

**IMAGE STEGANOGRAPHY BASED
ON CELLULAR AUTOMATA**

Biswapati Jana¹, Debasis Giri², Shymal Kumar Mondal³, Pabitra Pal⁴

^{1,4}Department of Computer Science
Vidyasagar University
Paschim Medinipur, INDIA

²Department of Computer Science Engineering
Haldia Institute of Technology
Haldia, 721657, India

³Department of Applied Mathematics with
Oceanology and Computer Programming
Vidyasagar University
Paschim Medinipur, INDIA

Proceedings of
NCRTMSA – 2012

Abstract: In this paper, a new approach of image steganography using two-dimensional Cellular Automata (2D-CA) has been proposed for a confidential message. We convert the message in such a way that message length becomes 1024 bits after padding some bits. If message size is more than 1024 bits, we subdivide the message of length 1024 bits using padding technique. Convert original message by XORing with shared secret key of length 1024 bits. Update the central pixel value of 3x3 2D-CA (rule 341) depending upon the parity (Odd or Even) of Least Significant Bits (LSB) of the cover work and converted bits of confidential message. During decoding only consider CA 341 rule and parity of LSB of stego image. XORing of decoded message and shared secret key, we can get the message of 1024 bits and combine different message component

to get the original message. Results are compared with the Discrete Wavelet Transform (DWT) based steganography schemes in terms of Peak Signal-to-Noise Ratio (PSNR). This Image Steganography based on Cellular Automata (ISCA) method increases embedding capacity of confidential message. The security is measure by calculating the relative entropy between the probability distributions of the cover and stego image.

AMS Subject Classification: 60A05

Key Words: two-dimensional cellular automata (2D-CA), cover work, shared secret key, discrete wavelet transform (DWT), image steganography based on cellular automata (ISCA), least significant bit (LSB), peak signal-to-noise ratio (PSNR)

1. Introduction

The term steganography refers to the art of hidden communications [1]. Sender will send a secret message to the receiver in such a way that no one else will guess that the message exists. Typically, the message is embedded within another object known as a cover work by using minimum change of its properties. The resulting output, known as a stegogramme that is a near identical of the cover work, but it will also contain the hidden message. If anybody intercepts the communication, they will obtain the stegogramme, but as it is so similar to the cover, it is a difficult task for them to identify that there is something embedded in the stegogramme. The modern age steganography is usually implemented computationally, where cover works such as text files, images, audio files, and video files are tweaked in such a way that a secret message can be embedded within them [2]. Two most popular steganographic methods are based on the least significant bits (LSBs) replacement [3], [4], [5] and the modulus operation [6], [7], [8]. Both methods can encode and decode the message successfully but a good method of practice is to keep the message data as short as possible when using steganography. Therefore, a stegogramme containing a high capacity message is traditionally a higher risk than that of one with a shorter capacity message, even though they have encoded the message in the same way. We have shown in this paper how a message can be subdivided using simple padding technique and embed within the cover work by the help of two-dimensional cellular automata (2D-CA) using parity bit checker.

To identify the hidden message within stegogramme, one can analyze the image by two different approaches targeted steganalysis and blind steganalysis. In targeted steganalysis, the suspect file is analyzed by known algorithms where

in blind steganalysis both method and file are unknown.

Steganalytical schemes for targeted steganalysis are visual, structural and statistical. Structural attacks are more useful than visual attacks because the steganalyst can check the image for inconsistencies and generate a feature set that is known to be associated with stegogrammes. This attacks work best for know stegogramme. Statistical attacks are the most successful form of targeted steganalysis because they have the capability to generate a set of features related to the hidden message. The early blind steganalysis techniques was developed by Nasir Memon [9] who used Image Quality Measure (IQM) that classify image according to the likelihood that they contain message data. Much current research is being carried out for blind steganalysis because of the growth of the online vulnerability.

Our motivation is to send a message of arbitrary length using the 2D-CA with parity checker. It is observed that, in the previously published schemes, one cannot detect the end of message embedded in a cover image. But our aim is to design in such a manner that one can easily find the end of message in a cover image because of the fact that last block after padding some bits contains the length of the message.

In this paper, we propose a new approach of Image Steganography based on Cellular Automata (ISCA). First, padded message is converted to a ciphertext using shared secret key between sender and receiver and then ciphertext is concealed in the LSB of cover image with the help of 2D-CA 341-update rule and parity bit checker. During decoding the system simple use CA 341 rule and parity checker to retrieve the cipher text. To get the original message, one has to combine the message component then XOR with shared secret key.

The rest of this paper is organized as follows: related work is covered in Section 2. Cellular Automata have been described in Section 3. In Section 4, we describe our proposed scheme. Section 5 provides experimental result and comparison between our proposed schemes with other existing schemes. Finally, the conclusion of this paper is presented in Section 6.

2. Related Work

Wolfram et al [10] studied one-dimensional cellular automata (1D-CA) with the help of polynomial algebra. Pries et al [11] also shown 1D-CA exhibiting group properties based on a similar kind of polynomial algebra. Packard et al [12] studies on 2D-CA depending on five nearest neighborhoods of CA. The theory and application of additive 1D-CA rules has been proposed by Ganguli et al in

[13] and Thomas et al explains the evolution of CA for image processing in [14]. Pal Choudhury et al [15] shown some extra theory of 2-D CA linear rules. P. Jebaraj Selvapeter and Wim Hordijk [16] studied cellular automata for image noise filtering using a majority CA update rule. Based on above technique, Jana et al [17] proposed a technique to reduce noise from image using 2D-CA with the help of nearest neighbor pixel information.

Secret sharing and hiding using modulus concept has been proposed by Wu et al [18]. Lin and Tsai [19] proposed a method of secret image sharing with steganography and authentication. Yang et al [20] proposed an improved version of Lin and Tsai's scheme. Chang et al [21] proposed sharing secret in the stego images with authentication. A secret sharing scheme has been proposed based on CA by A.M.del Rey et al [22]. To share secret color images, 2D-CA is used in [23]. The DWT based approach scheme [27] using a mapping table, the secret message is embedded in the high frequency coefficients resulted from DWT. Image steganography based on Discrete Wavelet Transform (DWT) and Huffman Encoding [28] has been proposed. This approach improves both image quality and security.

3. Overview of Cellular Automata

In the proposed scheme, Cellular Automata (CA) has been employed for embedding message within the cover image. Hence for the sake of completeness a brief overview of CA is provided in this section. Although the concept was proposed almost five decades back by John Von Neumann [24], but in the last two decades, researchers of various fields became interested to use the concept. CA has many applications in the field of steganography.

CA consists of array of cells which are connected locally. Each cell repeatedly updates its own state, where the next state depends on the cell's current state and those of its local neighbors. In the simplest case, the CA lattice is a one dimensional (1D) array of cells. Detail of one dimensional (1D) CA can be found in [25].

The extension of one dimensional (1D) CA to 2D-CA is significant for modeling many physical systems. Depending on the neighbors of 2D-CA it is divided into two types, Von Neumann neighborhood and Moore neighborhood.

The Von Neumann neighborhood is the set of all cells that are orthogonal adjacent to the region of interest. The Von Neumann neighborhood of range r is defined by in (1),

$$N_{(x_0, y_0)}^V = \{(x, y) : |x - x_0| + |y - y_0| \leq r\} \quad (1)$$

The Von Neumann neighborhoods for ranges $r = 1$ and 2 are illustrated in Figure 1. The number of cell in the Von Neumann neighborhood of range r is the centered square number, that is, $2r(r + 1) + 1$. If the range value $r \geq 2$ then it is consider as Extended Von Neumann neighborhood.

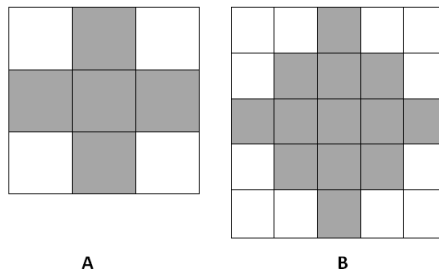


Figure 1: A) Von Neumann neighborhood; B) Extended Von Neumann neighborhood

The Moore neighborhood is the set of all cells that are orthogonal or diagonally adjacent to the region of interest. The Moore neighborhood of range r is defined by in (2),

$$N^M_{(x_0,y_0)} = \{(x, y) : |x - x_0| \leq r, |y - y_0| \leq r\} \tag{2}$$

Moore neighborhoods for ranges $r = 1$ and 2 are illustrated in Figure 2. The number of cell in the Moore Neighborhood of range r is the odd squares, that is, $(2r + 1)^2$. If the range value $r \geq 2$ then it is consider as Extended Moore neighborhood.

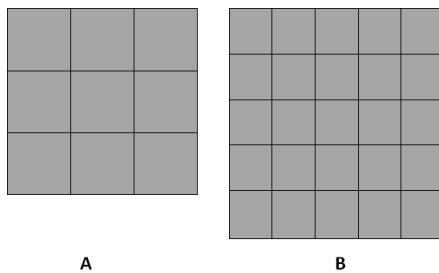


Figure 2: A) Moore neighborhood; B) Extended Moore neighborhood

The next state of a particular cell (middle cell) of 2D-CA is updated by the current state of itself and eight cells in its nearest neighborhood (Moore neighborhood) as shown in the Figure 3.

64	128	256
32	1	2
16	8	4

Figure 3: 2D rule box

The number within each box of Figure 3 represents the rule number characterizing the dependency of the current cell on that particular neighbor only. Rule 1 characterizes dependency of the central cell on itself alone where as such dependency only on its top neighbor is characterized by Rule 128, and dependency on all neighbors is characterized by Rule 511(=1+2+4+8+16+32+64+128+256) and so on. In case, the cell has dependency on two or more neighboring cells, the rule number will be the arithmetic sum of the numbers of the relevant cells. In our proposed method CA 341 rule has been used, which is include in-group 5 considering the dependency of current cell on its neighboring cells. Thus group 5 includes 1, 4, 16, 64, and 256 and the corresponding rule will be $1+4+16+64+256=341$ has been generated. When move the CA through the cover work then update the center pixel only by checking the parity of LSB of chosen CA rule which is non overlapping to each other during scanning or embedding.

4. Proposed Scheme

In this section, we propose a new approach of Image Steganography based on Cellular Automata (ISCA). Here, an image can be considered as the lattice configuration of a 2D-CA, where each cell corresponds to an image pixel, and the possible states are the different gray values or colors. Color image with Moore neighborhood (the eight neighboring cells surrounding a cell) is being considered. The proposed algorithms for encoding and decoding are described below.

Algorithm for Encoding:

Step 1: After padding technique (Ref. Giri et al [26]), the original message M is partitioned into some number blocks (say, M_1, M_2, \dots, M_n , where $M =$

$M_1 || M_2 || \dots || M_n$) each of length 1024 bits.

Step 2: If the number of portioned blocks is n after padding some bits and $n \times 1024$ is more than $512 \times 512 / 2 = 131072 = 128 \times 1024$, we can consider N number of color images where $N = \lceil n/128 \rceil$. The function $[x]$ denotes the least positive integer greater than or equal to x . Consider the color image C_k , where $k = 1$ to N .

Step 3: Convert M_i into cipher text H_i , where $H_i = M_i \text{ XOR } h(K || i)$ for $i = 1$ to n . h represents cryptographic one-way hash function which provides 1024 message digest [29]. K is the shared secret key between sender and receiver.

Step 4: For $k = 1$ to N

Consider 3×3 2D-CA of $r = 2$ and Moore neighborhood. So total neighbor $n = 8$ and total cell of CA is 9. Central cell value is R .

Step 5: For $k = 1$ to N

Step 6: For $row = 1$ to 512

Step 7: For $col = 1$ to 512

$B[row][col] = \text{LSB}$ of Cover image $C_k[row][col]$;

End for (in Step 7)

End for (in Step 6)

Step 8: For $row = 1$ to 512

Step 9: For $col = 1$ to 512

Step 10: For $p = 1$ to 3

Step 11: For $q = 1$ to 3

Step 12: Using 2D-CA 341 rule check the parity of binary number of 3×3 $B[p][q]$.

End for (in Step 11)

End for (in Step 10)

Step 13: Update R using the following Table- 1 and replace in the central cell of 2D-CA.

Step 14: Update cover image pixel value using updated R

Step 15: Move 2D-CA by $col = col + 1$

End for (in Step 9)

Step 16: Move 2D-CA by $row = row + 2$

End for (in Step 8)

Step 17: End for (in Step 5)

Step 18: End

Table 1: Rules for update center pixel of 2D-CA

Cipher bit \Rightarrow Parity \Downarrow	$H = 0$	$H = 1$
Odd parity	Change R	No Change R
Even Parity	No Change R	Change R

Algorithm for Decoding:**Step 1:** For $k = 1$ to N Consider a stego images S_k and the shared secret key K .**Step 2:** Consider 3X3 2D-CA of $r = 2$ and Moore neighborhood pixel where center pixel is considered as R . So total neighbor $n = 8$ and total cell of CA is 9.**Step 3:** For $row = 1$ to 512**Step 4:** For $col = 1$ to 512 $B_S[row][col] = LSB$ of stego image $S_k[row][col]$;

End for (in Step 4)

End for (in Step 3)

Step 5: For $row = 1$ to 512**Step 6:** For $col = 1$ to 512**Step 7:** For $p = 1$ to 3**Step 8:** For $q = 1$ to 3**Step 9:** Using 2D-CA 341 rule check the parity of binary number of 3x3 $B_S[p][q]$

End for (in Step 8)

End for (in Step 7)

Step 10: If parity is even then store 0 else 1 in H_i for $i = 1$ to n **Step 11:** Move 2D-CA by $col = col + 1$ within cover image

End for (in Step 6)

Step 12: Move 2D-CA by $row = row + 2$

End for (in Step 5)

Step 13: We can get the message $M_i = H_i XOR h(K||i)$ for $i = 1$ to n .**Step 14:** To recover the original plaintext message M , the receiver discards the lower ordered padding bits from the last block, that is, from M_n , the number

of padding bits is the number stored in the 11 least significant bits of M_n .

Step 15: End for (in Step 1)

Step 16: End

5. Experimental Result and Comparison

Here color image 512x512 pixel has been used as cover image, which is shown in Figures 4(a) to 4(e). Capacities in terms of number of bits are shown in Figure 4(f). The proposed algorithm is implemented in MATLAB Version 7.6.0.324 (R2008a).

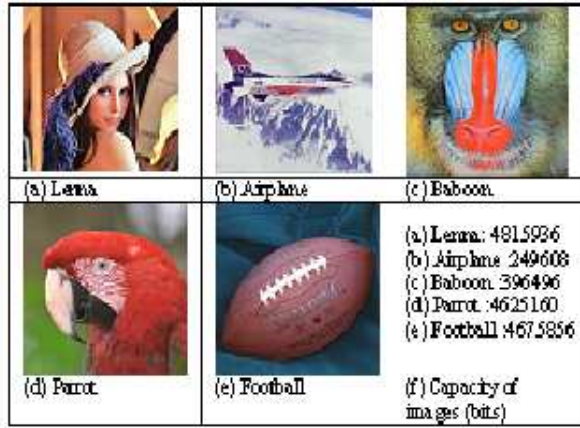


Figure 4: Standard cover image and their capacity

PSNR is used as a fitness measure shown in the equations (3) and (4).

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} ||I(i, j) - K(i, j)||, \tag{3}$$

where $I(i, j)$ represents the i -th row and j -th column of clean image and $K(i, j)$ represents the i -th row and j -th column of stego image.

$$PSNR = 10 \log_{10} \left(\frac{MAX_I^2}{MSE} \right) = 20 \log_{10} \frac{MAX_I}{\sqrt{MSE}} \tag{4}$$

Here, MAX_I is the maximum pixel value of the image.

Analysis in terms of PSNR of original and stego-image compared with DWT based [27] and DWT with Huffman based [28] has been shown in Table-2. Our proposed ISCA method gives promising result. To compare the proposed ISCA approach with DWT method and DWT with Huffman shown in Figure 5. It is clear that from the same capacity the PSNR of our proposed algorithm is better than other one. From Table-2 it is notice that for all images PSNR is near to 62.

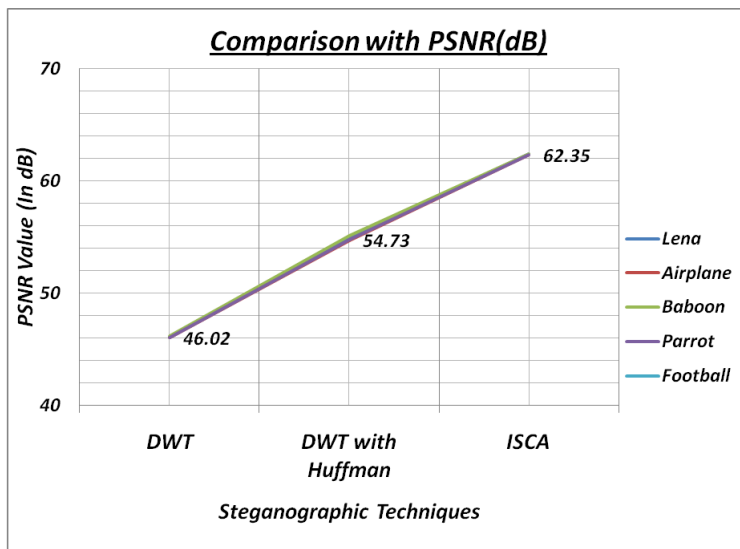


Figure 5: Comparison graph with existing techniques

Some output results are shown below in Figures 6(A)and 6(B):

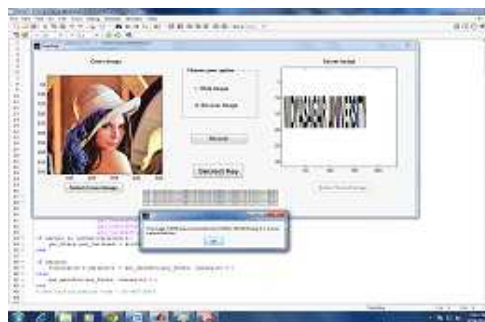
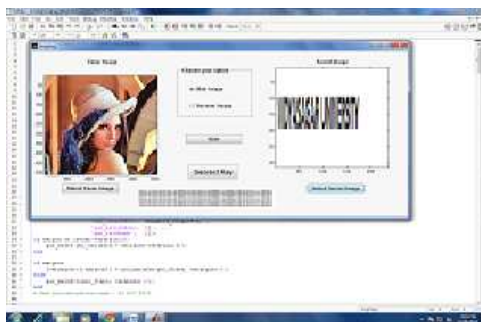
To test the security in our proposed method relative entropy (the differences) between the probability distributions of the cover and the stego image has been calculated by equation (5). let p_m and q_n be probability measures for clear image M and stego image N , respectively. The relative entropy distance $D(N||M)$ [30] (also known as Kullback-Leibler distance) is defined as

$$D(N||M) = \sum_n q_n(x) \log \frac{q_n(x)}{p_m(x)}. \quad (5)$$

Relative entropy between two probability distribution functions is zero that means the system is perfectly secure. $D(N||M)$ is a nonnegative continuous function and equals to zero iff p_m and q_n coincide. Thus $D(N||M)$ can be naturally viewed as a distance between the measures p_m and q_n . The corresponding entropy result are shown in the following Table-3.

	DWT Based [27]	DWT Based [27]	DWT with Huffman Based [28]	DWT with Huffman Based [28]	Our proposed Method	Our proposed Method
Cover Image (512 x 512)	Capacity (Bits)	PSNR (dB)	Capacity (Bits)	PSNR (dB)	Capacity (Bits)	PSNR (dB)
Lena	4815936	46.09	4815936	54.93	4815936	62.43
Airplane	249608	46.00	249608	54.67	249608	62.34
Baboon	396496	46.19	396496	55.11	396496	62.39
Parrot	4625160	46.02	4625160	54.73	4625160	62.35
Football	4675856	46.07	4675856	54.81	4675856	62.38

Table 2: Comparison of the result for the proposed method and some existing method



A) During encoding process

B) During decoding process

Figure 6: During encoding and decoding process.

6. Conclusion

In our proposed ISCA scheme based on Moore neighborhood CA, enhancement of the image steganographic system for sending confidential messages using LSB approach to provide a means of secure communication by using shared secret key has been introduced. In the following, we describe our contribution:

- If message length is arbitrary, our approach can be applicable.
- One can easily find the end of the embedded message into the cover image.
- Since PSNR is much more than some previously published schemes, which ensure that the image quality is better after the embedding the message in our scheme compared to these schemes.

Cover Image (512 x 512)	Our proposed (ISCA) Method	
	Clear Image Entropy	Stego-Image Entropy
Lena	6.9439	6.9439
Airplane	6.7915	6.7915
Baboon	6.7915	6.7915
Parrot	6.9439	6.9439
Football	6.7915	6.7915

Table 3: Relative entropy between the probability distribution of the cover and the stego image

- Since relative entropy of the probability distribution of the clean image and stego image is zero which implies that our system assumed to be perfectly secure.

One can develop a system using public key cryptosystem which can be applied to the smart card for authentication and other security challenges. For online transaction using this system, one can revise further for transmit the relevant information for checking and permitting the access of valid user.

References

- [1] N. Johnson and S. Katzenbeisser, A Survey of steganographic techniques, *Information Hiding*, Artech House (2000), 43-78.
- [2] D. Wu, W. Tsai, A steganographic method for images by pixel-value differencing, *Pattern Recognition Letters* (2003), 1613-1626.
- [3] C. Chan, L. Cheng, Hiding data in images by simple LSB substitution, *Pattern Recognition*, **37**, No. 3 (2004), 474-496.
- [4] C. Chang, J. Hsiao, C. Chan, Finding optimal least-significant-bits substitution in image hiding by dynamic programming strategy, *Pattern Recognition*, **36**, No. 7 (2003), 1583-1595.
- [5] R. Wang, C. Lin, J. Lin, Image hiding by optimal LSB substitution and genetic algorithm, *Pattern Recognition*, **34**, No. 3 (2001), 671-683

- [6] C. Chang, C. Chan, Y. Fan, Image hiding scheme with modulus function and dynamic programming, *Pattern Recognition*, **39 (6)** (2006), 1155-1167.
- [7] C. Thien, J. Lin, A simple and high-hiding capacity method for hiding digit by-digit data in images based on modulus function, *Pattern Recognition*, **36**, No. 12 (2003), 2875-2881.
- [8] S.J. Wang, Steganography of capacity required using modulo operator for embedding secret image, *Applied Mathematics and Computation*, **164**, No. 1 (2005), 99-116.
- [9] Z. Eslami, S.H. Razzaghi, J. Zarepour Ahmadabad, Secret image sharing based on cellular automata and steganography, *Pattern Recognition*, **43** (2010), 397-404.
- [10] Stephen Wolfram, statistical mechanics of Cellular Automata, *Rev Mod Phys*, **55** (1983), 601-644.
- [11] W. Pries, A Thanailakis and H.C. Card, Group properties of cellular automata and VLSI Application, *IEEE Trans on computers*, **C-35** (1986), 1013-1024.
- [12] N.H. Packard and S. Wolfram, Two dimensional cellular automata, *Journal of Statistical Physics*, **38**, No-s: 5/6 (1985), 901-946.
- [13] N. Ganguly, P. Maji, S. Dhar, B. K. Sikdar, P. P. Chaudhuri, Evolving Cellular Automata as Pattern Classifier, *ACRI 2002, LNCS 2493, Springer-Verlag Berlin Heidelberg* (2002) 56-68.
- [14] Christopher D Thomas, Riccardo Poli, Evolution of Cellular Automata for Image Processing, *Thesis, School of Computer Science, University of Birmingham (UK)* (2000).
- [15] P. P. Chaudhuri, D. R. Chaudhuri, S. Nandi, S. Chatterjee, Additive Cellular Automata, *Theory and Applications*, **1** (1997).
- [16] P. Jebaraj Selvapeter and Wim Hordijk, cellular automata for image noise filtering, *in Proc. NaBIC* (2009), 193-197.
- [17] Biswapati Jana, Pabitra Pal, Jaydeb Bhaumik, New Image Noise Reduction Schemes Based on Cellular Automata, *International Journal of Soft Computing and Engineering*, **2**, No. 2 (2012).

- [18] Y. Wu, C. Thien, J. Lin, Sharing and hiding sector image with size constraint, *Pattern Recognition*, **37** (2004) 1377-1385
- [19] C. Lin, W. Tsai, Secret image sharing with steganography and authentication, *Journal of Systems and Software*, **73**, (2004), 405-414.
- [20] C. Yang, T. Chen, K. Yu, C. Wang, Improvements of image sharing with steganography and authentication, *Journal of Systems and Software*, **80** (2007), 1070-1076.
- [21] C. Chang, Y. Hsieh, C. Lin, Sharing secrets in stego images with authentication, *Pattern Recognition*, **41**, (2008), 3130-3137.
- [22] A.M. del Rey, J.P. Mateus, G.R. Sanchez, A secret sharing scheme based on cellular automata, *Applied Mathematics and Computation*, **170** (2005), 1356-1364.
- [23] G. Alvarez Marañón, L.H. Encinas, A.M. del Rey, Sharing secret color images using cellular automata with memory, *CoRR 0312034* (2003).
- [24] J. Von Neumann, Theory of Self-Reproducing Automata, *Essays on Cellular Automata*, University of Illinois Press, Urbana, Illinois (1970).
- [25] A. S. Mariano, G. M. B. de Oliveira, Evolving one-dimensional radius-2 cellular automata rules for the synchronization task, *Theory and Applications of Cellular Automata* (2008), 514-526.
- [26] Debasis Giri, Prithayan Barua, P. D. Srivastava and Biswapati Jana, Cryptosystem for Encryption and Decryption of Long Confidential Messages, *International Conference on Information Security and Assurance (ISA-2010)* (2010) 23-25.
- [27] P.Y. Chen and W.E. Wu, A DWT Based Approach for Image Steganography, *International Journal of Applied Science and Engineering*, **4**, No. 3 (2006), 275 -290.
- [28] Amitava Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarka, A Novel Technique for Image Steganography Based on DWT and Huffman Encoding, *International Journal of Computer Science and Security*, **4**, No. 6 (2010).
- [29] Secure Hash Algorithm (SHA-3), *National Institute of Standards and Technology (NIST)* (2012).

- [30] J. Wang, Y. Du, C.-I Chang and P. Thouin, Relative Entropy Based Methods for Image Thresholding, *Proc. of IEEE International Conference on Image Processing (vol-II)* (2002), II-265-II268.

Received: January 10, 2013; **Revised:** February 2, 2013; **Revised:** February 18, 2013;
Revised: February 22, 2013; **Accepted:** February 28, 2013.

