Hybrid and Blind Steganographic Method for Digital Images Based on DWT and Chaotic Map

Samer Atawneh* and Putra Sumari
Univeristi Sains Malaysia (USM), Penang, 11800, Malaysia
Email: satawneh@yahoo.com; putra@cs.usm.my

Abstract—Steganography is the art and science of hiding secret information into digital media with the intention to transmit this information. Most of the steganographic methods either use spatial domain or frequency domain for embedding the secret information. Current hybrid methods require the original cover image to extract the secret information making these methods to become not practical. This paper proposes a new blind steganographic method for digital images that combines spatial and frequency domains and does not rely on the cover image in extracting the secret information. The proposed method utilizes a chaotic map to scramble the secret information before the embedding procedure takes place. A coding map is generated during the work on spatial domain, and the original image is transformed into DWT domain, then the generated coding map is embedded in the coefficients of LL and HL sub-bands of the cover image. The drawn experimental results show that the resultant stego-images have high quality and the proposed method provides high embedding capacity compared with other methods and is robust against the visual analysis and other image processing attacks such as lossy compression and added noise.

Index Terms—steganography, spatial domain, frequency domain, Haar-DWT, chaotic map.

I. Introduction

The increasing needs to provide secrecy in open networks gave an important role for steganography in the last few years [1]. The military and several governmental agencies are looking into steganography for their own secret transmissions of information. They are also desirous of discerning secret information communicated by criminals, terrorists and other aggressive forces. With power software and new devices, users worldwide gained the ability to access, develop and modify multimedia objects [2]. Steganography is the art and science of maintaining the existence of the communication secret through the concealment of the information within innocuous-looking objects [3]. Only the intended recipient can extract the hidden information correctly from the stego-media (the cover after embedding the secret information). Varying carrier file formats are utilized, despite that digital images are widely being used due to their Internet frequency [4].

Literally, the word steganography means the “covered writing" [3], [5]. Steganography is traced back to the ancient Greek centuries when messengers have the messages tattooed on their shaved heads. They then let their hair grow to have the message hidden until they reach the recipient when the need to shave their heads again arises for discerning of message [5]-[7]. Another method that was used during those times is the wax tablet for a cover source [3], [7]. In this method, text is written on the wood and covered by a layer of wax so that the tablet will appear blank upon inspection [5]. With the turn of the century, a method with the use of invisible inks was extremely popular [3]. After some time, the Germans introduced the microdot technique where microdots are considered as photographs as small as a printed period, but with a clear format of a typewritten page [4], [5]. They were included in a letter or an envelope, and because of their tiny sizes, they could be indiscernible. Documents themselves were used to hide messages; texts within the document can hide messages through null ciphers, camouflaging the actual message in an innocuous looking text. As most open-coded messages do not cause suspicion, a normal and innocent looking document is often overlooked. The main concept of contemporary steganography was described by Simmons [8] when he explained how the two prisoners, Alice and Bob, were planning to escape. They are under the surveillance of Eve, the warden, and they need to communicate in a covert way with no raising suspicion [7]. One of the earliest techniques to discuss steganography in digital media is credited to Kurak and McHugh [9], who developed a method to replace the 4 LSBs of 8-bit image by the 4 MSBs (most significant bits) of another image. They showed that contaminating digital images with information, which can be extracted later, is extremely simple.

Steganalysis is the art and science of discovering the presence of hidden information embedded into digital media. The need for reliable steganalytic methods for detecting hidden information has increasingly developed owing to the anecdotal evidence that steganography is being utilized by child pornographers and terrorists [7]. Malicious employee may discreetly transmit the organization’s sensitive information to unauthorized person [10].

Manuscript received June 27, 2013; revised October 28, 2013.

* Corresponding author: School of Computer Sciences, Univeristi Sains Malaysia.Phone: 604-653 3615; e-mail: satawneh@yahoo.com.

doi:10.12720/jcm.8.11.690-699

In security systems domain, cryptography and information hiding are the two common disciplines that are used to protect information (see Fig. 1). Cryptography is the scrambling of a secret message by using a crypto-key, so it becomes meaningless. No matter how unbreakable is the encrypted message, it will arouse suspicion, and will in itself be incriminating in some countries where encryption is prohibited [11], [12]. Steganography is superior to cryptography in a sense that it is not by means to prevent others from being privy of the hidden information, but it is to prevent them from being privy to the existence of the information [13]. It is more inconspicuous to hide information in an image than to communicate an encrypted file [4]. The main processes of a steganographic system can be graphically represented as in Fig. 2. Watermarking is the practice of altering a multimedia file to add information about that media to protect its copyright [7]. Steganography and watermarking are conceptually different in their communicative objects. While in watermarking the communication is the carrier data and the protection lies in the hidden data in the form of copyright protection, in steganography, the communication is the secret and the carrier one is just a cover [14]. Table I provides the main differences between steganography, watermarking, and cryptography.

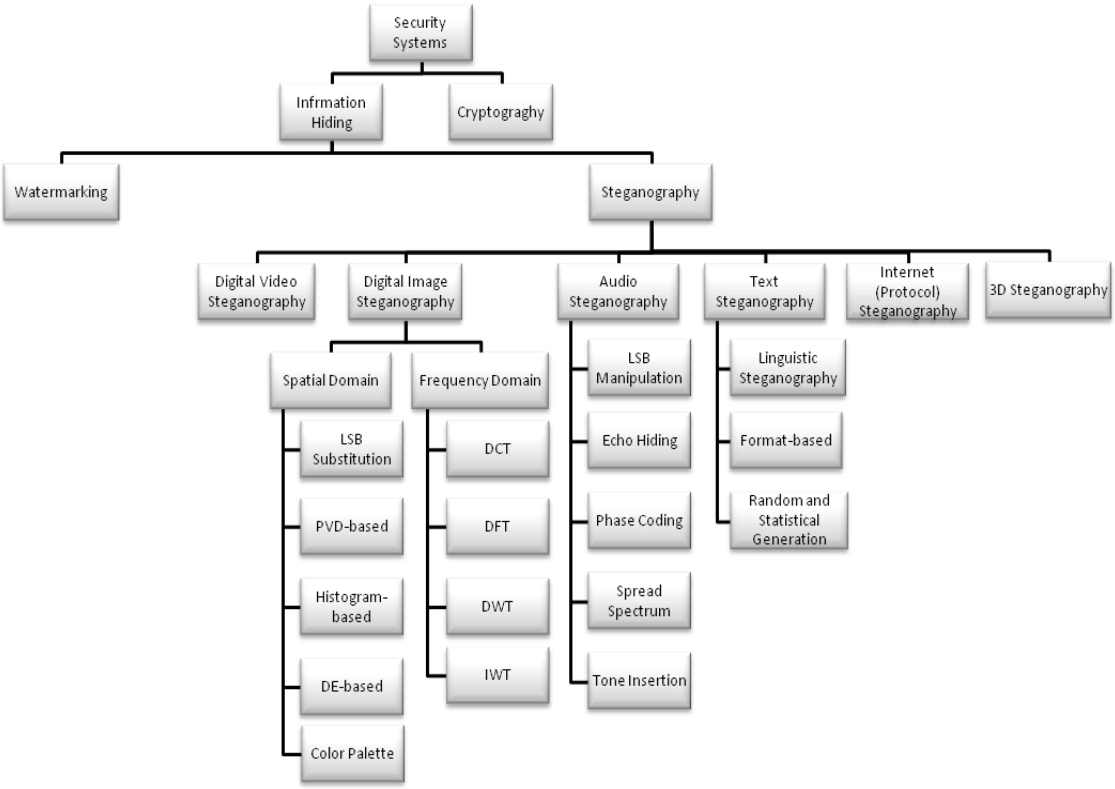


Figure 1. The umbrella of security system disciplines

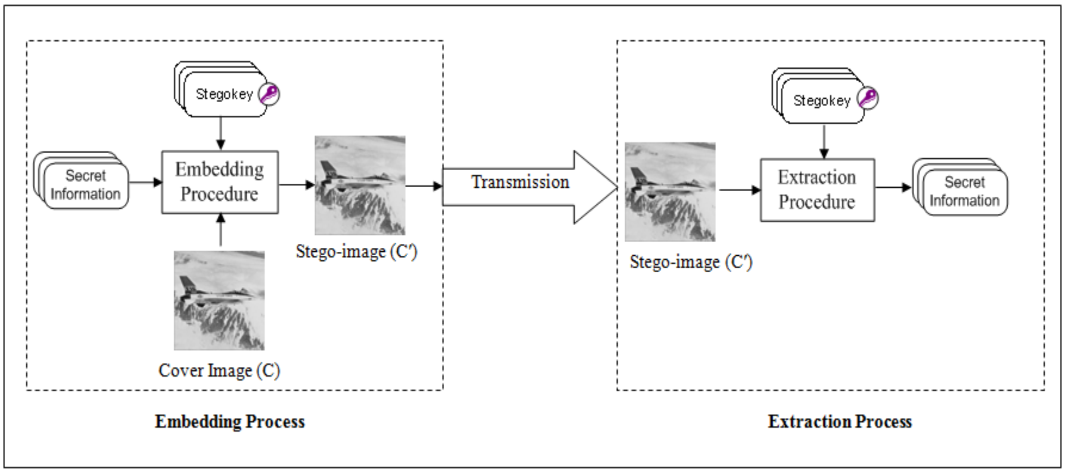


Figure 2. A general steganography system showing the embedding and the extracting processes. C denotes to the cover image and C′ denotes to the stego-image (the cover C after embedding the secret information)

The primary application of steganography is the secret communication [14]. However, steganography has a variety of other useful applications; some of the most interesting ones are file authentication [15], annotation [2], hide confidential data files (spreadsheets and documents) located inside computers [16], bank transactions [17], enhanced data structures [14], and protecting digital document files from forgery using self-embedding methods [18]. Moreover, since information can be hidden without modifying the cover media, steganography can be used for watermarking implementation [5], [19]. Steganography could also be used by dissident and criminal organizations [7].

TABLE I: DIFFERENCES BETWEEN STEGANOGRAPHY, WATERMARKING AND CRYPTOGRAPHY

Criteria	Steganography	Watermarking	Cryptography
Carrier	Any multimedia file, but image and audio files are the most used	Any multimedia file, but image and audio files are the most used	Text files
Objective	To prevent discovery of the existence of secret information	To protect digital media's copyright.	To prevent unauthorized entities from reading the contents of secret information
Significant applications	Secret communication, documents protection against forgery, authentication, and Medical imaging	Intellectual property and copyright protection	Network Communication, Information exchange protection; e-commerce, ATM encryption, online banking, and e-mail privacy
Visibility	Never	Usually not visible	Always
Types of attacks	Steganalysis	Image processing	Cryptanalysis
Fails when	Detected	Removed	De-ciphered
History in digital community	Modern era. Still being developed	Modern era. Still being developed	Common technology

The organization of the paper is as follows: section II gives the literature review of the domain. Section III presents the proposed method. Section IV shows the experimental results and analysis of the proposed method. Section V discusses the robustness of the proposed method to several attacks. Section VI draws the conclusion of the paper.

II. LITERATURE REVIEW

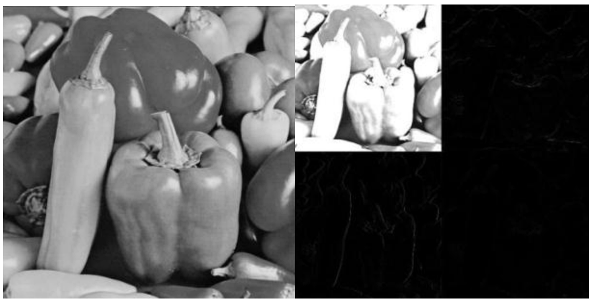
With the widespread of the digital technology, digital carriers, for example image, video and audio files, have become the most used carriers. Because they are insensitive to the Human Visual System (HVS), digital images are considered as a superior choice for hiding secret information [20], [21]. A digital image is represented as an array of numeric values that represent the intensities for various points which are called pixels. Images of monochrome and grayscales make use of 8 bits for every pixel, and they have the ability to present a total of 256 (2^8) different colors or gray shades. Images of digital colors are primarily kept in 24-bit files, where the RGB color model is used by these images, referred to as a true color. The color combinations for the pixels of a 24-bit image stem from the three primary colors of red (R), green (G) and blue (B), and 8 bits are used to represent each primary color.

Any text or digital image can be embedded in a digital image. When embedding secret information into an image, the pixels of the image are changed according to the information being embedded [22]. A digital image contains correlated amount of data in neighboring pixels, making them contain redundant information. Most digital formats are suitable for steganography, nonetheless, those with greater levels of redundancy, or noise, are more appropriate. In steganography, the selection of cover images is critical as it impacts the steganographic system's design and the security entailed [23]. It is significant not to make use of these images with large block-areas of solid colors, as changes in solid areas are easier to be detected [24]. Images having a few numbers of colors along with the computer art should not be selected [23]. It is better for steganographers to create their own cover images [25]. For the purpose of the undetection of steganography, the cover image must be completely concealed; because its exposure would reveal the changes on a comparison between it and the stego-image [23].

A. Image Steganography Domains

Steganography can be categorized in different ways. A straightforward categorization is according to the cover media used in hiding [27], [28]. Here, steganographic methods can be grouped into 6 different categories as shown in Fig. 1. In particular, they include Text steganography [29], [30], audio steganography [31], [32] image steganography [33], [34] video steganography [35], [36] protocol steganography [4], [37] and 3D steganography [38]. Cheddad *et al*. [33] gave a standard categorization by grouping the methods into spatial domain, frequency domain, and adaptive techniques. Spatial domain steganography embeds the secret information in the LSBs of the cover image's pixels selected sequentially or randomly. The advantages of spatial-domain methods comprise high payload and simple embedding of secret message bits to the LSB plane of the cover image in a direct way [13]. However, its sensitivity to filtering or to the changes in the stego-image is the major weakness. On the contrary of spatial domain steganography, the frequency domain steganography mainly embeds the secret information in the transform coefficients, and manages to satisfy the criteria of imperceptivity, as well as robustness [39]. Many frequency domain variations have been proposed in Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transformation (DWT), and Integer Wavelet Transformation (IWT).

Current researchers make use of the DWT owing to its widespread application in the image JPEG2000 compression standard [40]. The DWT can be performed by utilizing one of the wavelet transforms (known as filter banks). The most widely used filter banks are the Haar-DWT and the Daubechies-DWT [41]. The Haar-DWT can be used to decompose a two-dimensional image by first applying the 1-D Haar-DWT to each row of the image, then applying it again to each column of the image [42]. Upon applying the Haar-DWT on a 2-D image, the image is decomposed into one approximation sub-band known as LL sub-band and three details sub-bands namely LH, HL, and HH sub-bands [43]. The significant part of the image's spatial-domain exist in the approximation sub-band (LL sub-band) which holds the low-frequency coefficients, while other details of the image (the edge details) exist in the high-frequency sub-bands (LH, HL, and HH sub-bands). Fig. 3 shows an example of decomposing an 8-bit image after applying one level Haar-DWT to it.



(a) (b)

Figure 3. Discrete wavelet transform (DWT) (a) Original image "Peppers" (b) Result after one-level decomposition with 2-D Haar-DWT.

Nag *et al*. [44] proposed a hiding method based on encoding the secret message bits by Huffman coding prior to the embedding phase to increase the embedding capacity. 3 LSBs of wavelet coefficients in the high frequency sub-bands are then replaced by 3 bits from the encoded secret bit stream. However, the experimental results showed that the average PSNR value is nearly 44dB for the embedding capacity of 0.75 bit per coefficient (pbc). In addition, embedding in HH sub-band is not robust against attacks such as lossy compression [45], [46]. Current hybrid embedding methods that are available in the literature require the cover image to extract the secret information [47], [48]. In [48], authors utilized the spatial domain of the cover image and created a coding map for the secret bits then the resultant coding map is embedding into the DCT domain using a noise adding technique. Joshi *et al*. [48] presented a steganographic method where the secret information is first embedded in the LSBs of a cover image by utilizing the LSB substitution technique then the resultant stego-image is embedded again in the HH sub-band of another cover image obtained by applying first-level DWT to the image. While these methods may provide a reasonable embedding capacity, the using of the original cover images to extract the embedded secret information is not practical and may reduce the strength of the proposed methods. In this paper, the combination of spatial and DWT domains are utilized to develop a new information hiding method where the secret information is extracted from the stego-image without a reference to the cover image. The proposed method has good performance in terms of image quality and embedding capacity, and it is robust against the visual analysis and image processing attacks.

III. Proposed Method

In this section, a new hiding method that utilizes both spatial and frequency domains is presented. The contribution here is to develop a blind method, which means that the secret information can be extracted only from the stego-image without referencing the cover image, that is, a blind extraction. In addition, to add more robustness to the proposed method, only the 2-most significant bits (i.e., 8th and 7th bit planes) of each pixel in the cover image are utilized in the embedding process. This is because the existence of the trade-off between the robustness and the bit level utilized in the embedding as shown in Fig. 4; where choosing the correct bit level can effectively affect the robustness of the resultant stego-image.

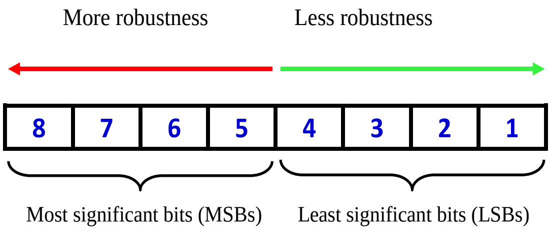


Figure 4. An 8-bit pixel shows the relationship between robustness and bit level

To increase the security of the proposed method, a chaotic map is utilized to scramble the secret image before the embedding procedure takes place. A coding map is generated during the work on spatial domain, and the cover image is transformed into 1-level DWT domain, then the generated coding map is embedded in the coefficients of LL and HL sub-bands of the cover image. The drawn experimental results show that the resultant stego-images have high quality and the proposed method provides high embedding capacity compared with other methods and is robust against the visual analysis and other image processing attacks such as lossy compression, adding noise.

A. Arnold Cat Map

Arnold's Cat Map is one of the simplest scrambling methods used to randomize the image by shuffling the pixels without changing their values. A 2D Arnold Cat Map of N × N digital image is defined as:

$$\begin{bmatrix} x_i' \\ y_i' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} \ (mod\ N) \qquad (1)$$

where $(x_i, y_i) \epsilon \{0,1,2, \ldots . N-1\}$ represents a pixel's coordinates of the original image and (x_i', y_i') is the new pixel's coordinate of (x_i, y_i) after transformation. The scrambling degree is used to measure the encryption quality of the Arnold Transform. After 20 iterations, the scrambling degree for the image will be high [49]. Fig. 5 shows an example of using Arnold Cat Map to scramble the original image.

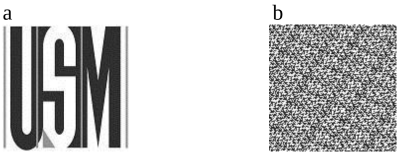


Figure 5. Arnold Cat Map (a) the original image "USMLOGO" of size 128×128, and (b) the transformed image after 45 iterations

B. Embedding Procedure

Let C be a grayscale image of size M × N, and S be the secret image of size m × n. The embedding phase is shown in Fig. 6 and the detailed steps are given below.

Input: A Cover image C of size M × N, secret image S of size m × n.

Output: Stego-image C'.

Step 1: Use a pseudorandom number generator (PRNG) to generate a random integer greater than 20 and less than 150. This random number will be used as a secret key k_1.

Step 2: Use Arnold Cat Map to scramble the secret image S by k_1 iterations to obtain the scrambled secret image S'.

Step 3: Use the pseudorandom number generator (PRNG) again to generate two random integers between 0 and 255. Use these random integers as secret keys k_2 and k_3 in Step 4.

Step 4: For secret bits in S', scan the cover image C starting from pixel $p(k_2, k_3)$ and perform the XOR operation between the 2-most significant bits (2-MSBs) of each pixel in C and 2 bits from S'.

Step 5: Create a coding map to save the results of XOR operations.

Step 6: Utilize the 1-level Haar-DWT to transform the cover image from its spatial domain to the frequency domain.

Step 7: Embed the coding map into the 2nd bit plane of the DWT coefficients of LL and HL sub-bands of the cover image utilizing the LSB substitution technique.

Step 8: Apply the inverse Haar-DWT to obtain the stego-image C'.

To reduce the error caused due to the embedding procedure, an adjustment process is applied. It is performed to enhance the quality of the resultant stego-images without affecting the hidden secret bits. It can lead to a gain of around 1 dB in the quality of resultant stego-images. The pixel (p', q') in the stego-image is replaced by the pixel (p'', q'') according to the following adjustment process:

$$(p'', q'') = \begin{cases} (p', q') + 1, & if\ 2^{nd} bit\ plane = 1\ and\ secret\ bit = 0 \\ (p', q') - 1, & if\ 2^{nd} bit\ plane = 0\ and\ secret\ bit = 1 \\ (p', q'), & otherwise \end{cases} \qquad (2)$$

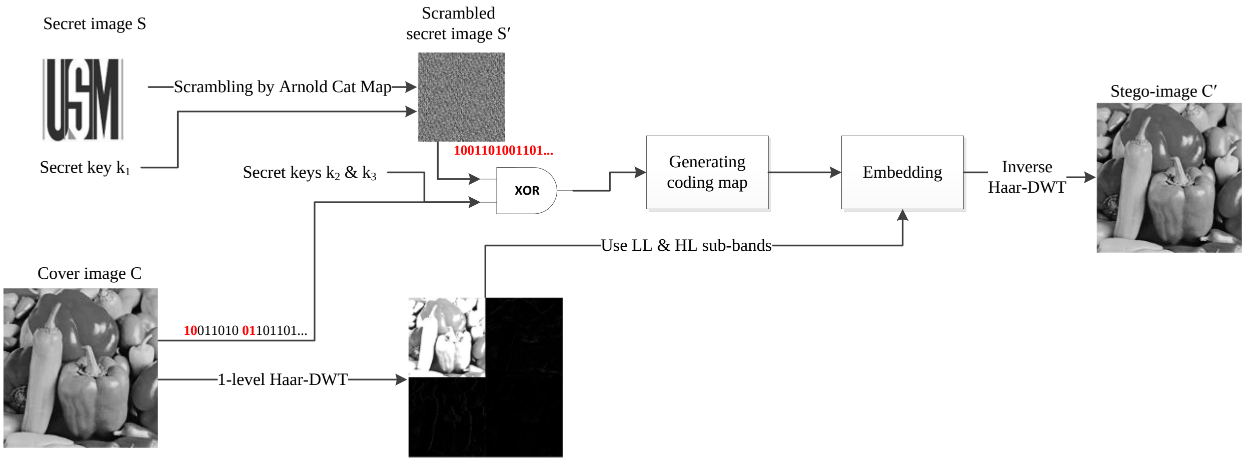


Figure 6. The flow diagram of embedding procedure using the proposed hybrid method

C. Extraction Procedure

Once the stego-image C' and secret keys k_1, k_2, and k_3 are obtained, the embedded secret image can readily be extracted from C'. The extraction phase is shown in Fig. 7 and the extracting steps are given as follows:

Input: A stego-image C', secret keys k_1, k_2, and k_3, size of secret image $m \times n$.

Output: Secret image S.

Step 1: Use the 1-level Haar-DWT to transform the stego-image C' from its spatial domain to the frequency domain.

Step 2: Extract the 2nd bit plane of each coefficient of LL and HL sub-bands and obtain the coding map.

Step 3: Use the resultant coding map and secret keys k_2 and k_3 to perform the XOR operations between the 2-most significant bits (2-MSBs) of each pixel $p(k_2, k_3)$ in C' and 2 secret bits obtained from the resultant coding map to generate the scrambled secret bits.

Step 4: Combine each 8 bits together to obtain the pixel values of the scrambled secret image S'.

Step 5: Use Arnold's cat map and secret key k_1 to obtain the pixels of the secret image S.

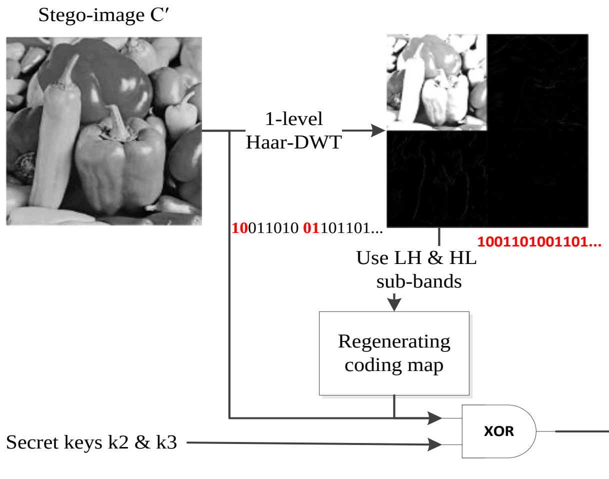


Figure 7. The flow diagram of extracting procedure using the proposed hybrid method

D. Simple Example

To show how the proposed method works, assume that the secret pixel from S' to be embedded is $(11001101)_2$, and a cover image C is composed of 4 pixels $(01011001)_2$, $(11101000)_2$, $(10011011)_2$ and $(01010110)_2$, then the resultant coding map is [1, 1, 0, 0, 1, 0, 1, 0]. Here, the first two ones in this coding map are produced by applying the XOR operation between the first 2-LSBs of the secret pixel and 8th and 7th bit planes of the cover image. The LSB substitution is then utilized to embed this coding map in the coefficients of LL and HL sub-bands of the cover image C that are obtained by applying Haar-DWT. The inverse Haar-DWT is applied and the stego-image C' is transmitted to the receiver.

During the extraction phase, with the knowledge of the size of the secret image and the secret keys k_1, k_2, and k_3, the secret image can readily be extracted from the stego-image C'. After the stego-image C' is transformed into its frequency domain using Haar-DWT, the 2nd bit plane of each coefficient of LL and HL sub-bands is extracted to obtain the coding map. If, for example, the obtained coding map is [1, 1, 0, 0, 1, 0, 1, 0] and the pixels of the cover image C have the values $(01011001)_2$, $(11101000)_2$, $(10011011)_2$ and $(01010110)_2$, then the resultant secret pixel is equal to $(11001101)_2$, which is the same value as the sent pixel. After extracting all secret pixels from the stego-image C', the Arnold Cat Map and the secret key k_1 are used to obtain the pixels of the secret image S.

Compared with other hybrid methods that are available in the literature, this method is a blind method; which means that the secret information can be extracted only from the stego-image without referencing the cover image. In addition, any hacker who tries to extract the secret image from the stego-image must know the following security parameters:

1) The algorithm used in extracting the secret image from the stego-image C'.
2) The secret keys k_1, k_2, and k_3.
3) The number of MSBs of the cover image's pixels utilized in generating the coding map.
4) The used frequency domain, which is DWT domain.
5) The size of the secret image.
6) The working on both domains – spatial and frequency domains.
7) The use of Arnold's Cat Map in scrambling the secret information

By adopting these parameters, the proposed steganographic method is more secure against attacks than any other methods that are available in the literature.

IV. Experimental Results and Analysis

This section presents the experimental results of the proposed technique. In our experiments, six 8-bit digital images of sizes 512 × 512 were used as test images to evaluate the performance of the proposed method where five of these images are benchmark images. These images are shown in Fig. 8 (a)-(f). Fig. 5 (a) was used as a secret image and the embedding capacity is 131,072 bits. Fig. 8 (g)-(l) shows the stego-images generated by the proposed method. It is clear that the proposed method does not produce any visual difference between any stego-image and its corresponding cover image.

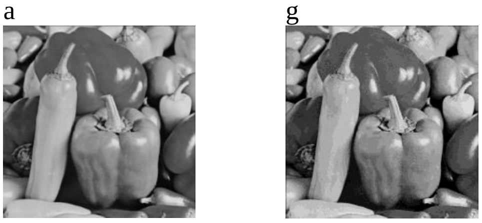
The proposed method is also tested using the visual analysis. The visual analysis of the image is performed by computing the peak signal-to-noise-ratio (PSNR). PSNR is used to measure the quality of a stego-image through a comparison between the cover image and the stego-image. PSNR is defined as:

$$PSNR = 10\log_{10}\frac{(2^{d}-1)^2}{MSE}dB \qquad (3)$$

where d denotes to the bit depth of the cover image. The MSE denotes to the mean square error between the cover image and the stego-image, and is defined as:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(S_{\text{ij}} - C_{ij}) \qquad (4)$$

where S_{ij} and C_{ij} denote to the pixel values of the cover image and the stego-image, respectively. M and N represent the dimensions of the cover image. The PSNR value that is lower than 30dB implies a low quality image, i.e., the embedding distortion can be obvious, while 40dB and above imply a high quality stego-image [33]. Table II shows the PSNR values of different stego-images generated by the proposed method. This table shows that all the PSNR values exceed 47dB. Thus, this concludes that the distortion which results due to the embedding process is invisible for human perception. Furthermore, a comparison with other related algorithms is presented in Table III. It is clear from the table that the proposed algorithm produces the lowest visual distortion to the original cover images after the embedding of 131072 bits.



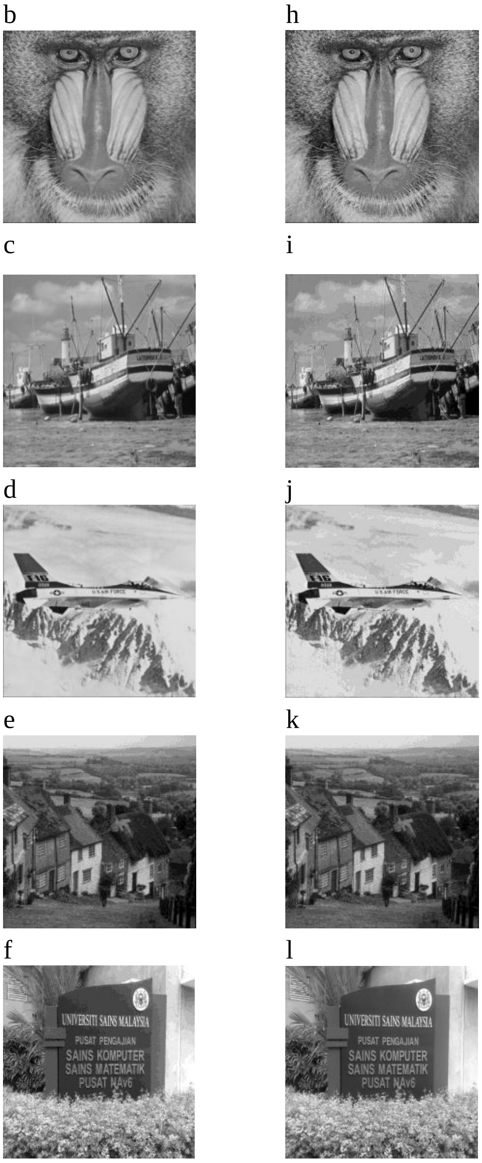


Figure 8. The experimental results of the proposed method: (a)-(f) the test images, (g)-(l) the stego-images.

TABLE II. QUALITY RESULTS FOR DIFFERENT STEGO-IMAGES

Stego-image	PSNR (dB)
Peppers	47.3493
Babban	47.4408
Boat	47.4854
Airplane	47.0534
Goldhill	47.3156
School	47.4041
Average	**47.3414**

TABLE III. QUALITY COMPARISONS WITH OTHER STEGANOGRAPHIC METHODS

Method	Transform used	Cover Image used	Payload (Bit)	PSNR (dB)
El Safy et al.[1]	IWT	Barbara 512 × 512	36850	38
Nag et al. [44]	DWT	Lena 512 × 512	130560	45.7064
Bhattacharyya & Sanyal [50]	DWT	Peppers 512 × 512	40000	34.472
Hemalatha et al. [51]	DWT	Peppers 512 × 512	131072	45
Narasimmalou & Joseph, 2012 [52]	DWT	Non-Benchmark 512 × 512	131072	33.5338
Proposed	DWT	Peppers 512 × 512	131072	47.3493
		Lena 512 × 512		47.3158
		Barbara 512 × 512		47.4077

V. Robustness of the Proposed Method

This section discusses the robustness of the proposed method to visual attacks. Image processing attacks such as lossy compression and salt and pepper were also performed to evaluate the robustness of the proposed method. Fig. 9 shows the cover image “Peppers” where Fig. 10 shows the result of compression attack. Fig. 11 shows the result of “Salt-and-Pepper” added noise. Fig. 12 shows the result of a visual attack. It is obvious that the proposed method can resist image processing and visual attacks.

Figure 9. The cover image “Peppers”

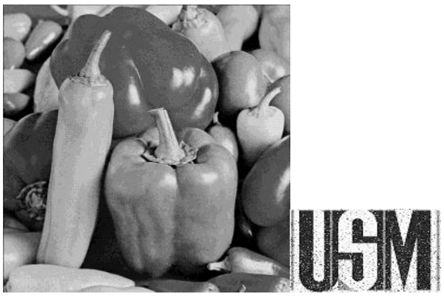


Figure 10. The stego-image after lossy compression attack (QF = 100%) and the generated secret image

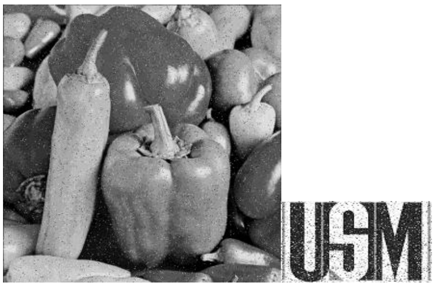


Figure 11. The stego-image after “Salt & Pepper” added noise and the generated secret image

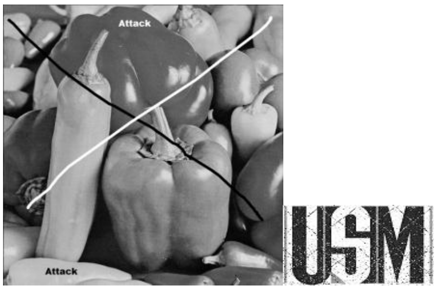


Figure 12. The stego-image after visual attack and the generated secret image

VI. Conclusion and Future Work

Blind and Hybrid steganographic methods can enhance the security of steganography since the secret information can be extracted from the stego-images without a reference to the original cover images. In this paper, a new simple embedding method that works on both spatial and DWT domains was proposed. Before embedding procedure starts, the secret image is scrambled by a chaotic map to increase the security of the proposed method, and the original image is transformed into DWT domain. A coding map is generated and then embedded in the coefficients of the LL and HL sub-bands of the cover image. For better extraction of the secret information, 3rd or 4th bit planes of the DWT’s coefficients can be utilized instead of using 1st bit plane to hide the secret information. While this may affect the quality of the stego-image, the extracted secret information has better quality if compared with extracted information from 1st bit plane. Additionally, the robustness can be increased. The drawn experiments showed that the proposed method has good performance in terms of image quality and embedding capacity, and it is robust against the visual analysis and image processing attacks such as “lossy compression,” and “salt and pepper” added noise. As future work, recent steganalysis algorithms such as ensemble classifier [53] and Extractor of 274 Merged Features [54] will be used to measure the undetectability of the proposed method. In addition, the proposed method will be improved to increase its robustness against other digital image attacks such as cropping and shifting.

References

[1] R. El Safy, H. Zayed, and A. El Dessouki, "An adaptive steganographic technique based on integer wavelet transform," in *Proc. International Conference on Networking and Media Convergence*, Cairo, 2009, pp. 111-117.

[2] M. Wu and B. Liu, "Data hiding in image and video. I. fundamental issues and solutions," *IEEE Transactions on Image Processing*, vol. 12, pp. 685-695, 2003.

[3] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer, IEEE*, vol. 31, pp. 26-34, 1998.

[4] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography," in *Proc. Fifth Annual Information Security South Africa Conference*, Sandton, South Africa, 2005, pp. 1-12.

[5] R. Krenn, "Steganography and steganalysis", University of California, City, January 2004.

[6] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. United Kingdom: Cambridge University Press, 2009, ch. 1.

[7] J. C. Ingemar, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. USA: Burlington, Morgan Kaufmann, 2008, pp. 1-624.

[8] G. J. Simmons, "The prisoners’ problem and the subliminal channel," in *Proc. International Conference on Advances in Cryptology*, Paris, 1984, pp. 51-67.

[9] C. Kurak and J. McHugh, "A cautionary note on image downgrading," in *Proc. Eighth Annual Computer Security Applications Conference*, San Antonio, Texas, 1992, pp. 153-159.

[10] J. Blasco, J. C. Hernandez-Castro, J. M. de Fuentes, and B. Ramos, "A framework for avoiding steganography usage over http," *Journal of Network and Computer Applications*, vol. 35, no. 1, pp. 491-501, 2012.

[11] D. Bloisi and L. Iocchi, "Image based steganography and cryptography," *Computer Vision theory and applications*, vol. 1, pp. 127-134, 2007.

[12] D. T. Meva and A. D. Kothari, "Adoption of neural network approach in steganography and digital watermarking for covert communication and copyright protection," *International Journal of Information Technology and Knowledge Management*, vol. 4, pp. 527-529, 2011.

[13] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Shamsuddin, "Information hiding using steganography," in *Proc. 4th National Conference on Telecommunication Technology*, Shah Alam, Malaysia, 2003, pp. 21-25.

[14] P. Wayner, *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*. USA: Morgan Kaufmann Publishers, 2009, ch. 1.

[15] W. Bender, W. Butera, D. Gruhl, R. Hwang, F. Paiz, and S. Pogreb, "Applications for data hiding," *IBM Systems Journal*, vol. 39, pp. 547-568, 2000.

[16] C. Bergman and J. Davidson, "An artificial neural network for wavelet steganalysis," in *Proc. Mathematical Methods in Pattern and Image Analysis*, San Diego, CA, 2005, pp. 1-10.

[17] S. Premkumar and A. Narayanan, "New visual steganography scheme for secure banking application," in *Proc. International Conference on Computing, Electronics and Electrical Technologies*, Kumaracoil, 2012, pp. 1013-1016.

[18] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "A secure and improved self-embedding algorithm to combat digital document forgery," *Signal Processing*, vol. 89, pp. 2324-2332, 2009.

[19] H. C. Huang and W. C. Fang, "Techniques and applications of intelligent multimedia data hiding," *Telecommunication Systems*, vol. 44, pp. 241-251, 2010.

[20] S. Das, B. Bandyopadhyay, and S. Sanyal, "Steganography and steganalysis: Different approaches," *Information Technology and Engineering*, vol. 2, pp. 1-11, June 2008.

[21] A. Kanso and H. S. Own, "Steganographic algorithm based on a chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, pp. 3287–3302, 2012.

[22] C. C. Lin, "An information hiding scheme with minimal image distortion," *Computer Standards & Interfaces*, vol. 33, pp. 477-484, 2011.

[23] J. Fridrich, M. Goljan, and D. Hogea, "Steganalysis of jpeg images: Breaking the f5 algorithm," in *Proc. Information Hiding Conference*, Noordwijkerhout, Netherlands, 2003, pp. 310-323.

[24] S. Atawneh, "A new algorithm for hiding gray images using blocks," in *Proc. Information and Communication Technologies*, Damascus, 2006, pp. 1484-1488.

[25] K. Curran, X. Li, and R. Clarke, "An investigation into the use of the least significant bit substitution technique in digital watermarking," *American Journal Applied Sciences*, vol. 2, pp. 648-654, 2005.

[26] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *Security & Privacy, IEEE*, vol. 1, pp. 32-44, 2003.

[27] Z. K. AL-Ani, A. Zaidan, B. Zaidan, and H. Alanazi, "Overview: Main fundamentals for steganography," *Journal of Computing*, vol. 2, pp. 158-165, 2010.

[28] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, "A tutorial review on steganography," in *Proc. International Conference on Contemporary Computing*, Noida, India, 2008, pp. 105-114.

[29] L. Por, B. Delina, Q. Li, S. Chen, and A. Xu, "Information hiding: A new approach in text steganography," in *Proc. 7th WSEAS Int. Conf. on Applied Computer & Applied Computational Science*, Hangzhou, China, 2008, pp. 689-695.

[30] L. Yee, K. S. Wong, and K. O. Chee, "Unispach: A text-based data hiding method using unicode space characters," *Journal of Systems and Software*, vol. 85, pp. 1075-1082, 2012.

[31] F. Djebbar, B. Ayad, H. Hamam, and K. Abed-Meraim, "A view on latest audio steganography techniques," in *Proc. International Conference on Innovations in Information Technology*, Abu Dhabi, 2011, pp. 409-414.

[32] M. L. M. Kiah, B. Zaidan, A. Zaidan, A. M. Ahmed, and S. H. Al-bakri, "A review of audio based steganography and digital watermarking," *Int. J. Phys. Sci*, vol. 6, pp. 3837-3850, 2011.

[33] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, pp. 727-752, 2010.

[34] A. Ioannidou, S. T. Halkidis, and G. Stephanides, "A novel technique for image steganography based on a high payload method and edge detection," *Expert Systems with Applications*, vol. 39, pp. 11517–11524, 15 October 2012.

[35] D. Stanescu, M. Stratulat, B. Ciubotaru, D. Chiciudean, R. Cioarga, and M. Micea, "Embedding data in video stream using steganography," in *Proc. 4th International Symposium on Applied Computational Intelligence and Informatics*, Timisoara, Romania, 2007, pp. 241-244.

[36] S. Bhattacharyya and G. Sanyal, "A novel approach of video steganography using pmm," in *Proc. 6th International Conference on Information Processing*, Bangalore, India, 2012, pp. 644-653.

[37] B. Xu, J. Wang, and D. Peng, "Practical protocol steganography: Hiding data in ip header," in *Proc. First Asia International Conference on Modelling & Simulation*, Phuket, 2007, pp. 584-588.

[38] K. Rama, K. Thilagam, S. M. Priya, A. Jeevarathinam, and K. Lakshmi, "Survey and analysis of 3d steganography," *International Journal of Engineering Science and Technology*, vol. 3, pp. 638-643, 2011.

[39] M. Chen, R. Zhang, X. Niu, and Y. Yang, "Analysis of current steganography tools: Classifications & features," in *Proc. International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, Pasadena, CA, USA, 2006, pp. 384-387.

[40] E. Ghasemi, J. Shanbehzadeh, and B. ZahirAzami, "A steganographic method based on integer wavelet transform and genetic algorithm," in *Proc. International Conference on Communications and Signal Processing*, Calicut, India, 2011, pp. 42-45.

[41] A. A. Abdelwahab and L. A. Hassaan, "A discrete wavelet transform based technique for image data hiding," in *Proc. National Radio Science Conference*, Tanta Univ., Cairo, 2008, pp. 1-9.

[42] O. M. Al-Qershi and B. Ee Khoo, "Two-dimensional difference expansion (2d-de) scheme with a characteristics-based threshold," *Signal Processing*, vol. 93, pp. 154–162, 2012.

[43] S. Barve, U. Nagaraj, and R. Gulabani, "Efficient and secure biometric image stegnography using discrete wavelet transform," *International Journal of Computer Science & Communication Networks*, vol. 1, pp. 96-99, 2011.

[44] A. Nag, S. Biswas, D. Sarkar, and P. P. Sarkar, "A novel technique for image steganography based on dwt and huffman encoding," *International Journal of Computer Science and Security*, vol. 4, pp. 561-570, 2011.

[45] M. R. Keyvanpour and F. Merrikh-Bayat, "Robust dynamic block-based image watermarking in dwt domain," *Procedia Computer Science*, vol. 3, pp. 238-242, 2011.

[46] M. Keyvanpour and F. M. Bayat, "Blind image watermarking method based on chaotic key and dynamic coefficient quantization

in the dwt domain," *Mathematical and Computer Modelling*, vol. 58, no. 1-2, pp. 56-57, 2013.

[47] A. I. Hashad, A. S. Madani, and A. Wahdan, "A robust steganography technique using discrete cosine transform insertion," in *Proc. 3rd International Conference on Information and Communications Technology* Cairo, 2005, pp. 255-264.

[48] S. V. Joshi, A. A. Bokil, N. A. Jain, and D. Koshti, "Image steganography combination of spatial and frequency domain," *International Journal of Computer Applications*, vol. 53, pp. 25-29, September 2012.

[49] S. Singh and T. J. Siddiqui, "A security enhanced robust steganography algorithm for data hiding," *International Journal of Computer Science Issues*, vol. 9, pp. 131-139, 2012.

[50] S. Bhattacharyya and G. Sanyal, "A robust image steganography using dwt difference modulation (dwtdm)," *International Journal of Computer Network and Information Security*, vol. 4, pp. 27-40, 2012.

[51] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A novel colorimage steganography using discrete wavelet transform," in *Proc. Second International Conference on Computational Science, Engineering and Information Technology*, Coimbatore, India, 2012, pp. 223-226.

[52] T. Narasimmalou and R. Joseph, "Discrete wavelet transform based steganography for transmitting images," in *Proc. International Conference on Advances in Engineering, Science and Management*, Nagapattinam, Tamil Nadu, 2012, pp. 370-375.

[53] J. Kodovsky, J. Fridrich, and V. Holub, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 432-444, 2012.

[54] T. Pevný and J. Fridrich, "Merging markov and dct features for multi-class jpeg steganalysis," in *Proc. SPIE Electronic Imaging*, San Jose, CA, USA, 2007, pp. 1-13.

Samer Atawneh received his Master degree in Computer Science from University of Jordan in 2003. Currently, Mr. Atawneh is a Ph.D. candidate at the School of Computer Sciences, Universiti Sains Malaysia (USM), Malaysia. His research interests lie in Computer Security and Digital media fields like Steganography in Digital Images.

Putra Sumari obtained his MSc and PhD in 1997 and 2000 from Liverpool University, England. Currently, he is associate professor and lecturer at School of Computer Science, Universiti Sains Malaysia. He is a member at ACM and IEEE and a reviewer of several journals and International Conferences. He has published more than hundred papers including journal and conferences. His research areas are multimedia communication, specifically on video on demand system, content distributing network and image retrieval.