard color images of different sizes has been used to embed different secret messages. The total image size is: (Width×Height×Palette) where Palette = 3 and represents the three colors Red, Green and Blue.

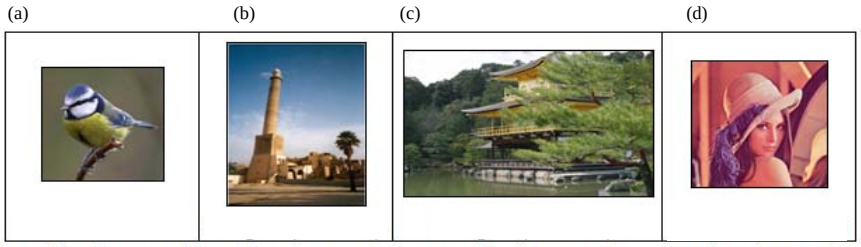

Fig. 7: Set of original images used in experiments as covers images: a) Image 1 (128×128); b) Image 2 (375×472); c) Image 3 (640×400) and d) Image 4 (256×256)

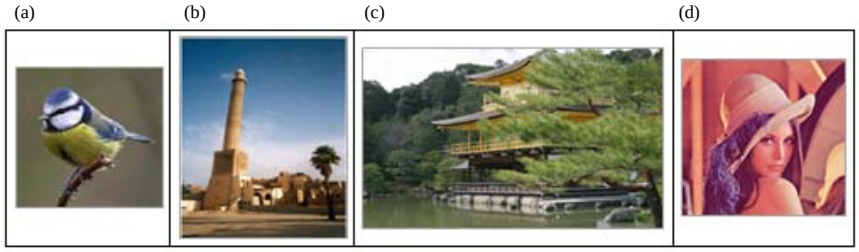

Fig. 8: Stego images that contain secret messages of the cover images in Fig. 7

Table 2: The results recorded in the experiments of the traditional LSB and the proposed steganography techniques

Image name	Image size (byte)	Length of secret message (byte)	LSB technique	NMAE (%)	SNR (dB)	Time (sec)
1	49152	6144	Traditional	0.51	43.28	0.53
			Proposed	0.52	43.33	0.82
2	531000	66375	Traditional	0.41	45.75	0.44
			Proposed	0.41	45.78	0.73
3	768000	96000	Traditional	0.49	44.51	1.00
			Proposed	0.49	44.49	1.80
4	196608	24576	Traditional	0.39	45.97	0.19
			Proposed	0.09	45.96	0.25

In order to assess the performance of the proposed image steganography technique and compare it with the traditional LSB technique (Yadav *et al*., 2014) both visual and statistical measurements have been used to ensure that the three major properties for any image steganography technique have been obtained (i.e., undetectability, robustness and capacity) to prove the strengths of the proposed technique.

Histogram analysis, Normalized Mean Absolute Error (NMAE), Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR) and the Time needed to complete the embedding operation has been taken into consideration in the experiments. The cover images that have been used to test the proposed technique are shown in Fig. 7. The randomly generated message bits have been regarded as hidden messages in the experiment. After the embedding step, the produced stego images are as shown in Fig. 8 and it is noticed that the imperceptibility of stego-images is high.

Capacity: It is clear that the proposed image steganography technique uses the full capacity of the cover image in order to embed the secret message bits. Although it uses a random sequence of pixels based on the (16×16) stego keys that are generated for each (16×16) block of the image but it actually uses all the pixels in the cover image. It was not possible to be achieved by most random selection based techniques. This considered a powerful point in this technique. Table 2 shows that, the number of bits equals the total number of pixels in the cover image.

Robustness: First, the time required to do the stages in the embedding operation is close to the time in the traditional LSB technique (Table 3). Second, the secret message bits are embedded in randomly selected pixels based on the stego key. It is very hard to extract the hidden message without knowing the stego key. Third, because one of the common attacks over image steganography techniques is the brute force attack. Which involves trying an exhaustive search on all possible stego keys until a valid key is found. But in the proposed technique, it is hard for the attacker guessing the stego key where the stego key size is relatively large (2048 bits).

Undetectability: The proposed image steganography technique has been evaluated to assess its performance

Table 3: Performance evaluation of the proposed method compared with other techniques (Mandal and Das, 2012; Yang and Wang, 2015; Swain, 2016)

	(Mandal and Das, 2012)		(Yang and Wang, 2015)		(Swain, 2016)		Proposed method	
Cover images 512×512×3	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Lena	1234394	40.21	196 608	41.58	1341192	46.17	1976671	31.01
Baboon	1406405	37.14	196 608	33.29	1489945	48.49	2219715	32.29
Peppers	1236715	40.37	196 608	39.43	1350251	47.06	2130772	35.66
Average	1292505	39.24	196 608	38.10	1393796	47.24	2109053	32.98

PSNR: Peak Signal to Noise Ratio, dB: decibel of the signal

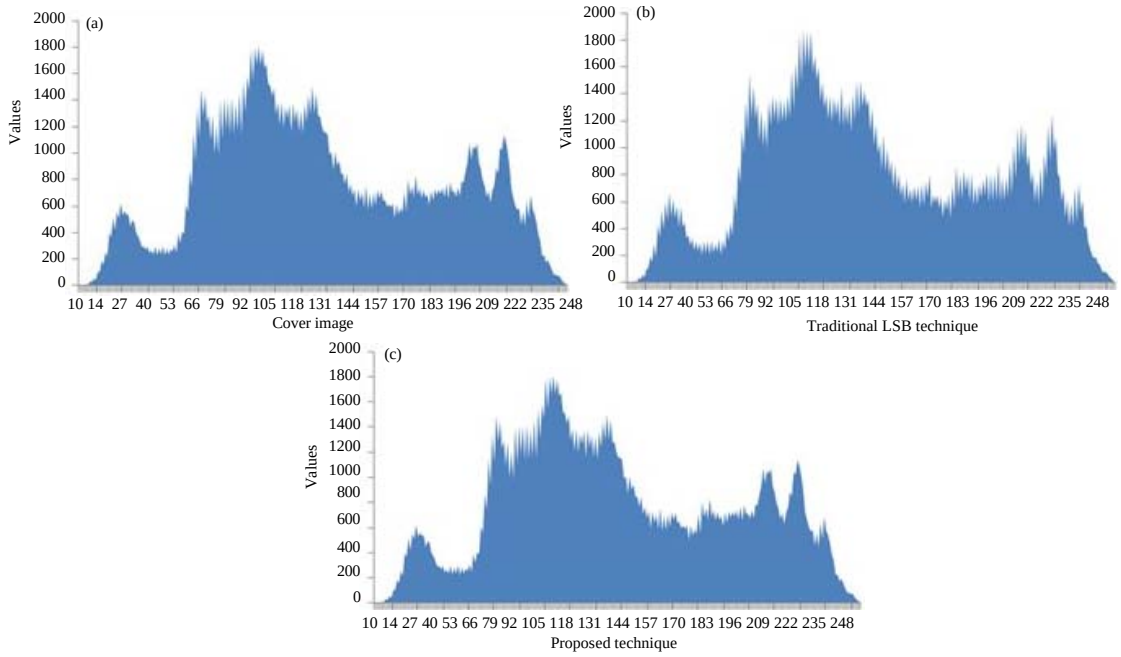

Fig. 9: Histogram of the cover and stego images used in the traditional LSB and the proposed techniques (Yadav *et al*., 2014)

by using both visual and statistical tests. Moreover, the differences in the pixels values between the stego and cover images are small and convergent in the proposed and traditional LSB techniques. It is very hard to recognize these small differences by the human eye (Fig. 7 and 8). This is the most important point of any image steganography technique and it is well achieved by the proposed image steganography technique. Table 2 summarizes the values of the three standards: NMAE, SNR and the time of hiding operation that are calculated in the proposed technique and the traditional LSB technique (Yadav *et al*., 2014).

Figure 8 shows the stego images, for the cover images (Fig. 7) that are generated during the experiments after hiding the secret message.

The histograms for the cover image and the stego image of the proposed and traditional LSB techniques have been depicted in Fig. 9. The histogram shows that, the randomness occurring due to embedding of secret message bits are not noticeable in the stego image.

The quality of stego image has been estimated in conditions of PSNR and capacity/payload. Table 3 evaluate the proposed method with (Mandal and Das, 2012; Yang and Wang, 2015; Swain, 2016) based on capacity and PSNR. We have achieved high acceptable PSNRs for stego images with a high capacity of hidden data. As a result, the proposed method gains a good performance in conditions of image capacity, visual quality and PSNR.

CONCLUSION

In this study, a secure image steganographic method has been proposed for secure transmission of secret data over the internet or cloud networks. Our method considered only capacity, robustness and imperceptibility issues. The proposed method used secret key and LSB to achieve a better trade-off between image quality, security and time complexity. We extracted chains randomly from a secret key and hide them in the LSB of the pixels in the

cover image. The sequence of elements in the extracted chains determines the sequence of the pixels that are used in the hiding operation. The proposed method maximized the randomization in the sequence of pixels to hide the secret message bits and also to improve the level of security for the secret message against adversaries.

ACKNOWLEDGEMENTS

The researchers are grateful to the Middle East University, Amman, Jordan for the financial support granted to cover the publication fee of this research article.

REFERENCES

Abhiram, M.V., S. Imadabathuni, U. Padmalochini, M. Imadabathuni and R. Ramnath, 2009. Pixel intensity based steganography with improved randomness. Intl. J. Comput. Sci. Inf. Technol., 2: 169-173.

Al-Asmari, A.K., M.A. Al-Qodah and A.S. Salama, 2011. Wavelet-pixel value differencing technique for digital images data hiding. Proceedings of the 2011 IEEE International Conference on System Engineering and Technology (ICSET'11), June 27-28, 2011, IEEE, Shah Alam, Malaysia, ISBN:978-1-4577-1256-2, pp: 15-18.

Amir, F.N. and A.R.N. Nilchi, 2013. Steganography on RGB images based on a matrix pattern using random blocks. Intl. J. Modern Educ. Comput. Sci., 5: 8-18.

Avcibas, I., M. Kharrazi, N. Memon and B. Sankur, 2005. Image steganalysis with binary similarity measures. EURASIP J. Appl. Signal Processing, 2005: 2749-2757.

Avcibas, I., M. Nasir and B. Sankur, 2001. Steganalysis of watermarking techniques using image quality metrics. Proceedings of the SPIE Conference on Security and Watermarking of Multimedia Contents III, Volume 4314, January 21-26, 2001, San Jose, USA., pp: 525-531.

Cheddad, A., J. Condell, K. Curran and P. McKevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

Chen, P.Y. and H.J. Lin, 2006. A DWT based approach for image steganography. Int. J. Applied Sci. Eng., 4: 275-290.

Desai, M.B. and S.V. Patel, 2014. Survey on universal image steganalysis. Intl. J. Comput. Sci. Inf. Technol., 5: 4752-4759.

Farid, H., 2002. Detecting hidden messages using higher-order statistical models. Proceedings of the 2002 International Conference on Image Processing, September 22-25, 2002, IEEE, Rochester, New York, USA., pp: II-905-II-908.

Fridrich, J., M. Goljan and R. Du, 2001. Detecting LSB steganography in color and gray-scale images. IEEE Multimedia, 8: 22-28.

Fridrich, J., T. Pevny and J. Kodovsky, 2007. Statistically undetectable jpeg steganography: Dead ends challenges and opportunities. Proceedings of the 9th Workshop on Multimedia and Security, September 20-21, 2007, ACM, Dallas, Texas, USA., ISBN: 978-1-59593-857-2, pp: 3-14.

Gul, G. and F. Kurugollu, 2010. SVD-based universal spatial domain image steganalysis. Trans. Inform. Foren. Sec., 5: 349-353.

Gutub, A.A.A., 2010. Pixel indicator technique for RGB image steganography. J. Emerg. Technol. Web Intell., 2: 56-64.

Hamid, N., A. Yahya, R.B. Ahmad and O.M. Al-Qershi, 2012. Image steganography techniques: An overview. Intl. J. Comput. Sci. Secur., 6: 168-187.

Han, D., J. Yang and W. Summers, 2017. Inject stenography into cybersecurity education. Proceedings of the 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA'17), March 27-29, 2017, IEEE, Taipei, Taiwan, ISBN:978-1-5090-6232-4, pp: 50-55.

Husainy, M.A.F., 2012. Message segmentation to enhance the security of LSB image Steganography. Int. J. Adv. Comput. Sci. Applic., 3: 57-62.

Kaur, S., A. Kaur and K. Singh, 2014. A survey of image steganography. Intl. J. Rev. Electron. Commun. Eng., 2: 102-105.

Lu, C.S., 2004. Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property. Idea Group Publishing, Hershey, PA., pp: 207-230.

Luo, W., F. Huang and J. Huang, 2010. Edge adaptive image steganography based on LSB matching revisited. IEEE Trans. Inform. Forensics Secur., 5: 201-214.

Mandal, J.K. and D. Das, 2012. Steganography using Adaptive Pixel Value Differencing (APVD) of gray images through exclusion of overflow/underflow. Cryptography Secur., 1: 1-9.

Manjula, Y. and K.B. Shivakumar, 2016. Enhanced secure image steganography using double encryption algorithms. Proceedings of the 3rd International Conference on Computing for Sustainable Global Development (INDIACom'16), March 16-18, 2016, IEEE, New Delhi, India, ISBN:978-1-4673-9417-8, pp: 705-708.

Purohit, A. and P.S.V.S. Sridhar, 2014. Image steganography: A review. Intl. J. Comput. Sci. Inf. Technol., 5: 4891-4896.

Qian-Lan, D., 2010. The blind detection of information hiding in color image. Proceedings of the 2nd International Conference on Computer Engineering and Technology (ICCET'10) Vol. 7, April 16-18, 2010, IEEE, Chengdu, China, ISBN:978-1-4244-6347-3, pp: V7-346-V7-348.

Rana, R. and D. Singh, 2010. Steganography-concealing messages in images using LSB replacement technique with pre-determined random pixel and segmentation of image. Intl. J. Comput. Sci. Commun., 1: 113-116.

Roy, R., A. Sarkar and S. Changder, 2013. Chaos based edge adaptive image steganography. Procedia Technol., 10: 138-146.

Saidi, M., H. Hermassi, R. Rhouma and S. Belghith, 2017. A new adaptive image steganography scheme based on DCT and chaotic map. Multimedia Tools Appl., 76: 13493-13510.

Saqer, W. and T. Barhoom, 2016. Steganography and hiding data with indicators-based LSB using a secret key. Eng. Technol. Appl. Sci. Res., 6: 1013-1017.

Sarreshtedari, S. and S. Ghaemmaghami, 2010. High capacity image steganography in wavelet domain. Proceedings of the 7th IEEE Conference on Consumer Communications and Networking (CCNC'10), January 9-12, 2010, IEEE, Las Vegas, Nevada, ISBN:978-1-4244-5175-3, pp: 1-5.

Sharma, V.K. and D.K. Srivastava, 2017. Comprehensive data hiding technique for discrete wavelet transform-based image steganography using advance encryption standard. Proceedings of the International IRSCNS 2016 Conference on Computing and Network Sustainability, July 6, 2016, Springer, Singapore, ISBN:978-981-10-3934-8, pp: 353-360.

Singh, A., S.K. Dhanda and R. Kaur, 2014. Secure image steganography using n-queen puzzle and its comparison with LSB technique. Intl. J. Innov. Technol., 3: 4-8.

Subhedar, M.S. and V.H. Mankar, 2014. Current status and key issues in image steganography: A survey. Comput. Sci. Rev., 13-14: 95-113.

Sumathi, C.P., T. Santanam and G. Umamaheswari, 2014. A study of various steganographic techniques used for information hiding. Intl. J. Comput. Sci. Eng. Surv., 4: 9-25.

Sun, Z., H. Li, Z. Wu and Z. Zhou, 2009. An image steganalysis method based on characteristic function moments of wavelet subbands. Proceedings of the 2009 International Conference on Artificial Intelligence and Computational Intelligence (AICI'09), Vol. 1, November 7-8, 2009, IEEE, Shanghai, China, ISBN:978-1-4244-3835-8, pp: 291-295.

Swain, G., 2016. Adaptive pixel value differencing steganography using both vertical and horizontal edges. Multimedia Tools Appl., 75: 13541-13556.

Thiyagarajan, P., G. Aghila and V. Venkatesan, 2010. Dynamic pattern based image steganography. J. Comput., 2: 1-9.

Tiwari, N., M. Sandilya and M. Chawla, 2014. Spatial domain image steganography based on security and randomization. Intl. J. Adv. Comput. Sci. Appl., 5: 156-159.

Trivedi, M.C., S. Sharma and V.K. Yadav, 2016. Analysis of several image steganography techniques in spatial domain: A survey. Proceedings of the 2nd International Conference on Information and Communication Technology for Competitive Strategies, March 4-5, 2016, ACM, Udaipur, India, ISBN:978-1-4503-3962-9, pp: 84:1-84:7.

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Pattern Recognit. Lett., 24: 1613-1626.

Xuan, G., Y.Q. Shi, J. Gao, D. Zou and C. Yang et al., 2005. Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions. Proceedings of the 7th International Workshop on Information Hiding (IH, 05), June 6-8, 2005, Springer, Barcelona, Spain, ISBN:978-3-540-29039-1, pp: 262-277.

Yadav, R.M., D.D.S. Tomar and D.R. Baghel, 2014. A study on image steganography approaches in digital images. Eng. Universe Sci. Res. Manage., 6: 1-6.

Yan, Y., L. Li and Q. Zhang, 2013. Universal steganalysis method based on multi-domain features. J. Inf. Comput. Sci., 10: 2177-2185.

Yang, C.Y. and W.F. Wang, 2015. Block-based colour image steganography using smart pixel-adjustment. Proceedings of the 8th International Conference on Genetic and Evolutionary Computing, October 18-20, 2014, Springer, Nanchang, China, ISBN 978-3-319-12285-4, pp: 145-154.

Zou, D., Y.Q. Shi, W. Su and G. Xuan, 2006. Steganalysis based on Markov model of thresholded prediction-error image. Proceedings of the 2006 IEEE International Conference on Multimedia and Expo, July 9-12, 2006, IEEE, Toronto, Ontario, ISBN:1-4244-0366-7, pp: 1365-1368.