IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

# An Efficient Approach for Data Security based on DNA Algorithm

**Deen Dyal Sharma[1], Er. Varinderjit Kaur[2], Dr. Naveen Dhillon[3]**

Dept. of Computer Science and Engg, Ramgarhia Institute of Engg and Tech, Phagwara, Punjab[1]

(HOD) Dept. of Computer Science and Engg, Ramgarhia Institute of Engg and Tech, Phagwara, Punjab[2]

Principal, RIET Phagwara, Ramgarhia Institute of Engg and Tech, Phagwara, Punjab[3]

**Abstract:** As technology is growing, role of digital media becomes productive. Consequently, recording, editing and duplication of multimedia contents happen. Thus, protection and illegal use of digital media should be blocked. For this purpose, digital watermarking has become a consideration for the researchers. Due to this concept, online contents can keep safe and protect. There are numerous techniques have been proposed for image watermarking. In this thesis, a new technique has been proposed named as DNA optimization technique. Evaluations have been performed on the image and results show the performance of the proposed work. Additionally, alluded to as basically watermarking, an example of bits embedded into a computerized picture, sound or feature document that recognizes the record's copyright data (creator, rights, and so on.). The name originates from the faintly obvious watermarks engraved on stationery that recognize the maker of the stationery. Using this concept secure transmission can be possible with this technique.

**Keywords:** Steganography, Watermarking, Spatial Domain, Frequency Domain,

## I. INTRODUCTION

A watermark is the concealed data inside an advanced sign, (for example, picture, feature, sound, polygonal model. It is coordinated into the substance of host sign itself, and obliges no extra record header or change of information arrangement also.

The reason for advanced watermarks is to give copyright security to protected innovation that is in computerized organization. Dissimilar to printed watermarks, which are planned to be to a degree obvious, advanced watermarks are intended to be totally undetectable, or on account of sound clasps, unintelligible.

Image watermarking is also known as steganography. It is a process in which the image is hidden behind the image. The image which is used for hiding the watermark is known as cover image. The watermarked image is embedded on the cover image by using various embedding techniques. The watermark is embedded after applying various encryption techniques for providing high security to the data or digital data.

### APPROACHES OF WATERMARKING

**Spatial Domain Approach**

The most punctual watermarking strategies are primarily this kind and the easiest case is to implant the watermark into slightest critical bits (LSBs) of the picture pixels. On the other hand, this system has generally low data concealing limit and can be effortlessly eradicated by lossy picture pressure**.**

**Frequency Domain Approach:** An alternate approach to create great watermarked picture is by first changing the first picture into the recurrence space by the utilization of Fourier, Discrete Cosine or Wavelet changes for instance. It is also known as Transform domain.

It uses various frequencies to insert the data or watermark behind the video. It uses domain methods to implement the watermark. Transform domain techniques are broadly classified such as

- **Discrete Fourier transformation technique (DFT):** It replaces the unique functions with frequency components. In case of digital image, the even function refers to the frequency value of sine or cosine functions and then this function is multiplied with the eight values. It generates the coefficient of Fourier transform in the signal.
- **Discrete cosine transformation technique (DCT):** It adds watermarks to a still digital image. In this the image is presented in the form of frequencies of cosine. Then 8*8 blocks of the image is considered calculating the DCT of the image**.**
- **Discrete Wavelet transformation technique (DWT):** It is a technique which is used for embedding watermark behind digital data like image or video. It generates the frequency corresponding to signals.

## II. METHODOLOGY

This section describes the methodology and Block diagram of proposed technique for image watermarking. The proposed methodology is divided into two sections.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

One is the embedding of the data into the image and other section is the extraction of data from the image. In this proposed methodology, the DNA technique is used for the purpose of efficient data hiding.

**3.3.1 Embedding of watermark:**

Methodology of the data embedding process is as follows:

1. Select a cover image on which the image is going to be watermarked.
2. Select the image which is going to be hiding behind the cover image.
3. In this step apply DNA encryption on image which is going to be used as watermark.
4. After encrypting the image of watermark, embed the image behind the cover image.
5. An image is generated in this step which is final watermarked image (Stegno image).
6. On the basis of obtained image calculate result parameters.

Following is the block diagram which shows the process of **embedding digital data** in image for the watermarking purpose.

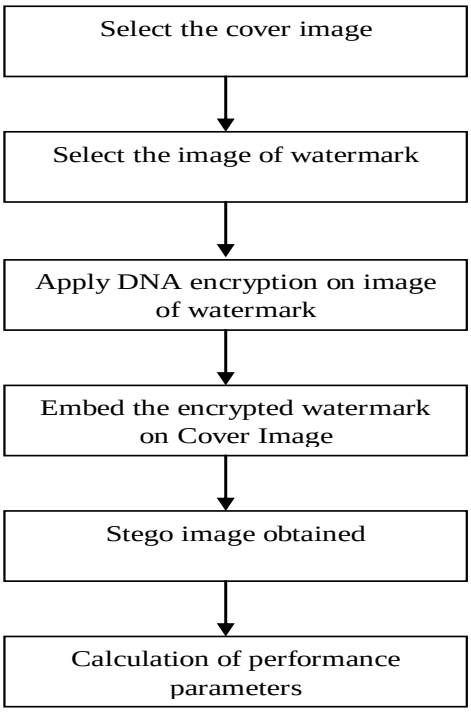


Figure 1 Block Diagram for embedding data

**3.3.2 Extraction of watermark**

After encrypting the data, it needs to be decrypting the stego image for extracting the watermark. The methodology is as follows:

1. For the extraction of the data the encrypted image (stego image) is loaded in which the data is hiding by the sender.
2. After selection of the image, next step is to extract the watermarked image. The extracted image contains the hidden information.
3. After extracting the image, DNA decryption is applied to extract the original image.
4. Finally, the original watermarked image will be obtained.

Following is the block diagram of **extracting data** after embedding watermarking in image.

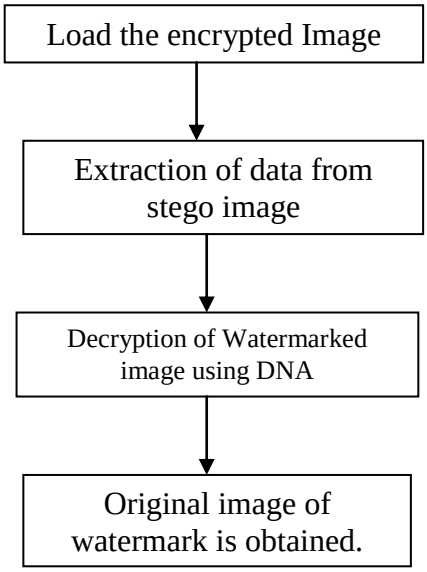


Figure 2 Block diagram for data extraction

## III. PROBLEM FORMULATION

Watermarking is a technique of hiding digital data in the image for authentication purposes. Watermark that is to be embedded in the image can be visible or invisible depending on the type of technique used to embed the watermark. The watermark embedded should not change the information of the image. The traditional technique of image watermarking is DCT. It adds watermarks to a still digital image. In this the image is presented in the form of frequencies of cosine. Then 8*8 blocks of the image is considered calculating the DCT of the image. DCT (Discrete Cosine Transformation): It add watermarks to a still digital image. In this the image is presented in the form of frequencies of cosine. Then 8*8 blocks of the image s considered calculating the DCT of the image. The disadvantages of DCT are as follows:

1. Block effect
2. Effect of picture cropping
3. One of the main problems and the criticism of the DCT is the blocking effect. In DCT images are broken into blocks 8x8 or 16x16 or bigger. The problem with these blocks is that when the image is reduced to higher compression ratios, these blocks become visible. This has been termed as the blocking effect.

## IV. PROPOSED SYSTEM

A watermark is hidden information within a digital signal. It had the problem that the information about the original image used for embedding data had to be preserved for

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

every image. That scheme had high tolerance for image processing in comparison with a conventional scheme. The conventional techniques of watermarking employed DCT i.e. Discrete Cosine Transformation which had various drawbacks like less security, more error probability and data compression. To improve the results of the conventional techniques some changes needs to be made in these techniques. The proposed technique introduced image watermarking DNA computing is applied in cryptography for massive parallelism, huge storage and ultra-low power consumption.

Therefore, the DNA-based schemes have been proposed in recent years. The DNA method is effective for solving the storage problem of the one- time pad, because DNA has extra ordinary information density and is very suitable to store a huge one-time pad. The huge one-time pad in crypto systems is efficient to resist chosen plain text attacks.

So, the aim of this proposed technique is to overcome the disadvantages of the conventional techniques like data compression, less security and more error probability. Need of security, lower error probability and lower data compression needs to be introduced in the new approach. Introducing a technique of DNA algorithm and works in spatial domain is helpful to overcome these drawbacks to a greater extent. This technique improves data compression as well as will encode lesser data size, number of bits will reduce and so the PSNR of the system improves. This hybrid technique also decreases error probability and so the security of the technique increases. The earlier techniques used for watermarking are improved in this new technique and a better-quality watermarking is achieved which yields better and efficient results than the conventional techniques.

## V. RESULTS AND DISCUSSIONS

In this section the proposed technique is simulated in MATLAB in order to calculate or measure its performance with respect to traditional techniques. The following results show that how the proposed technique is better than the previous once.

Figure 3 List of sample images used for watermarking

In above figure 3 there are 6 images which are used as cover image in proposed work for image watermarking.

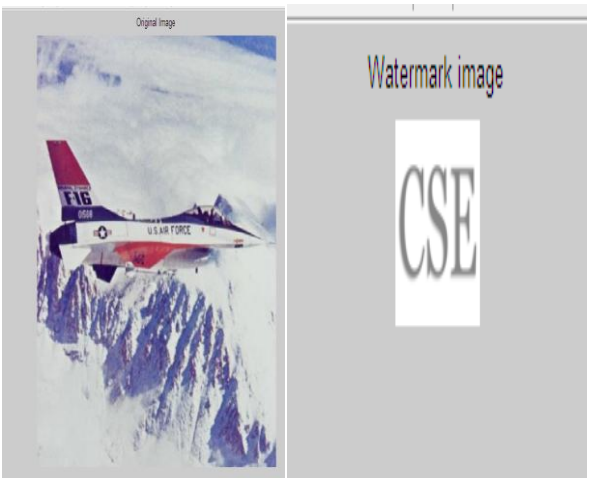


Figure 4 Original or cover image Figure 5 Image of watermark

In above figure 4 shows an image which is going to be used as the cover image for the purpose of watermarking.

Figure 5 shows an image of data which is going to be hidden behind the cover image for the purpose of providing security to the cover image from unauthorized access.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016

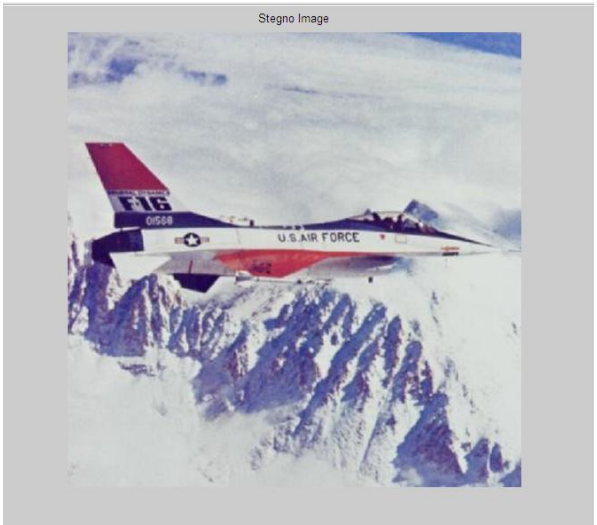


Figure 6 Watermarked Images

Figure 6 depicts an image (Stegno image) which is observed after implanting or embedding the watermark on the cover image. This is an invisible watermarking hence the watermark will not be visible by the end user directly. In order to view the watermarks extraction algorithms, have to be applied by using the Stegno image.

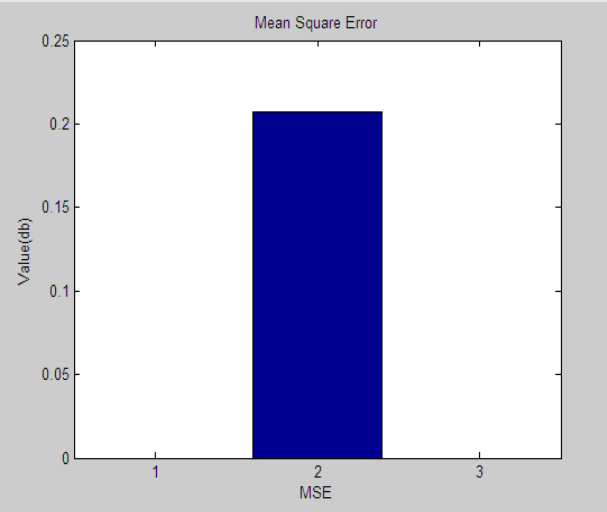


Figure 7 graph of MSE

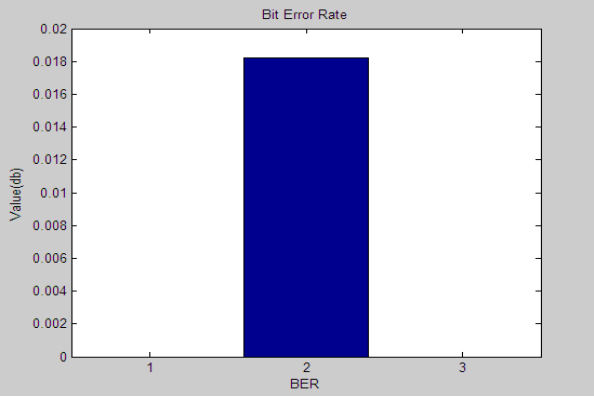


Figure 8 graph of BER

Figure 7 shows the graph which depicts the Mean Square Error of the proposed technique. Figure 8 shows the graph of the BER i.e. Bit Error Rate of the proposed technique.

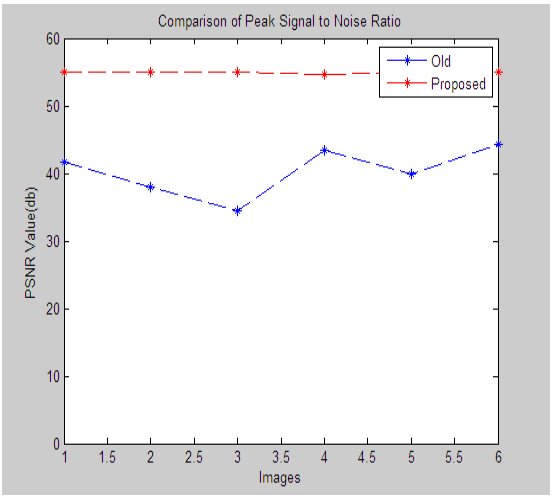


Figure 9 comparison graph of PSNR

Figure 9 shows a comparison graph PSNR (Peak Signal to Noise Ratio). It is a measurement used to measure the amount of data and noise in a signal. Higher the PSNR ratio means lesser the noise in the signals. From above figure, it is clear that the PSNR of proposed technique is higher than the older one. In older work the PSNR rate curve is fluctuating constantly along with the variations in the image. Whereas in proposed work the PSNR curve is stable and poses the higher value as compare to the older PSNR value.

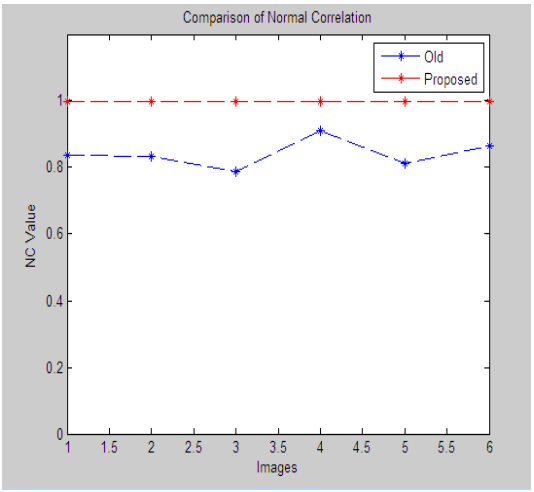


Figure 10 comparison graph of Normal correlation

In figure 10 graphs shows the comparison of NC i.e. Normal correlation between proposed and old work. Normal correlation is factor which is used for measuring the correlation between input and output. In this graph the correlation in case of proposed technique is high which shows the proposed technique is better than the older one where the correlation value is low and fluctuating constantly.


DOI 10.17148/IJARCCE.2016.51129

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 11, November 2016


Figure 11 Extracted Watermarks

Figure 11 shows the image of watermark which is observed after applying the extraction algorithms on the Stegno image.

## VI. CONCLUSION AND FUTURE SCOPE

Watermarking is an efficient method of hiding the data in the carrier signal; Watermarking is done to protect the confidential data from unauthorized access. Image watermarking is a process of hiding data in the image. The security of the data that is send is the major issue. Traditional may algorithm, have been proposed for the image watermarking but the results achieved were not efficient.

It is analyzed that in future further work can be done by using some trending encryption technique. This will also increase the security of the data that is the major concern. So, in future the work can be done on some other encryption technique or by combing the various compression techniques. In addition to this various other data hiding technique can also be used.

## REFERENCES

1. Myasar Mundher ,2014"Digital Watermarking for Images Security using Discrete Slantlet Transform", Appl. Math. Inf. Sci. 8, No. 6, 2823-2830
2. Monika Patel et al.," Analysis and Survey of Digital Watermarking Techniques", ijarcsse, vol 3(10), Pp 203-210, 2013
3. Antonio Cedillo-Hernandez," Transcoding resilient video watermarking scheme based on spatio-temporal HVS and DCT", ELSEVIER, Vol 97, Pp 40-54, 2014
4. Sunil Sharma "An Enhanced Video Watermarking Approach for Robustness and Security Using Pixel and Transform Domain in An Uncompressed Video", IJARSET, Vol. 2 Issue V, pp 41-46
5. Monika Sharma "A Hybrid technique of Video Watermarking in Wavelet domain and Scan based Encryption Method", IJEDR, Volume 2, Issue 3, pp 3220-3223
6. I. Sivakami* "A digital watermarking system for video authentication using the DCT", Integrated Journal of Engineering Research and Technology (IJERT) Jan-Feb 2014, Vol 01, 22-33
7. Li, Chen. (2013, December). The study on digital watermarking based on word document. IEEE. pp. 2265-2268.
8. Sghaier guizane (2012) "An audio/video crypto — Adaptive optical steganography technique", IEEE, 2012
9. Chang, E.,"A survey of digital image watermarking techniques", IEEE International Conference on ,IEEE, (pp. 709-716), 2005
10. Dong, Journal of Chemical and Pharmaceutical Research, 2014, 6 (3): 78-89. Journal of Chemical and Pharmaceutical Research, 6(3), 78-89, 2014
11. Ekta Miglani ,2014"Digital Watermarking Methodologies - A Survey", IJARCSSE, Volume 4, Issue 5, pp 826-832
12. Dr.V.Seenivasagam "A Survey on Video Watermarking and Its Applications", IJERA, Vol. 4, Issue 12( Part 6), pp.39-44, 2014
13. Sharma, "A Hybrid technique of Video Watermarking in Wavelet domain and Scan based Encryption Method", 2014
14. Pawan Singh Shekhawat ,"Non Blind DWT Based Multiplicative SVD Watermarking Algorithm", IJSRD, Vol. 3, Issue 03, pp 1844-1848, 2014
15. Islam, A Novel Approach for Image Steganography Using Dynamic Substitution and Secret Key. American Journal of Engineering Research (AJER) Volume-02, Issue-09, 2013
16. Al-Shatnawi, A. M. , A new method in image steganography with improved image quality. Applied Mathematical Sciences, vol 6, issues 79, Pp 3907-3915.
17. Mrs. Rashmi Soni "Digital Watermarking of Wavelet Transforms Based on Coding and Decoding Techniques", IJCSMC, Vol. 3, Issue. 3, pg.1045 – 1051, March 2014
18. A. Agrawal (2014). Securing Video Data: A Critical Review, .International Journal of Advanced Research in Computer and Communication Engineering, Vol:3, Issue:5).
19. Mc Kevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing,Vol:90, Issue:3, pp 727-752.
20. Al-Shatnawi (2012). A new method in image steganography with improved image quality. Applied Mathematical Sciences, Vol:6, Issue:79, pp 3907-3915.
21. Deshpande, N (2014). Robust Dual Watermarking Scheme for Video Derived From Strategy Fusion. International Journal Of Image, Graphics And Signal Processing (IJIGSP), 6(5), 19