



Available online at: <http://www.basra-science-journal.org>



ISSN -1817 -2695

Received 5-5-2015, Accepted 24-2-2016

Using IWT and LSB Method to Hide Encrypted image in Color image

Iman Qays Abduljaleel

Dept. of Computer Science/ College of Science/ University of Basra
emankais@yahoo.com

Abstract

In this paper, we transmit an encrypted secret image, where an image is used as medium to hide the encrypted secret image, called *cover image*. So, we have first encrypted a secret image by using Integer Wavelet Transform (IWT), then the secret image is scrambled by Arnold transform and xored operation with a two-type of chaotic map key to protect a cipher image and enhance the security. This proposed technique can achieve the perfect reversibility that is image recovery and data extraction are free of any error. In steganography stage, we have used the least significant bit (LSB) method to hide the three planes of the encrypted color image into true image. A modified scanning ordering is used, and IWT in each block divides into the hiding image.

This method presents a new data hiding system in which steganography and cryptography are used to deny unauthorized data access. The experimental results show that the assessment metric such as peak signal to noise ratio (PSNR) and Mean Square Error (MSE) is high imperceptibility for hidden images and significant encryption of information images. The time required for encryption and decryption is between 0.4043- 0.77641 seconds.

Keywords: steganography, cryptography, LSB, Arnold transform, IWT.

1. Introduction

Image security is a very important issue nowadays. It includes different aspects like information hiding, image encryption... etc. All these are different ways of providing security to digital images [1].

The goal of steganography is to hide the information and be undetectable to human eyes. Steganography focuses entirely on keeping the adversary completely unaware of the communication while cryptography focuses on keeping the communication contents secret. These purpose differences were first recognized during the 18th century when the two issues were split into separate fields of study; which we are currently familiar with [2]. Image encryption is urgently needed, but it is a challenging task because it is quite different from text encryption due to some intrinsic properties of images, such as, huge data capacity and high redundancy, which are generally difficult to handle by using conventional techniques [3].

Steganography has three parts:-the secret message, the cover media and the key. The secret message is embedded in the cover media in such a way that no outsider can decode it and only the party having the valid key for deciphering it can retrieve the secret message from it. Various forms of data like audio, video file, image, and text can be encoded by using steganography. To get back the secret message, the reverse of steganography, called steganalysis, is used [4, 5].

Many techniques have been proposed for image steganography. The image steganography is based on the image format. The image format is classified into two categories: - (i) Spatial Domain, and (ii) Transform Domain. In the spatial domain format, the most popular technique which is the simplest and widest known

steganography method is the *least significant bit*, which replaces the least significant bit of pixels selected to hide the content that holds information [6]. We found a color image encryption algorithm combining Integer Wavelet Transform with a chaotic key, where the three color components are encrypted and hidden in another color image to get a stego image. There are a number of previous works in this area such as W. J. Chen used two types of canny and fuzzy edges detection method applied for edge computation and simple LSB substitution is used to embed the hidden data. This scheme is successful to embed data with higher peak signal to noise ratio (PSNR) with normal LSB based embedding [7]. Madhu explained an image steganography technique, based on LSB substitution and selection of random pixel of required image area. It generates the random numbers and selects the region of interest where secret message has to be hidden. The limitation of this method it is not considers any type of perceptual transparency [8]. Ching Yu Yang proposed a color image steganography method based on module substitution [9]. Three types of module substitutions are used to embed secret bits, which is based upon the base value of the blocks under consideration. To improve hiding capacity, the R, G and B component is further encoded by mod u, mod u-v and mod u-v-w substitution. Experimental results show that hiding capacity and PSNR generated are better compared to the existing techniques.

In this paper, the section II is about the related work like IWT, chaotic maps, scan methodology and Arnold transform. Section III explains the proposed algorithm. Section IV shows performance metrics and section V Discusses the results.

2. Related Work

2.1 Integer Wavelet Transform (IWT)

By using WT, the significant parts of the spatial domain image exist in the

approximation band that consists of low frequency bands and the texture details

which usually exist in high frequency sub bands. Normally, the human eyes are not sensitive to the small changes in the textures of an image but very sensitive to the small variations in the smooth parts. This helps the secret image to be embedded at high frequency sub-bands without being perceived by the eye. The discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them; hence, it is expected to make the process of imperceptible embedding more effective. The wavelet transform along with integer mapping helps to improve the effectiveness of wavelet transform [10].

Integer Wavelet Transform is much faster than the floating point arithmetic in almost all general purpose computers because the

floating point wavelet transform demands for longer data length than the integer wavelet transform does. Another benefit of using integer wavelet is the reversibility. That is, the image can be reconstructed without any loss because all the coefficients are integers and can be stored without rounding off errors. The input data consist of integer samples. The lifting scheme is modified to a transform that maps integers to integers and that is still reversible [11].

The basic functions for the spaces V_j are called scaling functions and wavelet functions which are denoted by the symbol ϕ and ψ . A simple basis for V_j is given by the set of scaled and translated box functions [12]:

$$\Phi_{r,s}(x) = 2^{r/2}\Phi(2^r x - s) \quad \dots (1),$$

$$\Phi[x] = \begin{cases} 1, & x \in [0, 1] \\ 0, & elsewhere \end{cases}$$

Where r, s is the integers and x is a variable in continuous space. And the wavelet functions are given by $\Psi_{r,s}$ [12]:

$$\Psi_{r,s}(x) = 2^{r/2}\Psi(2^r x - s) \quad \dots (2),$$

$$\Psi[x] = \begin{cases} 1, & 0 \leq x \leq 0.5 \\ -1, & 0.5 \leq x \leq 1 \\ 0, & elsewhere \end{cases}$$

Whatever function is there with in the first subspace even that also we should be able to analyze using the function which covers the next subspace and based on this subspace coverage arguments are given as[12]:

$$\Phi(x) = \sum_n h\phi(n)\sqrt{2}\phi(2x - n) \quad \dots (3),$$

$$\Psi(x) = \sum_n h\Psi(n)\sqrt{2}\phi(2x - n) \quad \dots (4),$$

In Haar basis the transform is given as $X[2k] = \frac{1}{\sqrt{2}}(x[2k] + x[2k + 1])$, $X[2k + 1] = \frac{1}{\sqrt{2}}(x[2k] - x[2k + 1])$ and the reconstruction is obtained from $x[n] = \sum_{k \in \mathbb{Z}} X[k]\phi_k[n]$. The Transformation of the 2D image is a 2D generalization of the 1D wavelet transform. It applies the 1D wavelet transform to each row of pixel values. This

operation provides us an average value along with detail coefficients for each row. Next, the transformed are treated as if they were themselves an image and apply the 1D transform to each column. The resulting values are all detail coefficients except a single overall average coefficient. In order to complete the transformation, this process is repeated recursively only on the quadrant containing averages [12].

2.2 The Chaotic Maps

Chaotic maps are nonlinear maps that exhibit chaotic behavior. The chaotic maps generate pseudo-random sequences, which are used during encryption process. Chaotic maps are sensitive to initial conditions and parameters, non-convergent, non-periodic and topologically mixing [13]. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography. Therefore, chaotic cryptosystems have more useful and practical applications [14]. In this paper, we

$$\mathbf{X}_{k+1} = \lambda \times (\mathbf{X}_k) \times (1 - (\mathbf{X}_k)) \quad \dots (5),$$

where $0 < \lambda \leq 4, k = 0, 1 \dots N$.

The parameter λ and initial value X_0 may represent the key. The parameter λ can be divided into three segments, which can be tested experimentally on following conditions: $X_0 = 0.3$. When $0 < \lambda \leq 3$, the calculation results come to the same value after several iterations without any chaotic behavior. When $3 < \lambda \leq 3.6$, the phase space concludes several points only, the system shows periodicity. While $3.6 < \lambda \leq 4$, it

$$\mathbf{X}_{k+1} = 1 + u((\mathbf{X}_k) \cos[\mathbf{t}_k] - \mathbf{Y}_k \sin[\mathbf{t}_k]) \quad \dots (6)$$

$$\mathbf{Y}_{k+1} = u((\mathbf{X}_k) \sin[\mathbf{t}_k] + \mathbf{Y}_k \cos[\mathbf{t}_k]) \quad \dots (7)$$

Where u is a parameter, typically $u=0.8$ and \mathbf{t}_k is defined by the equation:

$$\mathbf{t}_k = 0.4 - \left(\frac{6}{(1 + X_k^2 + Y_k^2)} \right) \quad \dots (8)$$

2.3 Scan Methodology

The image scanning is a formal language-based on two-dimensional spatial-accessing methodology which could efficiently specify and generate a wide range of scanning paths filling curves. The scan based pixel permutation and block transformation is a widely used technique for image encryption [17]. The SCAN is a family of formal languages such as Simple Scan, Extended Scan, and Generalized Scan, each of which can represent and generate a specific set of scanning paths. Each Scan language is defined by a set of basic scan patterns; a set of partition patterns and a set of rules to recursively compose simple scan

have used two types of chaotic maps to decreases periodic effect of the ergodic dynamical systems in the chaos-based image encryption. Types which been used are:

i. The Logistic Map:

The chaotic system that we consider here is the logistic map. The logistic map is one dimensional chaotic system with x output and input variable, one initial condition X_0 and one control parameter λ and can be described as follows [15]:

becomes a chaotic system and periodicity disappeared. So, we can conclude the logistic map does not satisfy uniform distribution property and the cryptosystems based on it have small key space and weak security[15].

ii. Ikeda Chaotic Map

In mathematics, an Ikeda map is a discrete-time dynamical system given by (6) and (7) [16]:

patterns to obtain complex scan patterns [18].

There are three basic partition patterns that include [19]: B type partition patterns, Z type partition patterns, and X type partition patterns. These are clearly shown in the Fig. (1). We have four basic scanning patterns, namely [19]: Continuous Raster C, Continuous Diagonal D, Continuous Orthogonal O, Spiral S (as shown in Fig. (2)) [18]. In this paper, we have used a modified Spiral S by scanning each block image for image size 300×300 to get a vector for each loop (as described in Fig.(3)) by reading the four sides (two rows and two columns) in the

image matrix to save it in a vector. Because we have a 150 cycle in the image matrix of

size 300*300 values we have to get a 150 vector with a length from 1196 to 2 values. This technique adds a good mixing to the image blocks before hiding a secret image in the cover image.

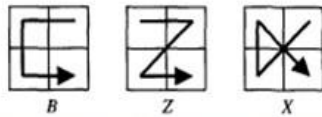
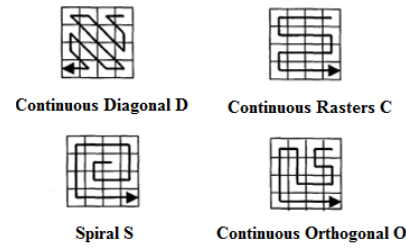


Fig. (1): Basic Partition Patterns

Fig. (2): Basic Scanning Patterns

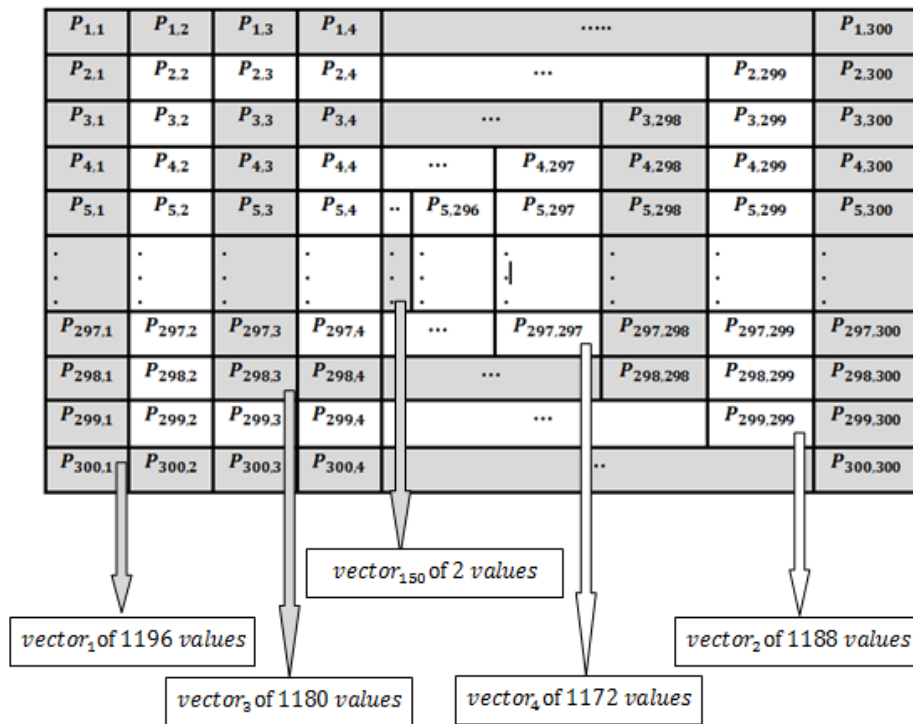


Fig. (3): Proposed Scanning patterns by using in each block of the cover image.

2.4 Arnold Transform

Arnold transform is commonly used to scramble pixels' locations. The transform is a process of clipping and splicing that realigns the pixel matrix of digital image.

Arnold transform is defined as the point (x, y) in the square matrix that transforms into the other point (x', y') [20, 21]:

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \pmod{N} = \begin{bmatrix} 1 & b \\ b & ab + 1 \end{bmatrix} \dots (9)$$

where a and b are two positive integers, and N is the order of the square matrix, $X_n, X_{n+1}, Y_n, Y_{n+1} \in \{1, 2, \dots, N-1\}$. For a digital image of size $N \times N$, the original image can be recovered after undergoing period s number of iterations [21].

Arnold mapping can be seen as to rearrange the points in the matrix of pixel values, as the number of pixel values in a digital image is limited. after N time's

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = A^{-1} \begin{bmatrix} X_n \\ Y_n \end{bmatrix} \pmod{N}, A^{-1} = \begin{bmatrix} 1 & -a \\ -b & ab + 1 \end{bmatrix} \dots (10)$$

2.5 Least Significant Bit(LSB)

It is the simplest and widest known technique for image steganography. This algorithm works for 8 bit (grayscale) or 24 bits (color image). By using this algorithm, the quality of image can be maintain by changing the negligible variations to each pixels of the image, so that, the visibility is indictable. Based on logical operation, the algorithm embeds one pixel value of secret image to the least significant bit of the pixel

transformation, the image will be restored to the original image. Arnold transformation has periodicity. So, this encryption method is unsafe if someone knows the encryption algorithm, starting from a random state of the cipher text space. After some rounds of iterations, an image will turn back to its original in a period of limited time, and the time is very short. The inverse formula of Arnold mapping is [22]:

value of cover image. The efficiency can be enhanced by using this algorithm because the algorithm allows low computational complexity [6]. For RGB, we analyze these LSB replacement techniques that replace the least three significant bits of each channels Red, Green, or Blue with secret encrypted image bits. Altering the LSBs will only cause minor changes in color, and thus is usually not noticeable to the human eye.

3. The Proposed Hiding Algorithm

The hiding process algorithm consists of two stages (fig. 4):

3.1 Encryption Stage (Fig. 5) :

- a- Read the original color image (256*256 pixels) and split the image into R, G, and B components.
- b- For each input matrix components (R,G, and B), do the following :
 - divide the image into 16 sub blocks,
 - convert each 16 modified blocks of size 64*64 bit to a 16 vectors of size 4096 values ($Vector_1, Vector_2, \dots, Vector_{32}$),
 - generate X chaotic Logistic map and (M and N) chaotic Ikelda Map,
 - apply 2-D pseudo Hadmard transform (2D-PHT) to the permuted image vectors using Equations (11, 12)[17],

$$y_1 = (2x_1 + x_2) \pmod{256} \dots (11)$$

$$y_2 = (x_1 + x_2) \pmod{256} \dots (12)$$

where x_1 and x_2 are inputs to 2D-PHT and y_1 and y_2 are outputs.

- take each vector from the 16 vectors and apply IWT which will result in two sub-bands (Approximation Coefficients (CA) and Detail Coefficients (CD)),
- converting each CA from decimal system to the binary system,
- perform XOR operation between CA values and X sequence:

$$CA_NEW_i = CA_i \text{ XOR } X_i \dots (13)$$
- apply inverse IWT on (CA_NEW and CD) sub-bands to obtain a new encrypted vector of size 4096 bit,

- convert back each 16 vectors to a 16 blocks of size 64*64 values,
- using Arnold transform for each sub block,
- two Xored operation is performed with the two Ikldia chaotic map keys, for example, if we take the first block(Block1), we can describe this operation as below:

$$\mathbf{Block1}_i = \mathbf{Block1}_i \mathbf{XOR} \mathbf{Y}_i \quad \dots (14)$$

$$\mathbf{Block1}_i \mathbf{Block1}_i \mathbf{XOR} \mathbf{Z}_i \quad \dots (15)$$

, and

- Convert blocks values to the decimal system.
- c- Combine all the 16 sub blocks back into an encrypted color image of size 256*256 bit.

3.2 Hiding Stage (Fig. 6):

- a- Read the encryption image resulted from the above stage as secret image that has to be hidden in another image then convert it to a binary system after that save each bit value ('0' or '1') in a vector . Do that to all the planes (Red, Green and Blue).
- b- Read the cover color image of size (600*600) pixels and separate it into Red, Green, and Blue planes.
- c- If the Red plane in cover images is not enough to save all the secret image bits, we can use the Green and Blue planes until we finish all the secret image bits. So, we will do the following steps to each requirement plane :
 - Divide the cover image plane into four sub blocks of 300x300 pixels.
 - For each sub block do the following:
 - ✓ use a modified Spiral S scan to read the values from each sub block and save them in vectors. Because of each sub block size is 300*300 pixel, we have to get 150 vectors of size from 1196 to 2 values.
 - ✓ For each vector, do the following:

- use Haar IWT Transform in each vector to get CA and CD coefficients,
- hide the secret image bits by altering the IWT coefficients of the sub-band (CA) in each vector. We modified the first, second and third LSB in each CA coefficient byte to save the R, G and B planes of the secret image,
- apply inverse IWT on the IWT transformed vector, including modified sub-band CA to produce a new vector which contains a secret image,
- ✓ Convert back each 150 vectors to a block of size 300*300 pixels by using an inverse modified Spiral S scan.
- d- Combine back all the four sub blocks to a stego color image.

Steps for extracting the encrypting image then decrypted it are:

- read the stego- image then, divide the cover image plane into four sub blocks of 300x300 pixels,
- for each sub block do the following:
 - ✓ use a modified Spiral S scan to read the values from each sub block and save them in vectors,
 - ✓ for each vector, do the following:
 - transform each vector to the transform domain by using 1D Haar IWT resulting CA and CD,
 - extract the secret image by using LSB method and save them in a color image (encrypted image), and
 - Apply inverse IWT on the IWT transformed vector.
 - ✓ Convert back vectors to a block of size 300*300 bit by using an inverse modified Spiral S scan.
- Combine back all the four sub blocks to a cover color image.
- Split the encrypted image extracting into R, G and B components, then store the pixel values in three matrixes .
- For each input matrix, do the following :

- divide the image to 16 sub blocks ($Block_1, Block_2, \dots, Block_{16}$ and each block of size 64×64 bit,
 - for each binary sub block, two-Xored operation is performed as explained in Equations (16) and (17),
 - use Arnold transform for each sub block,
 - convert back the 16 blocks to 16 vectors,
 - apply IWT in each vector,
 - perform XOR operation between CA values and X sequence (as described in Equation (15)),
 - apply inverse IWT to obtain a new encrypted vector,
 - Apply inverse (2D-PHT) to the permuted image sub-blocks by using Equations. (16 and 17) [17].
- $$x_1 = (y_1 - y_2) \bmod 256 \quad \dots (16)$$
- $$x_2 = (-y_1 + 2y_2) \bmod 256 \quad \dots (17)$$
- Convert back the 16 vectors to a 16 blocks of size 64×64 values, and then combine all blocks back into a decrypted color image.

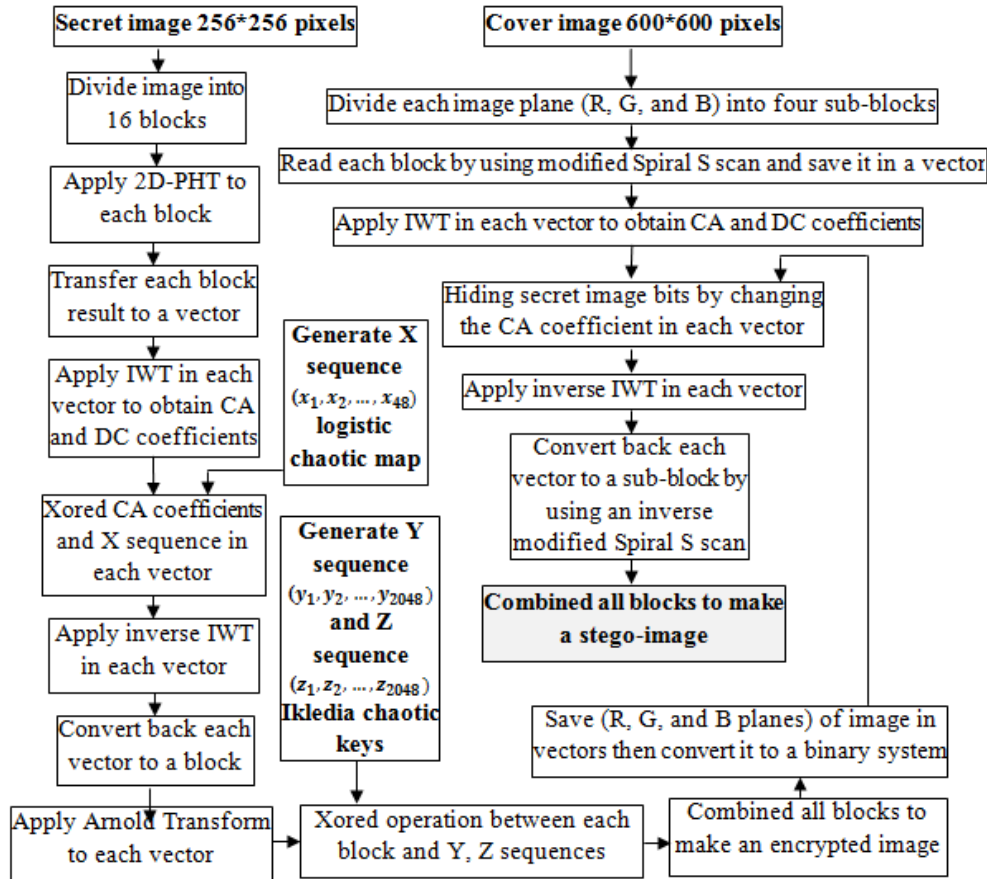


fig. (4): The scheme diagram of the encryption and hidden algorithm.

4. Performance Metrics

For data hiding and encryption, it is difficult to quantify how invisible embedded data, or the strength of the encrypted algorithm. For this reason, a number of

statistical metrics have been used to show the difference between the original hidden image and the encrypted image, such as, normal Mean Square Error (MSE), peak

signal to noise ratio (PSNR) and the entropy (as described in Table (1)). The two types of image quality measures Average Difference (AD), and Structural Content (SC)) have been tested to find out the similarity between

$$PSNR = 20 \times \log_{10} \left(\frac{255}{\sqrt{MSE}} \right) \text{ dB} \quad \dots (18) ,$$

where MSE is mean square error and is computed according to Equation (20)[13]:

$$MSE = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (|I(i,j) - I'(i,j)|)^2 \quad \dots (19),$$

where $I(i,j)$ is pixel value of the original plain image and $I'(i,j)$ is the pixel values of the encrypted image at location (i,j) .

The AD and SC values are computed as following [22]:

$$AD = \frac{1}{MN} \sum_{i=1}^M \sum_{j=1}^N (|S(i,j) - C(i,j)|) \quad \dots (20),$$

$$SC = \frac{\sum_{i=1}^M \sum_{j=1}^N (|C(i,j)|)^2}{\sum_{i=1}^M \sum_{j=1}^N (|S(i,j)|)^2} \quad \dots (21),$$

where $S(i,j)$ is pixel value of cover image and $C(i,j)$ is pixel values of stego-image at location (i,j) .

NPCR stands for the number of pixels change rate while one pixel of plain image changed. UACI stands for the average

$$NPCR = \frac{\sum_{ij} D(i,j)}{W \times H} \times 100\% \quad \dots (22),$$

$$UACI = \frac{1}{W \times H} \left[\frac{\sum_{ij} |C(i,j) - C'(i,j)|}{255} \right] \times 100\% \quad \dots (23).$$

Where W, H are the width and height of the image, $C(i,j)$ and $C'(i,j)$ are the two encrypted images before and after one pixel

the cover and stego-image of the proposed method (as described in Table(2)) [22].

The PSNR can be calculated by using the following formula [13],

intensity of differences between the plain image and ciphered image. The NPCR and UACI measure tested the different range between two images Calculate NPCR and UACI using the following formulas [23]:

of the plain image is changed respectively. $D(i,j)$ is determined by the following rules[23]:

$$D(i,j) = \begin{cases} 0 & C(i,j) = C'(i,j) \\ 1 & \text{otherwise} \end{cases} \quad \dots (24)$$

By using experimental result we found that MSE decrease causes PSNR increase and vice-versa. To measure the distortion introduced by the hiding in the cover-image, the PSNR after embedding was observed for some images. It was found that the PSNR is constantly higher than other methods as shown in Table (1) which means that the quality degradations could hardly be perceived by a human eye. In Table (2), we can find that the NPCR is over 99% and the UACI is over 48%. This means that proposed algorithm was very sensitive to tiny changes in bits of the plain image. In Table (3), we conduct an analysis between

cover-image and the stego-image based on AD and SC parameters. The time requirement for encryption and decryption algorithm is summarized in table (4). Minimizing parameters difference is one of the main objectives in order to get rid of statistical attacks. By comparing the proposed method with several other ways (as shown in Table (1, 2 and 3)) we found that the proposed method gives good quality Stego-image as well as good quality extracted secret image. This means that the proposed method of mixing values (using Spectral S scan, IWT, and chaotic map)

before you hide them may work well to add complexity to protect data from attack.

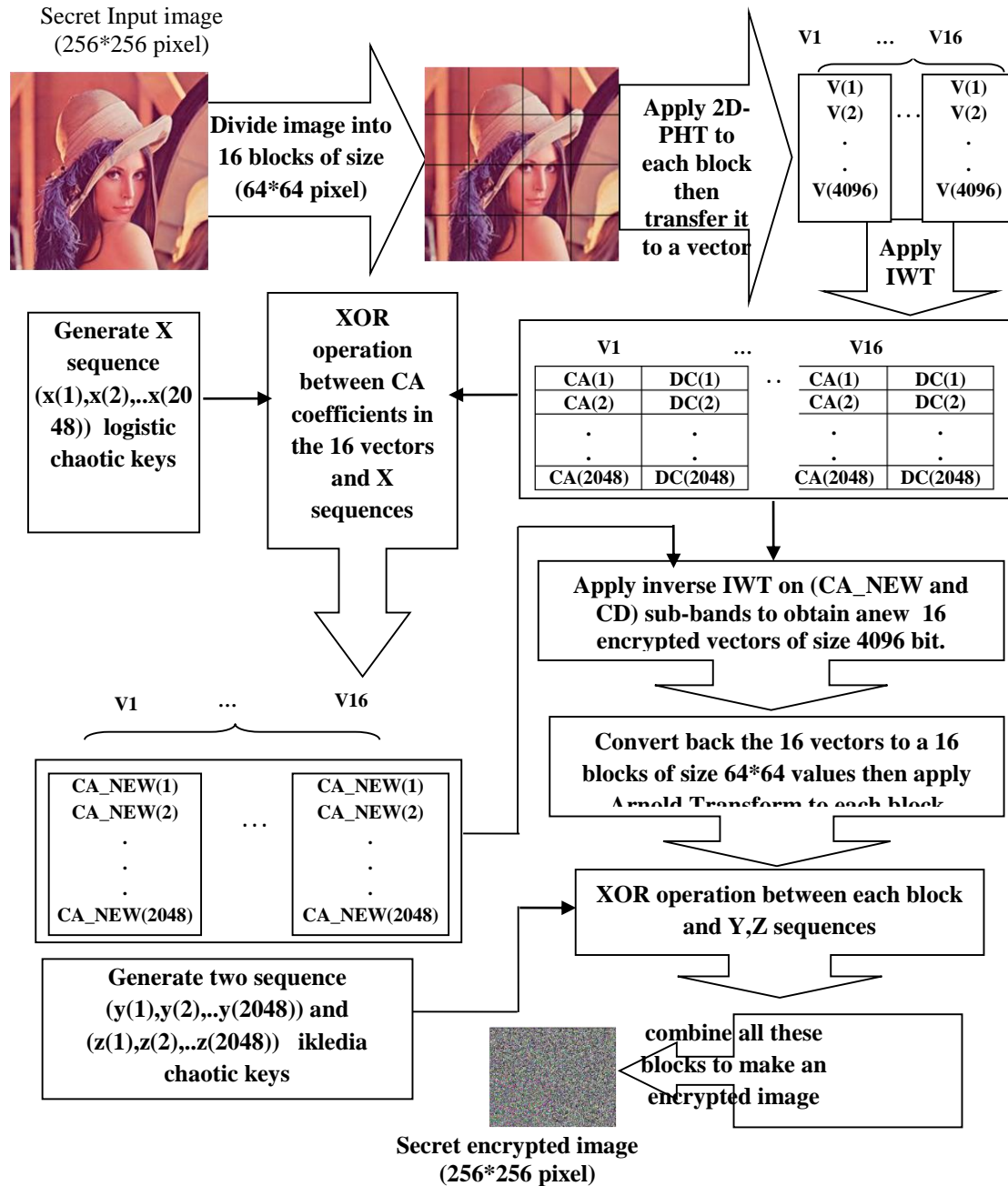


Fig. (5): Encrypted stage of the proposed algorithm

5. Conclusion

In this paper, a new color image encryption and hiding algorithm based on IWT, chaotic map keys and Arnold transform, is proposed. Here we have implemented an algorithm that satisfies both of the attributes such as high imperceptibility and high security. Future works in this direction include development

of some transform domain methods those will provide robustness along with Impeccability, security and insertion into higher order bits to achieve further higher capacity. From the survey it was found that Arnold cat map mixed with a chaotic map in the proposed algorithm performs better image scrambling because it works only on







accurate value and not with approximated value. If there is any modification in the value the original image cannot be retrieved correctly. We used also the scan methodology in order to add an unexpected way to read the data of the secret image to ensure more security and better performance.

A good encryption system should be sensitive to a small change in secret keys i.e. a small change in secret keys in decryption process may results into a completely

different output image. Our proposed encryption algorithm is sensitive to a very small change in the secret keys.

A number of parameters are also used to evaluate the proposed framework, such as the Mean Square Error (MSE), peak signal to noise ratio (PSNR), NPCR and UACI have been computed between the original and encrypted image. Also, we evaluate Average Difference (AD) and Structural Content (SC) between the cover and stego image.

Table (1): Comparison study using PSNR and MSE.

Secret Image	PSNR			MSE		
	method in [4]	method in [5]	proposed method	method in [4]	method in [5]	proposed method
	88.14002	90.0131526	92.139507	0.08184	0.07999	0.007927
	78.112010	77.821731	87.619953	0.09182	0.9733	0.008935
	83.000127	87.734291	89.196639	0.09273	0.09421	0.009850
	81.101869	78.099790	88.158287	0.10134	0.09997	0.009937
	66.726115	76.964417	79.812164	0.00302	0.0210	0.000108
	64.960012	69.930321	79.043136	0.00578	0.0228	0.000128

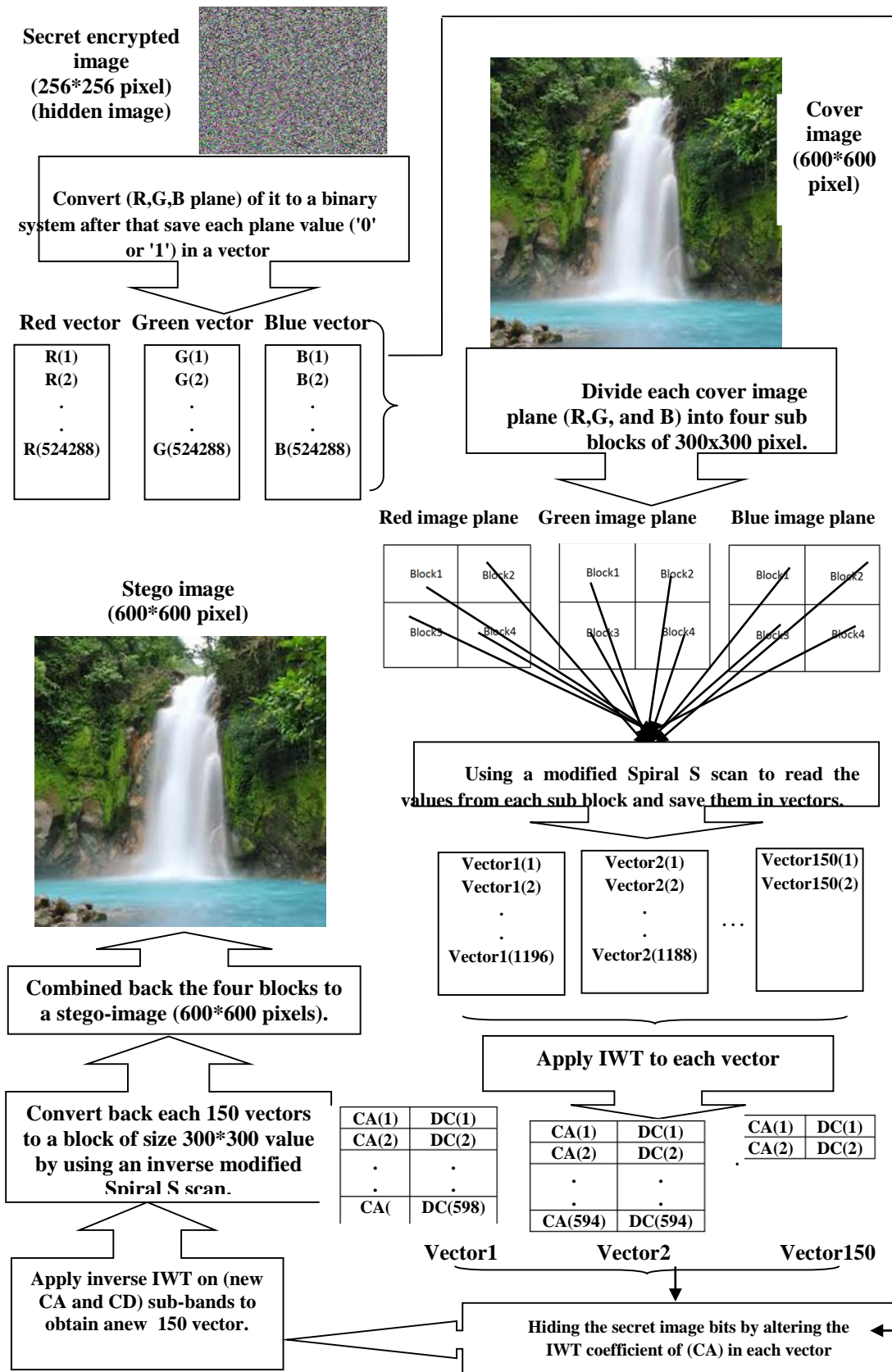


Fig. (6): The hidden stage of the proposed algorithm


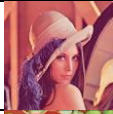


Secret Image	NPCR			UACI		
	method in [23]	method in [24]	proposed method	method in [23]	method in [24]	proposed method
	99.7%	99.61%	99.8%	33%	47%	48%
	99.6%	99.56%	99.7%	34%	49%	49%
	99.53%	99.41%	99.64%	33%	40%	39%
	99.54%	99.43%	99.59%	33.5%	44%	43%

Table (2): NPCR and UACI values for different Secret image (256*256 pixels)













Cover image (600*600 pixels)	Encrypted secret image (256*256 pixels)	AD			SC		
		method in [4]	method in [5]	proposed method	method in [4]	method in [5]	proposed method
		0.002291	0.00230	0.002075	0.9999361	0.9999331	0.999914522
		0.66012	0.6102	0.526047	1.00018	1.00108	1.00004
		0.042152	0.05222	0.034925	0.9999628	0.9999846	0.999905432
		0.02991	0.031871	0.019627	1.0007631	1.0070316	1.0001113
		1.55347	1.376710	1.250000	1.001064	1.001001	1.000164
		0.032671	0.016727	0.0151638	1.000970	1.002103	1.000110

Table (3): AD and SC values for different cover image (600*600 pixels)

Secret Image	encryption and decryption time(sec.)	Secret Image	encryption and decryption time(sec.)
	0.733102		0.633125
	0.732318		0.592318
	0.77641		0.4043

Table (4): time for encryption and decryption different Secret image (256*256 pixels)

6. References

- [1] Kekrel H., Tanuja S., & Pallavi H., "A Hybrid Approach for Information Hiding and Encryption using Multiple LSB's Algorithms", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 3, 2014.
- [2] Loay E. G., & Suad K. A., "Hiding Image in Image Using Iterated Function System (IFS)", Advances in Communications, Computers, Systems, Circuits and Devices, pp. 68-74, 2010.
- [3] Asmita, Shrikant L., "Chaotic Encryption Technique for Color Images by Coupling Two Chaotic Maps", (IJCSNS) International Journal of Computer Science and Network Security, Vol.14, No.10, October 2014.
- [4] N. S. Raghava, Ashish K., Aishwarya D. and AbhilashaChahal, "Improved LSB Method for Image Steganography Using Henon Chaotic Map", Open Journal of Information Security and Applications, Vol. 1, No. 1, 2014.
- [5] Naresh G. M., Arjun N., & Muni S. V., "Improved Qualitative Color Image Steganography Based on DWT", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5, No. 4, pp. 5136-5140, 2014.
- [6] Praneeta D., & Padma B., "Hiding Image in Image by using FMM with LSB Substitution in Image Steganography", International Journal of Advance Research in Computer Science and Management Studies, Vol. 2, Issue 11, 2014.
- [7] W. J. Chen, C. C. Chang & T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA), vol. 37, pp. 3292-3301, 2010.
- [8] V. Madhu Viswanatham & J. Manikonda, "A Novel Technique for Embedding Data in Spatial Domain", International Journal on Computer Science and Engineering, IJCSE, vol. 2, 2010.
- [9] Yang & Ching-Yu, "Color image steganography based on module substitutions," In Proceedings of IEEE Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP), vol. 2, pp. 118-121. 2007.
- [10] M.Vijay , & V.VigneshKumar, "Image Steganography Method Using Integer Wavelet Transform", International Journal of Innovative Research in Science Engineering and Technology Vol. 3, Special Issue 3, 2014.
- [11] K.Thaiyalnayaki, & A.Kala, "Dual Robust Watermarking Using Integer Wavelet Transform And Singular Value Decomposition", International Journal of Remote Sensing & Geoscience , Vol. 2, Issue 6, 2013.
- [12] Y. dinesh & A. P. ramesh," Efficient Capacity Image Steganography by Using Wavelets", International Journal of

- Engineering Research and Applications (IJERA), Vol. 2, Issue 1, pp.251-259, 2012.
- [13] Gururaj H. ,& Linganagouda K., "Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform", International Journal of Hybrid Information Technology, Vol.7, No.4, pp.185-200, 2014.
- [14] Zhang L., Liao X., & Wang X.," An Image Encryption Approach Based on Chaotic Maps", Chaos Solitons & Fractals Journal, No. 24, pp. 759-65, 2005.
- [15] Li T., Juan H., Chi Z. & Gang L.," Image Encryption Algorithm Based on Arnold Transformation and Logistic Mapping", Advances in information Sciences and Service Sciences(AISS), Vol. 4, No. 23, December 2012.
- [16] Aline S. P., & Marcelo A. S., "A Multiparameter Chaos Control Method Applied to Maps", Brazilian Journal of Physics, Vol. 38, No. 4, 2008.
- [17] S.S. Maniccam, & N.G.Bourbakis "Image and Video Encryption using SCAN Patterns", The Journal of the Pattern Recognition Society, Vol.37, pp.725-737, 2004.
- [18] Saisubha V., Priyanka U., Remya K. R., & Reenu R.," Image Encryption Using Scan Pattern", Proceedings of AECE-IRAJ International Conference, ISBN: 978-81-927147-9-0, July 2013.
- [19] Rinkee G., Jaipal B., & Amit G.,"Medical Image Encryption Using Two Dimensional Scan Approach", International Journal of Engineering Science and Innovative Technology (IJESIT), Vol. 3, Issue 2, March 2014.
- [20] Er. Ankita G., & Er. Maneesha G., " Review: Image Encryption Using Chaos Based Algorithms ", Journal of Engineering Research and Applications, Vol. 4, Issue 3, pp.904-907, March 2014.
- [21] Aidi Z., Nanrun Z., "Color Image Encryption Algorithm Combining Compressive Sensing with Arnold Transform", Journal of Computers, Vol. 8, No. 11,2013.
- [22] Tanusree P., Lalita K., & Abhishek M., "Text Hiding Scheme Using Mapping Technique for Spatial Domain ", International Journal of Advanced Computer Research, Vol. 4, No. 1, March 2014.
- [23] N.F.Elabady, H.M.Abdalkader, M. I. Moussa, & S. F. Sabbeh, "Image Encryption Based on New One-Dimensional Chaotic Map ", Engineering and Technology (ICET), International Conference, pp.1-6, 2014.
- [24] Xiangjun Wu, Yang Li , & Jürgen Kurths, "A New Color Image Encryption Scheme Using CML and a Fractional-Order Chaotic System", PLoS ONE journal, Vol.10, No.3, March 2015.

لاخفاء صورة مشفرة في صورة ملونة

إيمان قيس عبد الجليل

جامعة البصرة /كلية العلوم/ قسم علوم الحاسبات

emankais@yahoo.com

المستخلص

في هذه الورقة البحثية عملنا على اخفاء صورة سرية secret image عبر صورة اخرى تدعى بالصورة الغطاء cover image. حيث نعمل اولاً على تشفير الصورة المخبئة باستخدام التحويل المويجي الصحيح Integer Wavelet Transform ثم نقوم بخلط بيانات الصورة السرية باستخدام تحويل Arnold وعمليات XOR مع استخدام نوعين من المفاتيح المولدة عشوائياً chaotic map key لحماية الصورة المشفرة وتعزيز الامن. بهذه الطريقة المقترحة يمكننا استرجاع الصورة الاصلية ببيانات خالية من اي خطأ. اما في مرحلة اخفاء المعلومات فلقد قمنا باستخدام تقنية LSB لاخفاء القنوات الثلاث الخاصة بالصورة المشفرة الملونة في الصورة الغطاء. واستخدمنا في هذه المرحلة طريقة محورة لقراءة البيانات من كل الكتل التي قسمت اليها الصورة المراد تخبيتها بالاضافة الى تحويل IWT .

يعرض البحث اسلوب جديد لتشفير واخفاء المعلومات الصورية بالاعتماد على اسلوب مقترح لتقطيع الصورة قبل التعامل معها وبذلك نمنع الوصول غير المصرح به للبيانات. النتائج التجريبية باستخدام عدد من معلمات قياس الكفاءة مثل MSE و PSNR اظهرت صعوبة عالية لفك هذه الصور السرية. اما الوقت اللازم للتشفير وفك التشفير فهو بين 0.4043- 0.77641 ثانية.

الكلمات المفتاحية : الاخفاء، التشفير، تقنية LSB، تحويل Arnold، التحويل المويجي الصحيح IWT.