Secure Information Transmission using Steganography and Morphological Associative Memory

Sara Nazari
Department of Electrical, Computer and IT Engineering, Islamic Azad University, Qazvin Branch, Qazvin, Iran

Amir-Masoud Eftekhari
Department of Electrical, Computer and IT Engineering, Islamic Azad University, Qazvin Branch, Qazvin, Iran

Mohammad Shahram Moin
Department of Electrical, Computer and IT Engineering, Islamic Azad University, Qazvin Branch, Qazvin, Iran

ABSTRACT

This paper presents a new steganography algorithm based on Morphology associative memory. Often, steganalysis methods are created to detect steganography algorithms using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). In this paper, cover images are mapped to morphological representation by using morphology transform containing morphological coefficients, and each bit of secret message is inserted in the least significant bit of morphological coefficients. To evaluate stego quality, we measure the quality of the cover image after embedding by comparing with other image transformed steganography algorithms such as discrete cosine and Wavelet transforms. The quality of stego has considerably improved in comparison with the state-of-art methods. In the other experimentation, we test the robustness of our proposed method by using Wavelet and Block-based steganalysis methods. The results show a high level of robustness of our algorithm respect to other steganography algorithms.

Keywords

Security, Steganography, Morphological Associative Memory, Steganalysis, Image Complexity.

1. INTRODUCTION

Today, secure transmission of information is an essential factor in communication. There are two major branches of information hiding: steganography and watermarking. Steganography is the art of hiding information by embedding secret messages within multimedia tools such as image, video, and text as a cover. The set of cover, secret message, and password is defined as a stego. In spite of other information hiding, the existence of secret message is denied in steganography [1] [2].

The steganography methods can be categorized into two groups of spatial and transformation domains. In spatial domain, the secret message is embedded into cover by using direct replacing of least significant bits of cover with the bits of secret message. For example, the methods presented in [3][4] are stated in this group. The main advantage of spatial steganography to transformation domain steganography is high capacity. Another group is related to methods that a secret message is embedded in transformation domain. In this group, the cover is mapped to new domain, and then secret message is inserted in the new domain. The approach proposed in this domain is more robust against hacker attacks than the steganography methods in spatial domain. The steganography methods such as Discrete Cosine Transform (DCT) [5], Discrete FourierTransform[6], Discrete Wavelet Transform(DWT) [7-9], and Discrete Contourlet Transform [10] are examples in this group. Embedding in jpeg images is very popular, so techniques such as jsteg[11], F5[12], outguess[13] are based on DCT transformation.

Morphology associative Memory (MAM)[14-16] is an one layer neural network which maps incomplete input pattern to complete output pattern. It is organized based on human ability to remember whole information about an incident only by seeing a few section of it. The most advantage of MAM is high robustness against attacks such as dilation and erosion.

The new proposed algorithm is the transformed domain method based on Morphological associative memory. In our suggested algorithm, the cover image is mapped to morphological representation by using morphology transform, and then each bit of secret message is stored in the least significant bit of morphological coefficients. The most advantage of our method over other transformed methods such as DCT, Wavelet, and Contourlet steganography methods is that the current steganalysis methods are created to detect secret message in LSB, DCT, wavelet steganography methods, so our method decreases the probability of stego detection by steganalysis methods. As represented in paper [14], morphological associative memory is more robust against noises occurred in transmission such as erosive, dilation. Therefore, our method can retain the stego quality in transmission of information in comparison with other state-of-art transformed steganography methods: DCT, and wavelet. The rest of the paper is organized as follows: In the next section, a brief introduction to Morphological associative memory is presented. The proposed method is described in section 3. Section 4 shows experimental results. Finally, the conclusions of this paper are given in section 5.

2. MORPHOLOGICAL ASSOCIATIVE MEMORY

Associative memory is a class of neural network to retrieve complete information Y from incomplete input pattern X. The schema of associative memory is represented in Figure1.

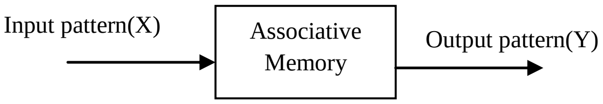

Fig 1: Structure of Associative Memory [14].

One of the famous groups in associative memory is Morphological associative memory which employs the operations of maximum and minimum instead of multiplication and additions [14]. Hence, the speed of algebra computations is increased in comparison with other neural network. The structure of morphological operation is defined by (R, $\vee$, $\wedge$, +), where R is a real number and $\vee$, $\wedge$ are maximum and minimum operations, respectively. The MAM is categorized into two groups: (1) auto-associative morphological memories (AMM), (ii) hetero-associative morphological memories (HMMs). The MAM is known as *HMM* if $\exists\mu \in \{1, 2, . . ., k\}$such that$x\mu \neq y\mu$, otherwise it is called *AMM*. In our proposed method, we employs HMM for transmission. The operations of maximum product and minimum product are defined in Equation 1 and 2 [15] [16].

1- The maximum product, $C = A_{n\times p}\nabla B_{p\times n}$,is defined for matrix A and B as:

$$c_{ij} = \bigvee_{k=1}^{p} a_{ik} + b_{kj} \qquad (1)$$

where $\vee$ is the maximum operator, and a, b are the elements of matrix A, B.

2- Similarity, the minimum product ,$C = A_{n\times p}\Delta B_{p\times n}$, is determined for matrix A and B as :

$$c_{ij} = \bigwedge_{k=1}^{p} a_{ik} + b_{kj} \, (2)$$

where $\wedge$ is the minimum operator, and a, b are the elements of matrix A, B.

The aim of this section is to provide an overview of Morphology image learning and morphology image recovery.

Morphology image learning: The operation of mapping one image to morphological representation is defined as Morphology image learning. In Morphology image learning, the image m*n is divided to sub-block m/d*n/d, and then the transform matrix with size of d*d is applied on each sub-block. There are different methods to determine transform matrix; we uses the transform matrix in paper [17], shown in equation 3. Each row of sub-block is called as image vector, and each row of transform matrix is known as transform vector.

$$Vt = \{ \begin{smallmatrix} 0 & m\neq n \\ >e & m=n \end{smallmatrix} \qquad (3)$$

After applying transform matrix to all sub-blocks with size of d*d, the morphological image representation is obtained. Forthis aim to be achieved, it is necessary to use Equation 4 which is organized based on HMM_{min}.

$$MT_{min} = o\{HMM_{min}^{xy} | x = 1,2, \ldots \ldots, \frac{m}{d},$$
$$y = 1,2, \ldots . \frac{n}{d}\} \qquad (4)$$
$$where: \; HMM_{min}^{xy} = \wedge_{\mu=1}^{d} [(vi^{w\mu})^{T} \nabla (-vt^{\mu})]$$
$$= [w_{ij}]_{d*d}^{xy} | \;\; w = 1,2, \ldots, N$$
$$where: \;\; [w_{ij}]_{d*d}^{xy} = \wedge_{\mu=1}^{d} \left[vi_{i}^{w\mu} - vt_{j}^{\mu}\right] | \;\; i,j = 1,2, \ldots, d$$

In this formula, vi , vt are image and transform vectors, respectively and μ specifies row matrix changed between 1 to d, and xy presents the location of each HMM_{min}corresponding with one sub-block.

Morphological Image Recovery: The process of mapping morphological image to original image is known as morphology image recovery. To do morphological image recovery, the transform matrix is applied to all morphological image sub-blocks with dimension of d*d by using Equation 5.

$$IMT_{min} = o\{SB^{xy} | x = 1,2, \ldots, \lambda, y = 1,2, \ldots, ŋ\} \qquad (5)$$
$$SB^{xy} = vi^{(xy)_{\mu}} | \; \mu = 1,2, \ldots, d,$$
$$vi^{(xy)_{\mu}} = HMM_{min}^{xy} \nabla vt^{\mu} = [\, vi_{i}^{(xy)_{\mu}}]_{d} \, ,$$
$$vi_{i}^{(xy)_{\mu}} = \vee_{j=1}^{d} \left(w_{ij}^{xy} + vt_{j}^{\mu}\right),$$

where$SB^{xy}$is a sub-block of original image and *xy* indicates the number of image sub-block. $vi^{(xy)_{\mu}}$is the μth row of the *xy*th image sub-block [17][18].The schema of image learning and image recovery is shown in Figure2. Each HMM corresponds to SB sub-block.

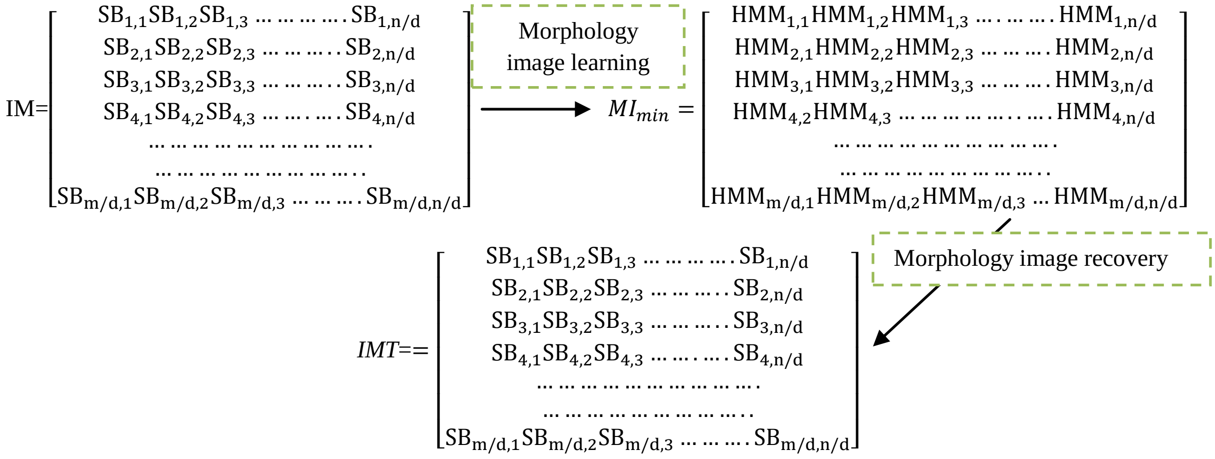
IM=
$SB_{1,1}SB_{1,2}SB_{1,3} \ldots \ldots \ldots \ldots SB_{1,n/d}$
$SB_{2,1}SB_{2,2}SB_{2,3} \ldots \ldots \ldots SB_{2,n/d}$
$SB_{3,1}SB_{3,2}SB_{3,3} \ldots \ldots \ldots SB_{3,n/d}$
$SB_{4,1}SB_{4,2}SB_{4,3} \ldots \ldots \ldots SB_{4,n/d}$
$SB_{m/d,1}SB_{m/d,2}SB_{m/d,3} \ldots \ldots \ldots SB_{m/d,n/d}$
Morphology image learning
$MI_{min} =$
$HMM_{1,1}HMM_{1,2}HMM_{1,3} \ldots \ldots \ldots HMM_{1,n/d}$
$HMM_{2,1}HMM_{2,2}HMM_{2,3} \ldots \ldots \ldots HMM_{2,n/d}$
$HMM_{3,1}HMM_{3,2}HMM_{3,3} \ldots \ldots \ldots HMM_{3,n/d}$
$HMM_{4,2}HMM_{4,3} \ldots \ldots \ldots \ldots HMM_{4,n/d}$
$HMM_{m/d,1}HMM_{m/d,2}HMM_{m/d,3} \ldots HMM_{m/d,n/d}$
Morphology image recovery
IMT==
$SB_{1,1}SB_{1,2}SB_{1,3} \ldots \ldots \ldots \ldots SB_{1,n/d}$
$SB_{2,1}SB_{2,2}SB_{2,3} \ldots \ldots \ldots SB_{2,n/d}$
$SB_{3,1}SB_{3,2}SB_{3,3} \ldots \ldots \ldots SB_{3,n/d}$
$SB_{4,1}SB_{4,2}SB_{4,3} \ldots \ldots \ldots SB_{4,n/d}$
$SB_{m/d,1}SB_{m/d,2}SB_{m/d,3} \ldots \ldots \ldots SB_{m/d,n/d}$

Fig 2: The schema of image Morphology representation in image learning, and reverse morphology transform in image recovery.

3. PROPOSED ALGORITHM

The proposed technique is based on morphology and inverse morphology transforms in embedding and extraction processes. The aim of our proposed method is storing secret message in morphological coefficients. Figure 3, shows the schema of our proposed algorithm which consists of four steps to encode the stego in the embedding phase and four steps in the recovery phase until the secret message and lossy cover are extracted. In the embedding phase, the secret message is inserted in quantized morphological coefficients. In the extraction phase, the secret message is extracted from the cover. As entropy encoding and decoding, we used Huffman encoding and decoding in the embedding and extraction procedures, respectively [18][19].

Embeddingdata:In the embedding process, the secret message is stored in quantized morphological coefficients of sub-blocks $d \times d$, where d is set to 8. In our method, we used the morphological learning phase (Equation 4) described in Section 2 to map the cover image in the morphological representation. To quantize the morphological coefficients, standard test images in [20][21] are first divided in sub-blocks $d \times d$, and mapped into the morphology representation. Then, using the Linde-Buzo-Gray (LBG) algorithm [22], a fix quantization table is obtained and shared between the sender and receiver. Levels of the embedding phase are represented in Figure 4.

The block diagram of the embedding phase is depicted in Figure 5. Embedding the secret message before the Morphology transform unit leads to a noisy image during the extraction phase when the data return to a spatial domain at the destination. Consequently, the extraction of the secret message is infeasible, since the encoding is used to compress the data. To solve this problem, the proposed algorithm is comprised of lossy and lossless stages, as seen in Figure 5. The lossy stage utilizes a morphology transform and a quantization schema to compress the image; then, the lossless stage uses Huffman encoding to compress the image. Hence, in order that the cover and secret message can be extracted by receiver correctly, the secret message must be embedded before the entropy encoding step.

Input: Cover image, Secret message

Output: Encoded Stego

Step 1. Divide the cover image into non-overlapping sub-blocks of 8×8 pixels.

Step 2. Apply the morphology transform to sub-blocks based on Equation 4 (the morphological coefficients of sub-blocks are obtained during the morphology learning phase described in Section 2).

Step 3. Quantize the Morphological coefficients based on the fixed quantization table (produced by using the transformed images corresponding to the images in [20][21]).

Step 4. Insert each bit of secret message into the least significant bit of quantized Morphological coefficient whose value is not equal to 1,-1, 0.

Step 5. Repeat Steps 4 until the entire secret message is embedded (using the recovery phase presented in subsection 2, leading to stego).

Step 6. Encode the quantized Morphology cover included in the secret message using Huffman encoding and then transmit it.

Fig 4: Algorithm of embedding and transmitting a secret message.

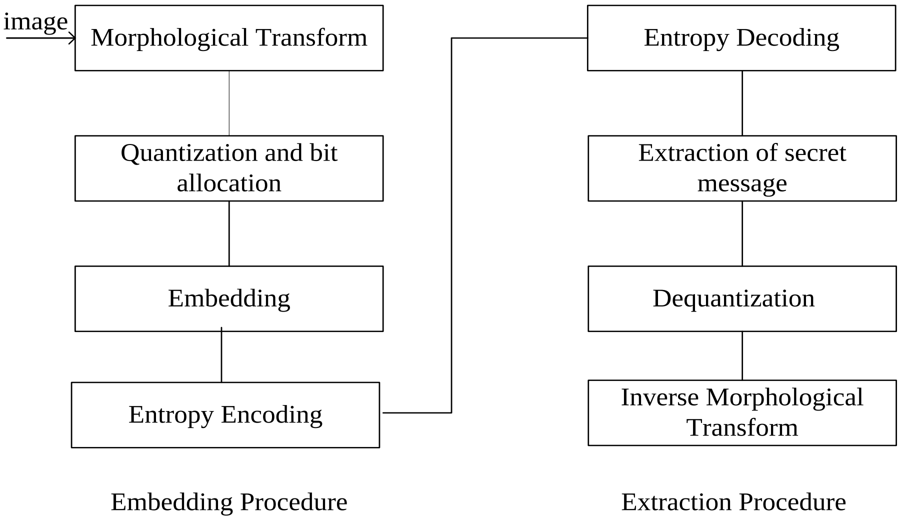

Fig 3: Block diagram of the Proposed Algorithm.

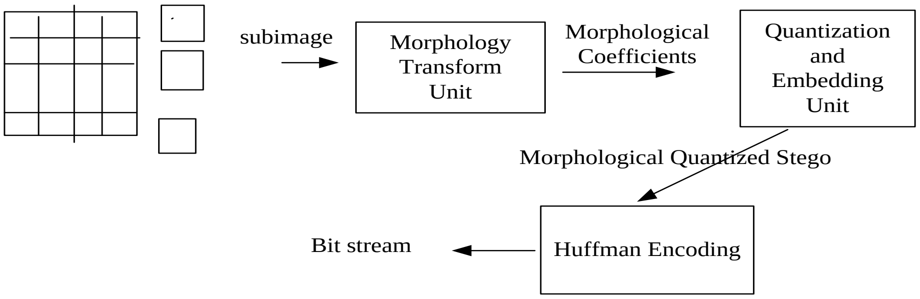
subimage
Morphology Transform Unit
Morphological Coefficients
Quantization and Embedding Unit
Morphological Quantized Stego
Huffman Encoding
Bit stream

Fig 5: Embedding and transmission phases of the new proposed algorithm.

Extracting Embedded Data: Extractionprocess in our method is depicted in Figure7. As shown in Figure 7, there exists four processing units in receiver: Huffman decoding, extraction, dequantization and recovery. At the destination,we must find the locations of the pixels of the stego image with the hidden secret message. To extract the secret message from the stego, the encoded quantized morphological stego is decoded using Huffman decoding until the quantized morphology stego is obtained. The secret message is extracted from the least significant of the quantized stego whose values are not equal to 0,1 and -1. Also, the lossy cover can be restored after dequantization and recovery units. The dequantization unit is performed based on the unique quantization table common between sender and receiver. The levels of extracting secret message are represented in Figure6.

```
Input: Encoded Stego

Output: Cover image (approximately), Secret message (exactly).

Step 1: Decode the encoded stego using Huffman decoding. Thus, the quantized morphological stego is obtained as an output.

Step 2: while the secret message is not extracted completely, repeat steps 2.1 and 2.2.

    2.1 Obtain the next Morphological coefficient of the quantized morphological stego.

    2.2 If the Morphological coefficient $\neq$ 0, 1, -1, then Extract the secret message from the least significant bit of the morphology coefficient.

Step 3. Dequantize the stego until the Morphological coefficients are obtained.

Step 4. Apply the Inverse morphology transform (Equation 5) on the stego image until the cover image is restored.
```

Fig 6: Algorithm of extracting secret message

4. EXPERIMENTAL RESULTS

All experiments were performed on a PC with core 2.35GHZ processor and 4GB main memory. The database contains 800 standard images derived from the Image Processing database [20] and Washington image database [21]. All images are converted to gray-level format with PSNR=70, and size of 512*512. In this section, the capability of the proposed method is tested using three different experiments. In experiment 1, we evaluate the quality of our method over the state-of-art methods such as DCT, wavelet steganography methods. In experiment 2, we assess the textural features of standard images:"Lena", "Cammeraman", "Peppers", and "House". In experiment 3, we check robustness of our algorithm over steganalysis attacks.

Experiment 1: Quality Assessments:

In this experiment, we used a number of standard images such as "Lena", "Peppers", "Cammeraman", and "House" with the size of 512 * 512 are selected as cover images, and we created a random secret message with a payload of 4096. To assess stego quality in our method over DCT, wavelet steganography, we computed PSNR between cover image and stego as a quality metric. As could clearly be seen in the Table 1, the quality of the stego image in the proposed algorithm is much higher than other steganography algorithm. The standard images andcorresponding stego versions are shown in Figure 8, and 9. As seen in this Figures, our method can retain the quality of stego images, so visual distortion in stego images are not visible.

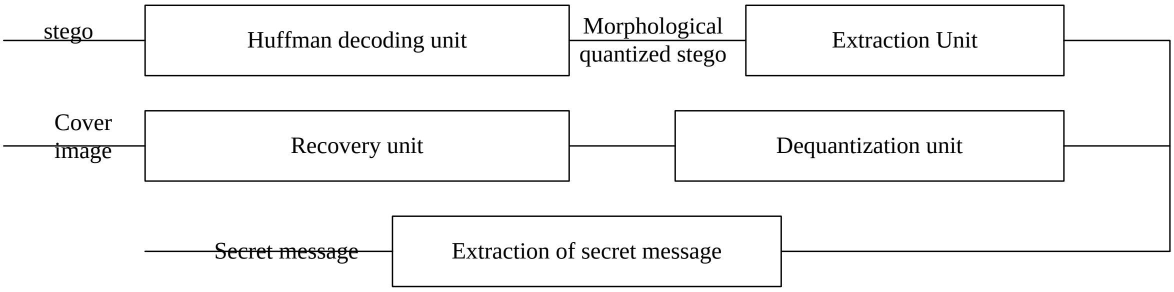

Fig 7: Extraction process of the new proposed algorithm.

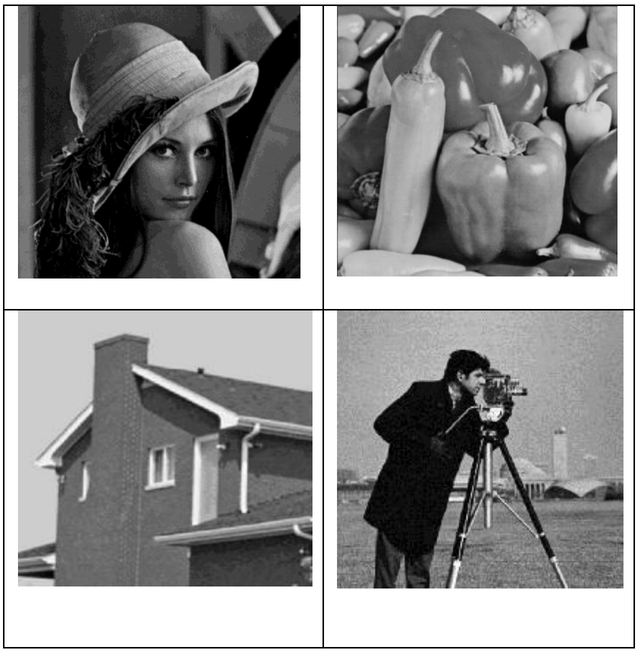

Fig 8: Standard cover images:Lena, Peppers, House, and Cammeramab

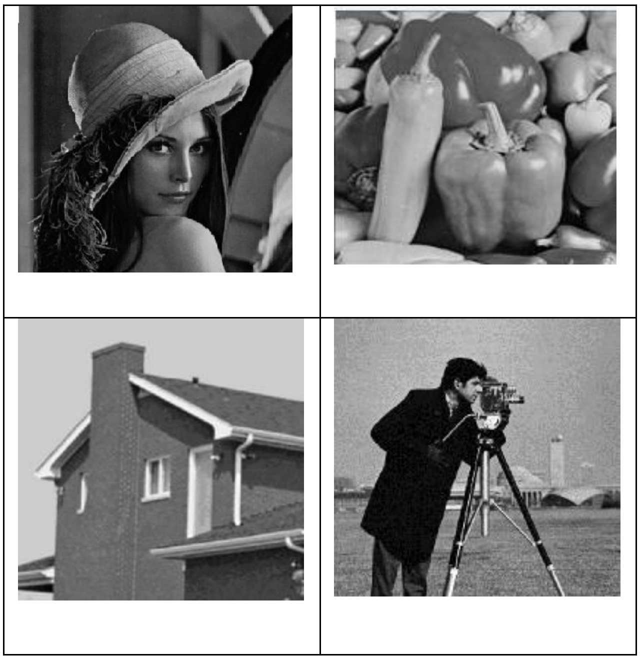

Fig 9: Stego images corresponding to standard cover images.

Table 1: PSNR of the proposed and existing steganography algorithms for test images.

Image	Transform	PSNR (Embedded bits=4096)
Lena	DCT	38.6
	DWT	40.76
	Morphology	42.9
Peppers	DCT	37.99
	DWT	38.98
	Morphology	41.87
Cammeraman	DCT	36.72
	DWT	37.9
	Morphology	40.96
House	DCT	35. 76
	DWT	37.82
	Morphology	40.3

Experiment2: Evaluation of Textural Specifications in cover images

Texture is an important feature of images that can be used for selecting appropriate cover images. Image texture represents the spatial relationship of image pixels. In this section, we extract textural features of the image via the co-occurrence matrix [23]. Textural features, including entropy, contrast, energy and homogeneity, are illustrated in Table 2 for the standard test images (Lena, Peppers, Cammeraman, House). According to texture specifications, images can be divided into two groups: (i) images with smooth texture and (ii) images with coarse textures. Coarse images contain higher frequencies and more textural details than smooth images. The image with high entropy and contrast and low energy and homogeneity is the coarse image which we expect it to encounter less distortion than the smooth image with an equal payload.

Table 2: Textural Features of Test Images.

Image	Entropy	Contrast	Energy	Homogeneity
Lena	7.5	178.76	0.258	2.42*e-4
Peppers	6.76	286.71	0.2435	6.03* e-4
Cameraman	6.434	109.31	0.25	0.0011
House	5.7	63.93	0.5	0.068

Table 3: PSNR in the proposed method.

Image	PSNR (embedded bits=10000)
Lena	38.38
Peppers	37.78
Cameraman	35.53
House	33.6

Table 2 shows that Lena and Peppers images have higher entropy and contrast, and lower Energy and homogeneity compared to Cammeraman and House images. As it can be seen in Table 3, visual distortion in coarser images is much less visible and PSNR is higher. As a result, by using coarse images as cover, we can increase PSNR.

Experiment 3: Steganalysis Results

In this experiment, we have investigated the robustness of the proposed method against steganalysis methods such as Wavelet-based and Block-based steganalysis methods introduced in [24][25]. Wavelet-based steganalysis[24] employs statistical features such as mean, variance, skewness, and SVM classifier to detect stego from clean image. Other steganalysis method, Block-based steganalysis [25], divide image into sub-blocks , and then corresponds one classifier to each sub-block, and finally it uses a voting process to decide about stego or clean cover of whole image.

All of the 800 images are employed to create two stego database with payloads of 5000, and 10000. Therefore, the size of each pair of stego-cover database is 1600 images. We randomly select 1000 images to train classifier and 600 images to test it. The accuracy of each steganography algorithm is computed based on its average true detection of stego and cover over random subset selection. The comparison of the proposed method and other state of methods is illustrated in Table 4. As seen in this table, our proposed approach has much more robustness compared to the detection algorithms.

Table 4: Accuracy of two steganalysis methods (in %) for Steganography algorithms using DCT, DWT, and Morphology Transforms.

Payload rate (bits)	**DCT**		**DWT**		**Morphology**	
	WBS	BBS	WBS	BBS	WBS	**BBS**
5000	60	61	56	57	49	**51**
10000	65	66	61	63	56	**59**

5. CONCLUSION

In this paper, a novel steganography algorithm based on Morphological Associative Memory is suggested. In our method, each bit of secret message is stored into the least significant bits of morphological coefficients. The advantage of using the Morphology operations in the embedding message is its low complexity due to the use of binary operations instead of sum of products. Also, using MAM, even if the pattern contains erosive, dilation and other noises, it can be retrieved. Consequently, the proposed algorithm inheriting the MAM specifications, can eliminate some noises generated in stego transmission procedure.The quality of stego image in this method has improved compared to the state-of-art methods. The textural assessment represents that the complex images retain the stego quality more than smooth images. In addition, this method is much more robust against to steganalysis attacks.

6. REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul McKevitt, Digital image steganography: Survey analysis of current methods, Signal Processing(2010), pp. 727–752.

[2] Mahendra Kumar, Steganography and Steganalysis of JPEG Images, Ph.D. thesis, Florida,2011.

[3] Chin-Chen Chang, Ju-Yuan Hsiao and Chi-Shiang Chan, Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy, Pattern Recognition, vol.36(2003), pp. 1583 – 1595.

[4] R.Z. Wang, C.F. Lin, J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (2001) 671–683.

[5] Z. Xiong, O. G. Guleryuz, and M. T. Orchard, A DCT-based embedded image coder, IEEE Signal Processing Letters, vol. 3 (1996), pp. 289–290.

[6] S.Winograd, On computing the discrete Fourier transform, Proceedings of the National Academy of Sciences of the UnitedStates of America, vol. 73, no. 4 (1976), pp. 1005–1006.

[7] Ahmed A. Abdelwahab and Lobna A. Hassaan, A discrete wavelet transform based technique for image data hiding, 25th National radio science conference, 2008.

[8] M. F. Tolba, M. A. Ghonemy , I. A. Taha, A. S. Khalifa, Using Integer Wavelet Transforms In Colored Image Steganography, IJICIS Vol. 4 No. 2, July 2004.

[9] RajaVikas, VenugopalPatnaik., High capacity lossless secure image steganography using wavelets,Proceeding of International Conference on Advanced Computing and Communications(2006), pp. 230–235.

[10] HediehSajedi, Mansour Jamzad, Using Contourlet Transform and Cover selection for secure Steganography. International Journal of Information Security (2010), vo. 9, Issue: 5, Publisher: Springer, pp. 1–16.

[11] Derek Upham, Jpeg-jsteg, http: //www .funet .fi/pub/crypt/steganography/jpeg-jsteg-v4.diff.gz.pp. 519–528, Cancun, Mexico.

[12] Andreas Westfeld, F5: a Steganographic Algorithm, Proceedings of the 4th International Workshop on Information Hiding, Springer-Verlag(2001), pp. 289-302.

[13] J. Fridrich, M. Goljan, and D. Hogea, Attacking the Outguess, Binghamton University Press(2000).

[14] J.Serra, Image Analysis and Mathematical Morphology, vol.2, Theoretical Advances, Academic Press, Boston,USA, 1988.

[15] G. X. Ritter and P. Sussner, An Introduction to Morphological Neural Networks, Proceedings of the 13th International Conference on Pattern Recognition (ICPR '96), vol. 4, August 1996, pp. 709–717, Vienna, Austria.

[16] G. X. Ritter, P. Sussner, and J. L. Diaz-de-Le on, Morphological Associative Memories, IEEE Transactions on Neural Networks, vol. 9, no. 2 (1998), pp. 281–293.

[17] E. Guzman, O. Pogrebnyak, C. Yanez, and J. A. Moreno, Image compression algorithm based on morphological associative memories, Proceedings of the 11th american Congress in Pattern Recognition (CIARP '06), vol. 4225

[18] Khalid Sayood, Introduction to Data Compression, second ed., Academic Press, San Diego, CA, 2000.

[19] Yu-Chen Hu, Chin-Chen Chang,A new lossless compression scheme based on Huffman coding scheme for image compression, Signal Processing: Image Communication, Volume 16, Issue 4, November 2000, pp. 367-372.

[20] Image Database , http:// www. Image processing place.com / root _files_ V3/image _ databases .htm.

[21] http://www.cs.washington.edu/research/imagedatabase/groundtruth.

[22] Y. Linde, A. Buzo, and R. M. Gray, An algorithm for vector quantizer design, IEEE Transactions on Communications, vol. 28, no. 1(1980), pp. 84–95.

[23] R.Jain, R.Kasturi, B.G.Schunk, "Machine Vision", MIT press and McGrawhill 1995.

[24] Lyu., Farid, Detecting hidden messages using higher-order statistics and support vector machines, Proceedings of 5th International Workshop on Information Hiding (2002).

[25] Seongho Cho, Byung-Ho Cha, Jingwei Wang and Jay Kuo, Block-Based Image Steganalysis: Algorithm and Performance Evaluation, IEEE International Symposium on Circuits and Systems (ISCAS) (2010), Paris, France.