Data Hiding Based on Contrast Mapping Using DNA Medium

Hayam Mousa, Kamel Moustafa, Waiel Abdel-Wahed, and Mohiy Hadhoud
Faculty of Computers and Information, Menoufia University, Egypt

Abstract: *Recently, biological techniques become more and more popular, as they are applied to many kinds of applications, authentication protocols, biochemistry, and cryptography. One of the most interesting biology techniques is deoxyribo nucleic acid and using it in such domains. Hiding secret data in deoxyribo nucleic acid becomes an important and interesting research topic. Some researchers hide the secret data in transcribed deoxyribo nucleic acid, translated ribo nucleic acid regions, or active coding segments where it doesn't mention to modify the original sequence, but others hide data in non-transcribed deoxyribo nucleic acid, non-translated ribo nucleic acid regions, or active coding segments. Unfortunately, these schemes either alter the functionalities or modify the original deoxyribo nucleic acid sequences. As a result, how to embed the secret data into the deoxyribo nucleic acid sequence without altering the functionalities and to have the original deoxyribo nucleic acid sequence be able to be retrieved is worthy of investigating. This paper applies reversible information hiding scheme on deoxyribo nucleic acid sequence by using the reversible contrast mapping technique. The reversible property makes the secret data hidden in anywhere in deoxyribo nucleic acid without altering the functionalities because the original deoxyribo nucleic acid sequence can be recovered exactly in our scheme.*

Keywords: *Security, steganography, DNA, and RCM.*

Received November 17, 2008; accepted May 17, 2009

1. Introduction

Today, network technologies have improved a lot so that more and more people access the remote facilities and send or receive various kinds of digital data over the Internet. However, the Internet is a public but insecure channel to transmit data. Thus, important information must be manipulated to be concealed while delivered via the Internet such that only the authorized receiver can get it. There are two main methods for concealing secret message traditional encryption and steganography.

Traditional encryption schemes can have the secret data concealed [6, 14, 15, 18]. In general, encryption scheme make the product of the encrypted data is meaningless, and they are like random codes. Due to the above property, they must come to the adversary's notice while delivered on the Internet, consequently, how to hide the secret information such that the product is still meaningful.

Steganography schemes hide the secret message so it can't be observed. The product of this scheme not only meaningful but also may be the same. Different methods of steganographic techniques were used from ancient times [10, 12, 16].

Nowadays, biology techniques become more and more popular, and they are applied to many kinds of applications, authentication protocols [11], biochemistry, cryptography [7, 11, 15] and so on. One of the most recently used biology techniques is Deoxyribo Nucleic Acid (DNA). DNA based steganographic techniques were used. DNA has many characteristics which make it a perfect steganographic media. These techniques depend on the high randomness of the DNA to hide any message without being noticed [7, 19].

As known, DNA is two twisted strands composed of four bases. Every DNA strand, Ribo Nucleic Acid (RNA), seems both random and meaningful. Recently, hiding secret data in DNA becomes an important and interesting research topic because of this property. In [13], a simple substitution scheme is used, where three consecutive bases are treated as a character. For example, 'B' = CCA, 'E' = GGC, and so on. As a result, there are at most 64 characters can be encoded in [13]. In [17], two methods are proposed. The first method is a simple technique to hide data in non-transcribed DNA or non-translated RNA regions, and it can be treated as a complicated version of the scheme proposed in [13]. The second method is to hide data in active coding segments without influencing the result amino acid sequence by using arithmetic coding. In [19], another DNA steganography approach is shown.

Unfortunately, these schemes either alter the functionalities or modify the original DNA sequences. As a result, how to embed the secret data into the DNA sequence without altering the functionalities and to have the original DNA sequence be able to be retrieved is worthy of investigating. Nowadays, plenty of data hiding schemes are proposed. To have the hidden data unnoticeable, the steganographic medium must be

meaningful. Different from the products of the data hiding schemes and the traditional encryption ones, DNA is not only random but also significant. Thus some schemes based on DNA were been presented. In this paper, some preliminaries were discussed in section 2. Section 3 proposes data hiding scheme. In this scheme, secret message are hidden in a DNA sequence so that the hidden data will not be detected. Moreover, the host DNA sequence can be reconstructed after the reverse operation, which far differs from the previous schemes also based on DNA. This property not only ensures the security of the secret data but also preserves the functionality of the original DNA. Some tests and experimental results are shown in Section 4. In section 5 the conclusion was driven.

2. Preliminaries and Related Work

DNA is two twisted strands composed of four bases, Adenine (A), Cytosine (C), Thymine (T) and Guanine (G). The four bases represent the genetic code. (A) bonds with the complementary (T), (G) bonds with the Complementary (C), and vice versa. Thus one strand and the corresponding complementary strand constitute DNA [17]. For example, one strand is AACGTC, and the other must be TTGCAG as shown in Figure 1. The DNA sequence determines the arrangement of amino acids which form a protein.

Transcription is the process to create RNA, an intermediary copy of the instructions contained in DNA. RNA is a single strand and contains nucleotide uracil (U), where thymine (T) would appear in DNA. For clarity, the four bases in RNA are adenine (A), cytosine (C), uracil (U) and guanine (G).

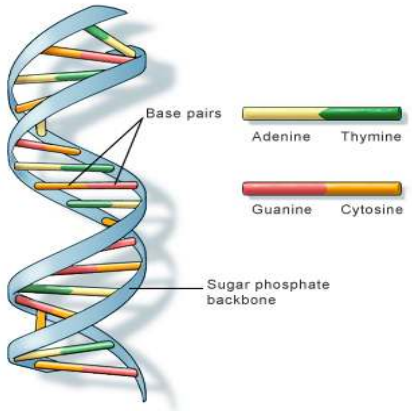

Figure 1. The structure of part of a DNA double helix.

The RNA copy (transcript) is referred to mRNA (message RNA). There are twenty distinct amino acids see Table1. On an messenger RNA (mRNA), a codon, three nucleotides, indicates which amino acid will be attached next.

In 2003, Shimanovsky *et al.* Codon redundancy is exploited in [17] to hide data in mRNA sequence. Generally, an mRNA codon is composed of three nucleotides. The possible nucleotides are U, C, A, and G. Hence, there are 4^3=64 combinations to form an mRNA codon. However, there are only twenty distinct amino acids, encoded from the mRNA codon. This clearly shows that some codons might be mapped to the same amino acids. For example, the codons 'UUA', 'CUU', 'CUA', 'UUG', 'CUC', and 'CUG' are mapped to the same amino acid Leu. Shimanovsky *et al.* exploited this redundancy to embed information in the mRNA codon. In their scheme, if the codon should be encoded with 'UUA' but the secret message is four, they use the codon 'UUG' to replace the original one. It is because 'UUG' is the fourth codon of the set of codons whose mapping amino acid is Leu, see Table 1. The replacement will not influence the transcription results, but they will modify the nucleotides of the original DNA sequence. Therefore, we need a reversible hiding mechanism that can not only conceal information into the DNA sequence but also completely restore the original sequence [2] and [3].Another watermarking schemes doesn't concern in the retrieval of the secret messages it use it as a logo or proof of ownership or as copyright protection such schemes not in need to be reversible such [8, 9].

Table 1. The mapping of codon to amino acid.

First letter	Second letter: U	Second letter: C	Second letter: A	Second letter: G	Third letter
U	UUU Phe	UCU Ser	UAU Tyr	UGU Cys	U
	UUC Phe	UCC Ser	UAC Tyr	UGC Cys	C
	UUA Leu	UCA Ser	UAA Stop	UGA Stop	A
	UUG Leu	UCG Ser	UAG Stop	UGG Trp	G
C	CUU Leu	CCU Pro	CAU His	CGU Arg	U
	CUC Leu	CCC Pro	CAC His	CGC Arg	C
	CUA Leu	CCA Pro	CAA Gln	CGA Arg	A
	CUG Leu	CCG Pro	CAG Gln	CGG Arg	G
A	AUU Ile	ACU Thr	AAU Asn	AGU Ser	U
	AUC Ile	ACC Thr	AAC Asn	AGC Ser	C
	AUA Ile	ACA Thr	AAA Lys	AGA Arg	A
	AUG Met	ACG Thr	AAG Lys	AGG Arg	G
G	GUU Val	GCU Ala	GAU Asp	GGU Gly	U
	GUC Val	GCC Ala	GAC Asp	GGC Gly	C
	GUA Val	GCA Ala	GAA Glu	GGA Gly	A
	GUG Val	GCG Ala	GAG Glu	GGG Gly	G

3. Data Hiding Scheme

The proposed scheme adopts the reversible contrast mapping technique to hide the secret message in a DNA sequence, respectively. DNA sequence is composed of four nucleotides A, C, G, and T. Hence, we need to transform the representation format of the nucleotides such that the hiding techniques can be used to conceal the secret message in a DNA sequence.

First, each nucleotide symbol of the DNA sequence is converted into a binary string. A convenient strategy is to encode each nucleotide with two bits in

alphabetical order. For example, the nucleotide A is encoded with '00', C is encoded with '01', G is encoded with '10', and T is encoded with '11'. Next, several bits of the binary formatted DNA sequence are combined to form a bit string, and then the bit string is converted to a decimal integer. Each integer in the decimal formatted DNA sequence is called a word. Let w be the length of a bit string to form a word. Let us take a DNA sequence 'AGTTCAGTA' as an example. The binary format of the sequence is '001011110100101100'. Assume that $w = 6$, the first six bits '001011' are converted to the decimal integer 11 because $(001011)_2 = (11)_{10}$. Hence, the decimal format of the DNA sequence 'AGTTCAGTA' is '11 52 44'. After that, the decimal formatted DNA sequence can be used to conceal the secret message.

3.1. Contrast Mapping

Let [0, L] be the range of values for each word (L=63 for six-bit word length), and let (x, y) be two consecutive words. The forward Reversible Contrast Mapping (RCM) transforms pairs of values into another pairs of values.

$$x' = 2x - y, y' = 2y - x. \quad (1)$$

To prevent overflow and underflow, the transform is restricted to a sub Domain (D) D $\subset$ [0, L] $\times$ [0, L] defined by the equations

$$0 \le 2x - y \le L, 0 \le 2y - x \le L \quad (2)$$

As shown in Figure 2, D is the domain located along the diagonal of [0, L] $\times$ [0, L].

The inverse transform is defined as follows:

$$x = \left\lceil \frac{2}{3}x' + \frac{1}{3}y' \right\rceil, y = \left\lceil \frac{1}{3}x' + \frac{2}{3}y' \right\rceil \quad (3)$$

where $\lceil a \rceil$ is the ceil function (the smallest integer greater than or equal to a). The pair forward-inverse transform should give exact results, even if the Least Significant Bit (LSBs) of the transformed values is lost. If x' and y' are not changed, equation 3 exactly inverts equation 1, even without the ceil functions. By watermarking, the LSBs of x', y' are lost. Let us set to "0" the LSBs of x' and y'. It immediately appears that if the LSB of x' was "1" the values inside the ceil functions for the computation of x and y decrease with 2/3 and 1/3, respectively. Similarly, if the LSB of y' was "1" the corresponding values decrease with 1/3 (for the computation of x) and 2/3 (for the computation of y). Except when both LSBs are "1" the ceil function recovers the correct results. An LSB of "1" means an odd integer number. From equation 1, it follows that (x', y') are both odd numbers only if (x, y) are odd numbers too. To conclude, on D without the set of odd pairs, the inverse RCM transform performs exactly, even if the LSBs of the transformed pairs of values are lost.

3.2. Data Hiding Scheme

The watermark substitutes the LSBs of the transformed pairs of values. At detection, in order to extract the watermark and to restore the original values, each transformed pair should be correctly identified. The LSB of the first value of each pair is used to indicate if a pair was transformed or not "1" for transformed pairs and "0" otherwise.

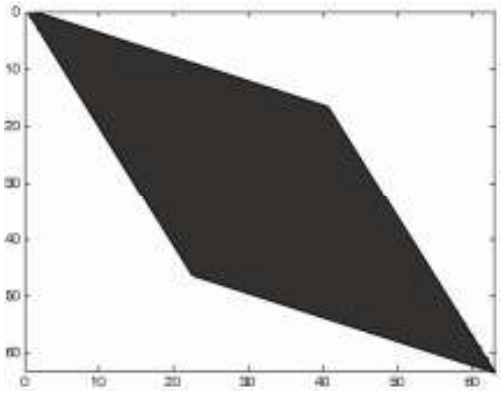

Figure 2. Transform domain.

The forward transform should not introduce visual artifacts. [1] The inverse RCM fails to recover the pairs (x, y) $\in$ D composed of odd values. Such pairs can be used as well for data embedding as long as they are correctly identified at detection. This can be easily solved by setting the LSB of the first value to "0". At detection, both LSBs are set to "1" and equation 2 is checked. If equation 2 is fulfilled, the pair was composed of odd values. In order to avoid decoding ambiguities, some odd pairs of values should be eliminated, namely, those pairs located on the borders of D. The pairs subject to ambiguity are found by solving in odd numbers the equations: $2x$-y=1, $2y$-x=1, $2x$-y=L and $2y$-x=L. Let further D_c be the domain of the transform without the ambiguous odd pixel pairs. [4]

3.2.1. Hiding Algorithm

The detail of the hiding procedure is illustrated in Figure 3. A different marking procedure is proposed in [5]. A map of transformed pairs and the sequence of LSBs for all non-transformed pairs are first collected. Then, the entire sequence LSB plane is overwritten by the payload and by the collected bit sequences.

Thus, all the information needed to recover any original word pair is embedded into the pair itself or very close to it. In the case of cropping, except for the borders where some errors may appear, the original words of the cropped sequence are exactly recovered together with the embedded payload. For word pairing on row or column direction, there are no problems of

synchronization. Some control codes should be inserted in the payload to validate watermark integrity.

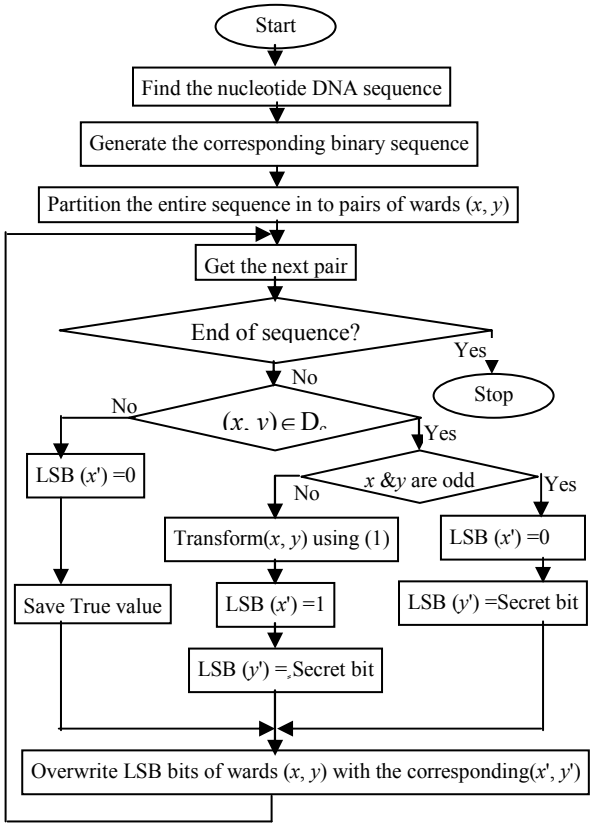

Figure 3. Flowchart of hiding scheme.

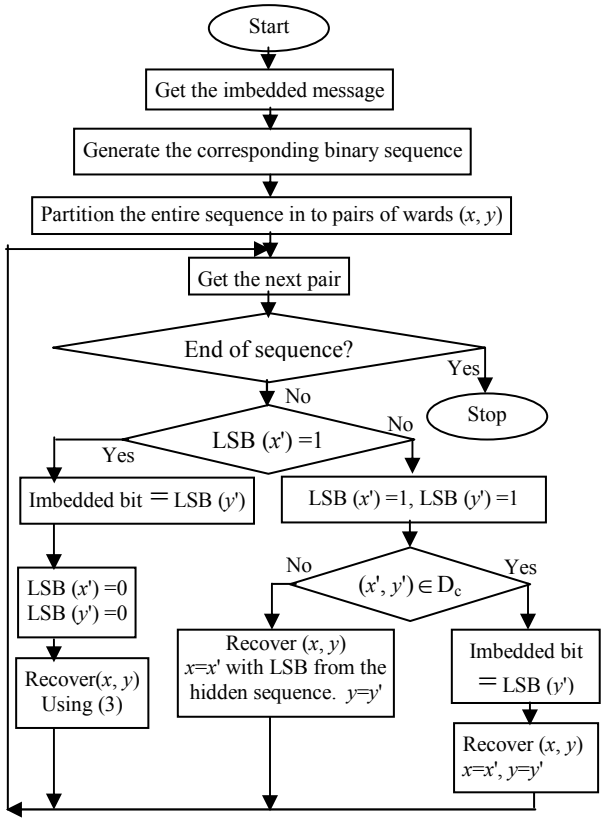

Figure 4. Flowchart of the detection scheme.

3.2.2. Detection of Hidden Data and Recovering the Original Data

Hidden message extraction and exact recovery of the original DNA sequence is performed as in Figure 4.

4. Experimental Results

Experiments were carried out to evaluate the performance of the proposed scheme. The proposed scheme was tested on a 797 MHz CPU. Laptop with 256 RAMS. The system uses the Visual C++ function random ( ) to generate pseudo-random numbers and a secret message.

First, the proposed data hiding scheme was tested on a sequence with different Word Length (|w|'s) to determine the proper length of a bit string to form a word. In this experiment, we only hide a secret bit in the rightmost bit of the second word of the pairs if it belongs to D_c. The experimental results are given in Table 2. The column |w| in the table is the length of a bit string to form a word. The column 'Total # words' is the total number of words in the DNA sequence, '# Hidden bits' is the total number of bits which we conceal in the sequence ,we can call it the payload, and '# unused words' is the total number of words which doesn't involved in hiding a bit of the secret message (which doesn't belong to D_c) , and '# used words' is the number of words which actually conceal our secret message(# unused words + # used words = Total # words) .Figure 5 show the relation between the variables illustrated above.

Now we want to know the value of |w| which make the scheme give the best performance. The performance is measured by bit per nucleotide (bpn). '*bpn*' is the abbreviation of *bit-per-nucleotide* that is the measurement to estimate the hiding capability of each nucleotide in the DNA sequence. The *bpn* is computed by:

$$bpn = \frac{number\ of\ \ hidden\ bits}{total\ \ number\ of\ \ words}$$

We used the same DNA sequence in this experiment RSNn256728 (Sequence: RSNnx where RSNnx is the sequence name, Random Sequence of Nucleotides (RSN) stands for RSN, n is the word length (one digit), x is number of nucleotides in this sequence). Each time we divide this sequence into different word length (different values for n) and evaluate the corresponding *bpn.* The results of this experiment are shown in Table 3. Obviously, the reversible contrast mapping scheme has the best performance for |w| = 4 as shown in Figure 6. This is not usually the best value of |w| as it is constrained by some randomness.

Table 2. Results of the proposed scheme.

|w|	Total Words	Hidden Bits	Unused Words	Used Words	bpn
2	168936	37072	94792	74144	0.219444
4	84468	20095	44278	40190	0.237901
6	56312	9130	28504	18260	0.162132
8	42234	426	28204	852	0.010087

From the results shown in Table 3, we notice that the maximum value of *bpn* is 0.47 approximately 0.5. This is a natural conclusion where the algorithm use two words of the available DNA sequence to hide only one bit of the secret message, consequently the maximum value that can *bpn* reach is 0.5 corresponding to hiding one bit every two words. Moreover, not all pair of words is available for concealing a bit of the secret message (the pairs which doesn't belong to D_c), so that *bpn* value isn't exactly 0.5 it is less than this value somewhat.

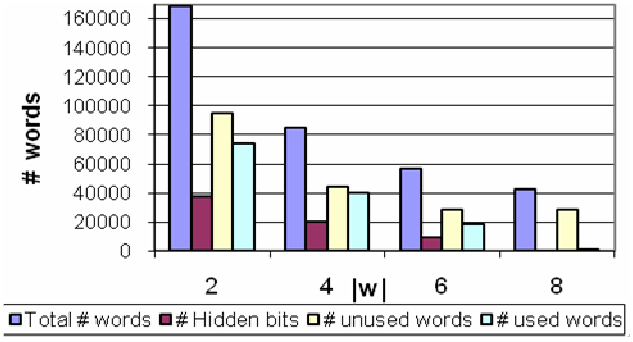

Figure 5. The relation between the variables.

Table 3. The value of bpn for different values of |w|.

|w|	1	2	4	6	8
bpn	0.249142	0.438888	0.475802	0.324264	0.324264

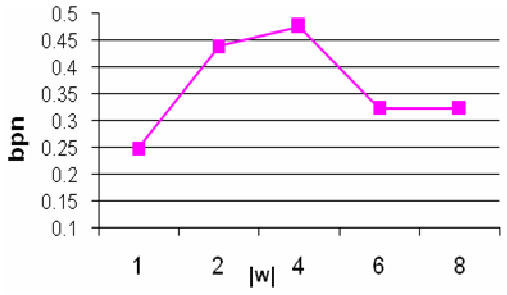

Figure 6. The performance of the algorithm is the best where |w|=4.

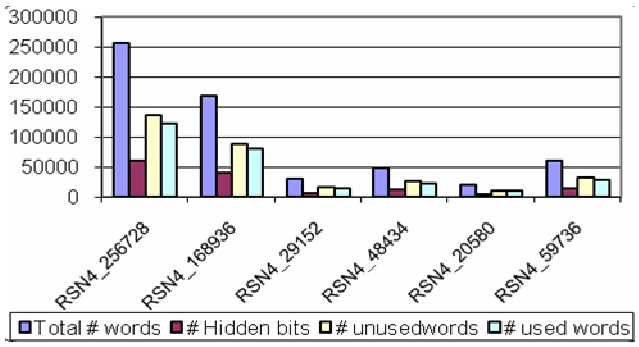

Figure 7. The value of the scheme variables for the same |w| on different DNA sequences.

Next, we tested the proposed data hiding scheme on some DNA sequences with w =4 to examine the hiding performance. The experimental results are shown in Table 4. The relation between the scheme variables is shown in Figure 7. From the results we can conclude that the value of *bpn* follow the same ratio approximately. It is the same for different sequences with the same word length as shown in Figure 8.

Table 4. Results of the proposed scheme on the tested sequences with |w|=4.

Sequence Name	Total Words	Hidden Bits	Unused Words	# Used Words	bpn
RSN4256728	256728	60781	135166	121562	0.236753
RSN4168936	168936	40127	88682	80254	0.237528
RSN429152	29152	6883	15386	13766	0.236107
RSN448434	48434	11462	25510	22924	0.236652
RSN420580	20580	4900	10780	9800	0.238095
RSN459736	59736	14185	31366	28370	0.237461

The proposed scheme not only can conceal secret data in DNA sequence but also it can do so in the gray-level images and color images. In this subsection, we compare the performance of the proposed scheme with that of Alattar's scheme applying spatial triplet and quad algorithm and Tianding algorithm using Lena and Baboon color images [1, 3].

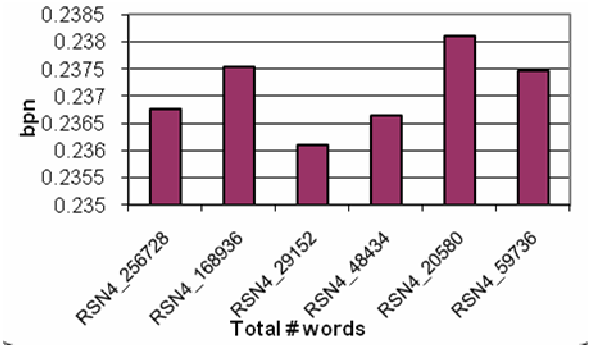

Figure 8. The performance of the algorithm for the same word length on different DNA sequences.

The results of the proposed scheme on Lena true color image is shown in Figure 9 The results of the above mentioned schemes are shown in Figure 10 derived from [3] for the same image. The results of the proposed scheme on the Baboon true color image are shown in Figure 11 and the results for the same image using the above schemes are shown in Figure 12. We can determine to what extent the proposed scheme influence the media if it is translated into image instead of DNA. This is illustrated in Figure 13 we can see the original Baboon image. In Figure 14 we can see the Baboon image after applying the proposed scheme. The proposed scheme doesn't outperform the Alattar's triplet, quad and Tianding in the values of Peak Signal to Noise Ratio (PSNR). The proposed scheme isn't effective if we are interested in the PSNR as it leads to lower PSNR values. Although, this characteristic is very important in some applications where we want the steganographic medium not to be influenced by the

secret message in the hiding process such as medical, military and other applications which use very sensitive data, the algorithm is reversible so that, the original data can be recovered entirely.

The experimental results of the proposed scheme on Lena, with Different values of word lengths are shown in Table 5. The results on Baboon are shown in Table 6**.** Column bit per pixel (bpp) refers to "bit per pixel". This value differs from *bpn* where each pixel is 8 bit length. Each pixel may be divided into 2 or 4 words depending on the word length |w|. This process duplicates the number of words which increase the payload.

if |w|=8 ------◊*bpp*=1**bpn*
if |w|=4-------◊*bpp*=2**bpn*
if |w|=2-------◊*bpp*=4**bpn*

Thus the maximum value of *bpp* achieved in this experiment is 0.74.

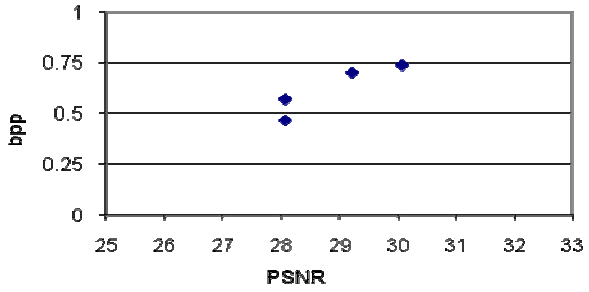

Figure 9. Capacity-distortion performance of the proposed scheme on colored Lena image.

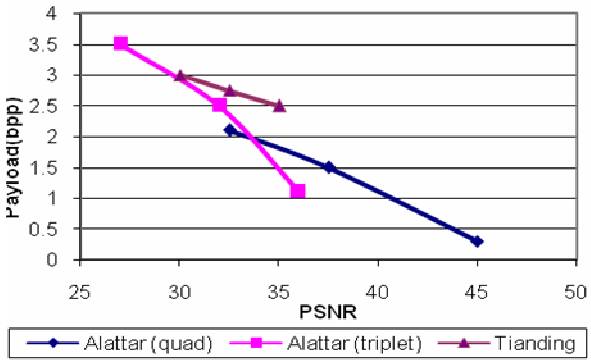

Figure 10. Capacity-distortion performance comparisons between Alattar's scheme and the Tianding scheme on Lena.

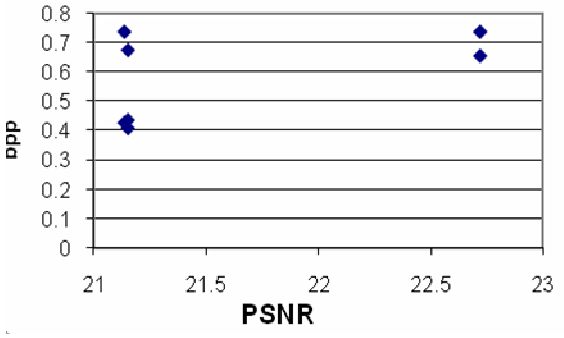

Figure 11. Capacity-distortion performance of the proposed scheme on colored baboon image.

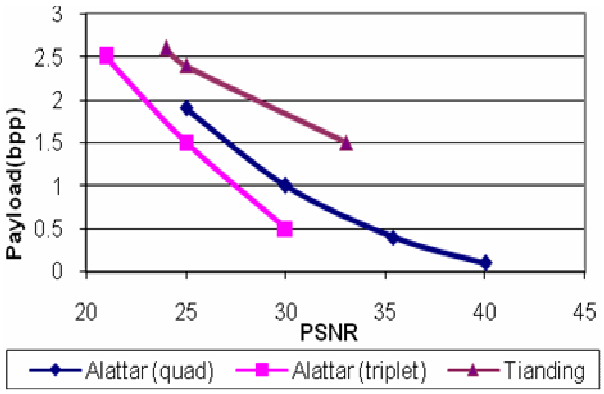

Figure 12. Capacity-distortion performance comparisons between Alattar's scheme and the Tianding scheme on baboon.

Figure 13. Original baboon image.

From the Figures illustrated above the proposed scheme doesn't achieve good results from the PSNR point of view. The PSNR usually does not exceed 31 db, but it is comparable from the *bpn* as the maximum *bpp* achieved is 0.74. This property doesn't influence our algorithm performance as it is applied on DNA medium. If DNA medium changed, it is still random, meaningful and significant, so that, they didn't come to the adversary's notice while delivered on the Internet.

Figure 14. Baboon after applying the proposed scheme.

Table 5. Results of the proposed scheme on Lena colored image with different values of |w|.

Color Component	|w|	Total Words	Hidden Bits	bpn	bpp
R	8	262144	130144	0.496460	0.496460
	4	524288	148890	0.283985	0.567970
	2	1048576	244943	0.233596	0.467192
G	8	262144	127470	0.486259	0.486259
	4	524288	117087	0.223326	0.446652
	2	1048576	183512	0.175011	0.700044
B	8	262144	130705	0.498600	0.498600
	4	524288	130702	0.249294	0.498588
	2	1048576	194238	0.185240	0.740960

Table 6. Results of the proposed scheme on baboon with different values of |w|.

CC	|w|	Total Words	Hidden Bits	bpn	bpp
R	8	262144	111824	0.426575	0.426575
	4	524288	172092	0.328239	0.656478
	2	1048576	193749	0.184773	0.739092
G	8	262144	111824	0.426575	0.426575
	4	524288	172092	0.328239	0.656478
	2	1048576	193749	0.184773	0.739092
B	8	262144	106871	0.407681	0.407681
	4	524288	114223	0.217863	0.435726
	2	1048576	177318	0.169104	0.676416

5. Conclusions

This paper introduced a reversible information hiding scheme for DNA sequence based on reversible contrast mapping. The scheme uses two words of the sequence with the reversible contrast mapping to achieve reversibility.

The scheme was implemented and performed on different DNA sequences. For |w|=4, the algorithm gives the best performance. The value of *bpn* is approximately the same for the same value of word lengths |w| even if we change the sequence length. The proposed scheme can not only hide secret information in the DNA sequence but also recover the original DNA sequence from the hidden results without loss. Reversible information hiding is a new technique that can be broadly applied in covert communication, digital rights management, and content authentication and sensitive data applications. In such domains one of the most effective parameter in data hiding is the noise versus the amount of hidden data, so the proposed scheme is so comparable in such cases, as it cause high rate of hiding secret data in the media used compared with the ratio of noise which affect the media.

References

[1] Alattar M., "Reversible Watermark Using the Difference Expansion of a Generalized Integer Transform," *Computer Journal of IEEE Transactions on Image Processing*, vol. 13, no. 8, pp. 1147-1156, 2004.

[2] Chang C., Lu T., Chang Y., and Lee C., "Reversible Data Hiding Schemes for DEOXYRIBONUCLEIC ACID Medium," *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 5, pp. 1-16, 2007.

[3] Chen T., *A Novel Biology-Based Reversible Data Hiding Fusion Scheme*, Springer-Verlag, 2007.

[4] Coltuc D. and Chassery J., "Very Fast Watermarking by Reversible Contrast Mapping," *Computer Journal of IEEE Signal Processing Letters*, vol. 14, no. 4, pp. 144-146, 2007.

[5] Coltuc D. and Tremeau A., "Simple Reversible Watermarking Schemes," *Computer Journal of SPIE: Security, Steganography, Watermarking Multimedia Contents*, vol. 5681, no. 214, pp. 561-568, 2005.

[6] ElGamal T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *Computer Journal of IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[7] Gehani A., Labean T., and Reif J., "DNA Based Cryptography," *Computer Journal of IMACS DNA-Based Computer, American Mathmatical Society*, USA, vol. 2950, no. 456, pp. 34-50, 2004.

[8] Heider D. and Barnekow A., "*DNA- Based Watermarks Using the DNA-Crypt Algorithm*," *Computer Journal of BMC Bioinformatics*, vol. 8, no. 1, pp. 176-176, 2007.

[9] Heider D. and Barnekow A., "DNA Watermarks: a Proof of Concept," *Computer Journal of BMC Molecular Biology*, vol. 9, no. 5, pp. 45-49, 2008.

[10] Hwang J. and Chang C., "Hiding a Picture in Two Pictures," *Computer Journal of Optical Engineering*, vol. 40, no. 3, pp. 342-351, 2001.

[11] Leier A., Richter C., Banzhaf W., and Rauhe H., "Cryptography with DNA Binary Strands," *Computer Journal of BioSystems*, vol. 57, no. 2, pp. 13-22, 2000.

[12] Lin H., Hu C., and Chang C., "Both Color and Gray Scale Secret Images Hiding in a Color Image," *Computer Journal of International Journal on Pattern Recognition and Artificial Intelligence*, vol. 16, no. 6, pp. 697-713, 2002.

[13] Peterson P., "Hiding in DNA," *in Proceedings of Muse*, pp. 22, 2001.

[14] Rijmen P., "Advanced Encryption Standard," *in Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pp. 19-22, 2001.

[15] Rivest L., Shamir A., and Adleman L., "A Method for Obtaining Digital Signature and

Public Key Cryptosystem," *Computer Journal of Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[16] Saeb M., El-abd E., and El-Zanaty M., "On Covert Data Communication Channels Employing DNA Recombinant and Mutagenesis-based Steganographic Techniques," *Computer Journal of BioSystems*, vol. 57, no. 2, pp. 13-22, 2000.

[17] Shimanovsky B., Feng J., and Potkonjak M., *Hiding Data in DNA*, Springer, UK, 2003.

[18] Smid E. and Branstad M., "Data Encryption Standard," *in Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, pp. 550-559, 1988.

[19] Wendell M., "DNA Based Steganography for Security Marking," *in Proceedings of Xix International Security Printers Conferences, Montreux*, pp. 14-16, 2003.

Hayam Mousa received her BSc degree in 2006, Information Technology Department, Faculty of Computers and Information. She prepares her MSc in Menoufia University, Shiben El-Kom, Egypt.

Kamel Moustafa is an assistant professor, Information Technology Department, Faculty of Computers and Information, Menoufia University, Shiben El-Kom, Egypt.

Waiel Abdel-Wahed is a professor and head of Operations Research & Decision Support Department, Vice Dean of Faculty of Computers and Information, Menoufia University, Shiben El-Kom, Egypt.

Mohiy Hadhoud is a professor and dean of Faculty of Computers and Information, Menoufia University, Shiben El-Kom, Egypt.