ENHANCEMENT IN SECURITY USING HASH-SECC STEGNO-CRYPTO FOR SECURE COMMUNICATION

Ankit Sharma[1]
Parag Rastogi[2],
Department of computer science& Technology
Subharti Institute of Technology & Engineering

ABSTRACT

The Cryptology is the learning of techniques for ensuring the privacy and verification of the data. PKE systems are safe only if the validity of the public-key is guaranteed. ECA (elliptic curve arithmetic) is used to grow a diversity of ECC systems plus key altercation, encryption and decryption. Secure hash based Elliptic curve DNA (**HASH-SECC**) that overcome the problem of Euler totient function based, fix key for prime number measurement analogous matrix based ASCII values of the plain text that presence proposed that overcomes the difficulties of Diffie-Hellman and RSA. The paired values describe as input for hash key in the Elliptic curve cryptography. Thus in this work also show that a comparison of existing work and our proposed technique which is simulated in MATLAB-2014Ra tool.

Keywords: Elliptic Curve, Cryptography, Network Security, Wireless Technology, Wireless Communication

I. INTRODUCTION

1.1 Background

Internet brings different ways for helping end user, it also brings risk associated with it. Making payment online, sending secure information over the web, using passwords and user ids for secure access are such deleterious works [1]. Therefore using these two techniques, cryptography and steganography together provides two level of security [3]. From many years a lot of research has been done to contrive new techniques and applications for encoding and decoding of data to be transferred. These algorithms can be enhanced by using DNA based computing method which provides better data security [4]. With the development of modern cryptographic techniques, users are assured of the below four security attributes namely:

i. Integrity
ii. Confidentiality
iii. Availability
iv. Authenticity

1.2 Cryptography

While transmitting the data, users of communication system find an inherent need to:

(1) Communicate and share information with the people and

(2) Selectively Communicating.

The encryption and decryption process is based on the mechanism of cryptography method and key being used. The process of encryption and decryption is written as:

$$C_T = E_k(P_T) P_T = D_k(C_T)$$

Where

$\mathbf{P_T}$ = plaintext to be transmitted

$\mathbf{C_T}$ = converted ciphertext

E = encryption mechanism used

D = decryption mechanism used, which is generally opposite of encryption method.

k = shared key.

1.2. Classification of Cryptography

Cryptography is divided into two main branches:

- **Symmetric cryptography**

The identical key must be used while encrypting the message and decryption of the message otherwise at recipient side it will be difficult to transform ciphertext back to plaintext message. The key is a shared secret between two or more parties who want to communicate secretly over the channel.

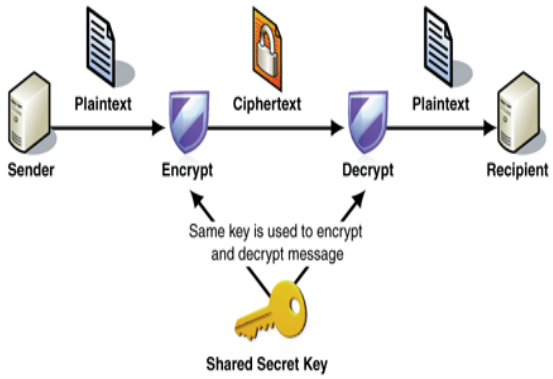


Figure 1.3:Symmetric-key cryptography

Symmetric-key cryptography has limitation that the secret key is known to both of the parties and shared secretly which became the reason for popularity of public-key encryption. Some popular examples of Symmetric-key cryptographic system are Substitution Cipher, Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, 3-DES , IDEA.

The elliptic curve is symmetric with respect to the *x*-axis i.e.

$$y_i = \sqrt{x_i^3} + a \cdot x_i + b \quad (1.4)$$

$$y_i = -\sqrt{x_i^3 i} + a \cdot x_i + b \quad (1.5)$$

both are solutions.

In order to build a strong EC, we have to find a curve equation such that:

1. Curve with a large cyclic group which means curve equation has set of elements.
2. group operation with those points

1.3. Group Operations on Elliptic Curves

A. Point Addition

Addition in Elliptic curve is, given two points on curve and their coordinates finding third point C such
A+B = C (1.6)

(x1,y1) be the coordinates of A

(x2,y2) be the coordinates of B

(x3,y3) be the coordinates of C

In case of point addition we assume that A is not equal to B. While computing point C, we will draw a line through points A and B. The resultant point C after addition will be obtained at the intersection of the elliptic curve and the line through points A and B. The mirror image of the third point C along the x-axis will be the result of addition [28].

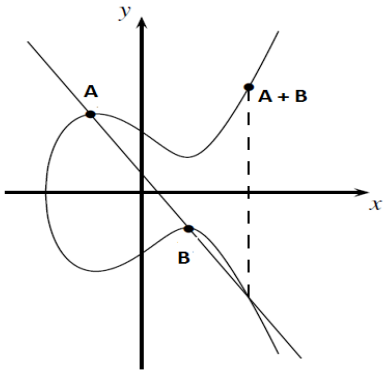


Figure 1.5: point addition over the real numbers on an elliptic curve

Above figure shows the point addition over the real numbers on an elliptic curve.

1.2 STEGANOGRAPHY

Text Steganography

Data hiding in text steganography is done by making changes in the construct of the text document without making significant changes in the output. In Text steganography one text file is hidden into another text for the secure communication.

Random and statistical generation methods:

Least Significant Bit based Steganography

Let's take an example of 24- bit image data is hidden in RGB (3 bits) of each pixel by modifying least significant bit of red, green and blue colour components of the image. The RGB component represents a byte. Let's say we want to hide letter 'A' in the first eight bytes of three pixels. In pixel terms the value of RGB will consists of either 0 or 1. The original raster data for 3 pixels may be

R	G	B
01100110	11001010	10001010
11100101	11011010	10101011
11101010	00101101	11100011

Letter to hide, A with ASCII value 065 and binary value-01010011

Hiding character 'A' into the LSBs will result as:

R	G	B
01100110	1100101**1**	10001010
11100101	11011010	1010101**0**
11101010	00101101	11100011

To hide letter A, we just have to manipulate two underlined bits. In general LSB substitution only few bits get changed. Manipulating the values of the MSBs will cause a detectable impact on the image colour but modifying the LSB value will not be detectable and preserves the quality of image. Therefore, 11111010 could be changed to 11111011 or remains unchanged would go undetectable to the casual reader. Only last bits of the RGB value are used to embed data. This means that one set of value of zeroes and ones are exchanged with another set of zeroes and ones.

II. LITERATURE REVIEW

Ushl et al. in [4] proposed an encrypting technique which combines cryptography and steganography for data hiding. The message is encrypted two times for providing data security. The cipher text is hidden inside the image. It makes use of a reference matrix in order to select passwords depending on the image properties.

Bharti and Soni [5] proposed a novel scheme to embed data in color images. This method shows its larger capacity for hiding data than other methods without loss of imperceptibility integer wavelet transform and Genetic algorithm. The method is very efficient, especially when applied to those images whose pixels are scattered homogeneously and for small data. Watada in [5], illustrate the current state of the art of DNA computing achievements and also explain new approaches or methods contributing to solve either theoretical or application problems.
Catherine Taylor [6]suggested an indication in which data is programmed into DNA elements, and then transformed into microdots. A microdot is an extremely reduced photograph of a typewritten page. Industrialized DNA based particularly steganographic technique. First done DNA encryption and before reduced it to a microdot. Simple substitution cipher is used for encryption. Because of the vast prospects of DNA nucleotides, it performances as a complex background for storage secret message. Arbitrary key is used for encryption.

Xing Wang in [7] applied computing theories in cryptography which will solve many hard problems successfully. He proposes a new way to use Cryptography with DNA Computing to transmit message securely and effectively. The RSA algorithm combined with DNA computing technique to encrypt and decrypt the message which requires more key size for providing same level of security as ECC.

Guozhen Xiao, Mingxin Lu, Lei Qin and XuejiaLai in [8], uses DNA or other biological macromolecules as computing hardware. It examines the possibilities of DNA computing and opens up the general molecular computation and achieves the problems faced by DNA computing technique.

Guangzhao Cui in [9] can realize several security technologies such as encryption, Steganography, signature and authentication by using DNA molecular as information medium. He introduces the basic idea of DNA computing, and then discusses the information security technology in DNA computing.

R.Poornima et al, [10]This paper is proposed that the hiding capacity for the important concern of data hiding or steganography. Steganography is a method which hides the data behind the image or audio, video etc. In this method that the original data can't be noticeable to the user. Only receiver can decrypt the data. Several methods for steganography are like audio, video, text or image.

III. SYSTEM MODEL

3.1. ECC Method

Elliptic Curve Cryptography is a PKC. In PKC every operator or the scheme enchanting portion in the safe message essentially have a couple of keys, a public key and a private key, and a set of processes related to keys which used cryptographic procedures for communication.

3.2 Elliptic Curve and Hyper elliptic Curve Cryptography proof

Normally in the procedure of cryptography, user have two objects, one side is and second size decryption. Supposing that Alice is the encryption side who is encoding and Bob is the other side who decoded text.

3.3. Mathematical derivation

Description: Assume x is smooth, geometrically linked, leading curve in excess of an area k, of type $g \geq 1$. x is a hyperelliptic curve if here occurs a finite discrete morphism $X \longrightarrow P^{1}{}_{k}$ of grade 2.

Proposal: Suppose x is a hyperelliptic arc of type g ended an area. Formerly k(x) = k(t)[y] by a relative

$$Y^2 + Q(t)\,y = P(t)\,P(t),\ Q(t) \in k[t]$$

$$\text{and } \deg Q(t) \le g+1,\ 2g+1 \le \deg P(t) \le 2g+2$$

For cryptography usages individual the arcs with degree Q (t) ≤ g & deg P (t) = 2g + 1 are dignified. They have simply one opinion at eternity.

As for any arc, It will assign to a hyperelliptic arc its Jacobian diversity, That an abelian diversity J of dimension of g like J(K) ~= Pic0 (XK) for some delay K/k checking X(K) ≠ ∅. It drives available that the plot sure in Proposal 3 is in overall individual injective.

It assembly instruction on behalf of J (F_q) is almost q g , through a consequence of Weil.

$$(\sqrt{q}-1)^{2g} \le |J(\mathbb{F}_q)| \le (\sqrt{q}+1)^{2g}.$$

It resources it is equivalent extent as unique acquires in ECC occupied ended the addition area Fq g. In addition, if g is huge, one cans exertion completed a minor ground.

3.4 PROPOSED hECCS METHOD

HECC-HASH hash purpose changes a big and variable-sized quantity of DNA information addicted to a single number value in instruction to be help for numerous bio informatics examines. The proposed ECCSH-DNA for repetitive sequence exploration motif exploration, segment-based arrangements and database applications. A relative speed investigation accompanied alongside other three hashing functions, MD5, SHA1 and SHA256, presented considerable qualities of ECCSH-DNA technique, specifically the speed and the output size.

3.5. Sender Side Algorithm

The secret text file is encrypted by ECCSH encryption algorithm by the help of secret key at the sender's side. Then the encrypted text is surrounded into a cover image by DNA algorithm and it can produce the stego image.
The following steps are followed at sender side; the result of below steps is a stegoimage:

Step 1 Get the cover image.

Step 2 Get texts which need to be securely transmitted.

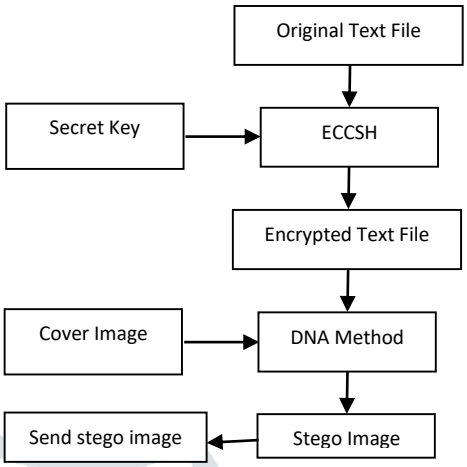
Step 3 Encrypt text message using HECCSH points using Koblitz method.

Step 4 Hide data into file.

Step 5 Convert stego image into DNA nucleotide.

Step 6. Convert DNA nucleotide into binary digits.

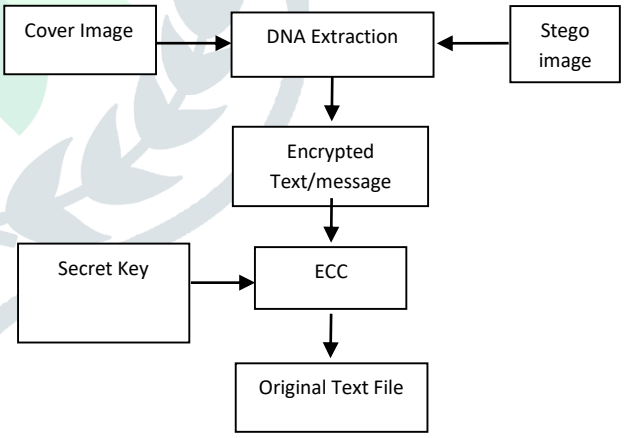
Step 7. Send stego image using email



3.6. Receiver Side Algorithm:

First step is to extract the encrypted text file from the stego image received using SMTP. The extracted secret text/message is decrypted by the HECC algorithm with the shared secret key and the original text is then produced.

Below are the steps followed at receiver side to decrypt the original message:



Step 1 Get the stego image.

Step 2 Compute the XOR operation using cover image.

Step 3 Convert the resultant binary digits into the DNA nucleotide.

Step 4. Convert DNA nucleotide into alphabets.

Step 5 Recover the original message

Koblitz's Method for Encoding the Message:

- Select an elliptic curve C.
- Let us say Elliptic Curve C has N points, denoted

as (x1,y1),(x2 ,y2),(x3,y3)..(xn ,yn).

- Let us say message m consist of numbers from 0,1,2..9 and alphabets A,B,C…Z coded as 0,1,2,3…35
- Select an assisting base parameter k = 20.
- For each digit in message, mk (say), take x =mk + 1 and try to solve for y.
- If not capable to resolve for x= mk+1, then try x = mk +2, x = mk +3, x = mk +4 until y value is gained.
- In preparation we will be able to compute for y before we hit x=mk+1.
- Resultant value of x and y is the point (x,y) which corresponds to digit m.
- By repeating above steps we will be able to decode entire message in sequence of points.

Koblitz's Method for Decoding the Message:

- For each point on the curve, set the worth of m as the greatest integer less than (x-1)/k.
- By repeating above step all the points are converted back to the message.

IV. RESULTS AND DISCUSSIONS

The Elliptic curve cryptography is a cryptography method which considers PKC (public key cryptography) on the arithmetical construction of elliptic curves that completed finite grounds [6].

The proposed method is tested on different sets of cover images as well as messages. The best suited type of image for DNA steganography is png or bmp file because both type of image uses lossless compression. While applying DNA Steganography data will not be lost. Below shows the result of proposed approach:

Enter 1 for TEXT Message:1

27	27	33	40	46	44	41	39	37	35	34	34	32	28	24	24	24	22	19	17
26	30	39	47	51	51	47	46	41	42	39	35	34	32	31	31	27	25	20	18
20	25	35	40	45	44	44	42	39	40	35	32	31	31	30	30	28	26	20	17
17	25	37	40	44	44	42	40	39	37	33	31	31	31	31	32	31	28	23	18
15	20	32	39	42	41	39	38	34	32	27	27	27	30	31	31	28	26	19	16
11	15	22	26	27	27	27	26	26	24	19	19	25	26	27	27	24	20	18	16
8	9	11	11	12	13	13	13	17	16	13	15	18	17	17	17	17	15	13	10
5	5	6	6	9	9	10	10	8	6	10	12	13	12	12	12	11	11	10	10
2	3	5	8	9	8	9	9	5	4	9	11	10	9	9	8	9	11	10	9
4	5	6	6	9	9	10	9	5	6	9	9	9	9	9	9	10	9	8	

Fig 4:1 Matrix generation of input image

This test is performed as to show the level of separate sub-matrices of the whole image order. The purpose of above experimental result is to show the direct requirement between fixed size substrings of the authentic order.

Please Enter an Encryption Key Between 0 - 255: 10

Enter 1 for Encrypted Text Embedding 1

n=15 phi(15) is 8

Public key is (7,15)

Private key is (7,15)

ASCII equivalent MSE by using ECC

7.0493

ASCII equivalent MSE by using PRECC

5.4948

Accuracy using PRECC

77.7224

The encrypted message is 9 9 7 9

The decrypted message in ASCII is 41 45 41

The decrypted message is:

Enter File Name for Image + Message: a.png+msg.txt

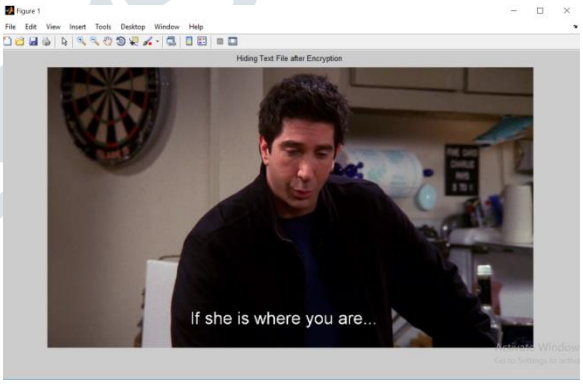


Fig 4.2: Sender image

Fig 4.3: Confirmation of email of Sender image

Welcome to the Stegano-Crypto Program

Enter 2 for Extraction:2

Please Enter an Encryption Key between 0 - 255:10

Enter 1 for ECCSH-DNA for Extraction:1

Enter File Name for File + Message:

a.png+msg.txt

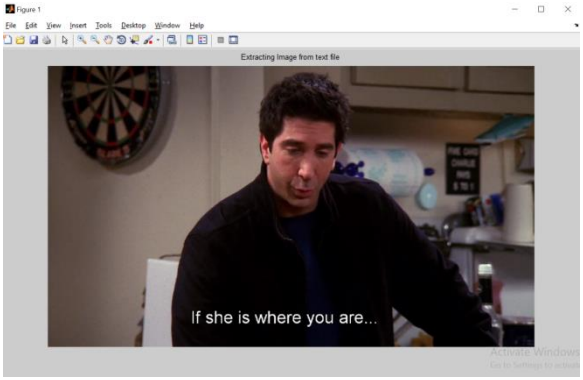


Fig 4.5: After receiver/decryption image

Extracted Message with decryption

we are working for mtech thesis

xyz

Extraction Elapsed time is : 0.111962 seconds.

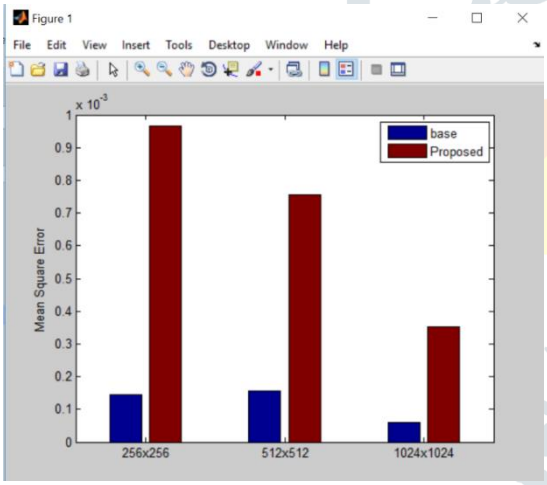


Fig 4.6: Comparison of Mean Square Error

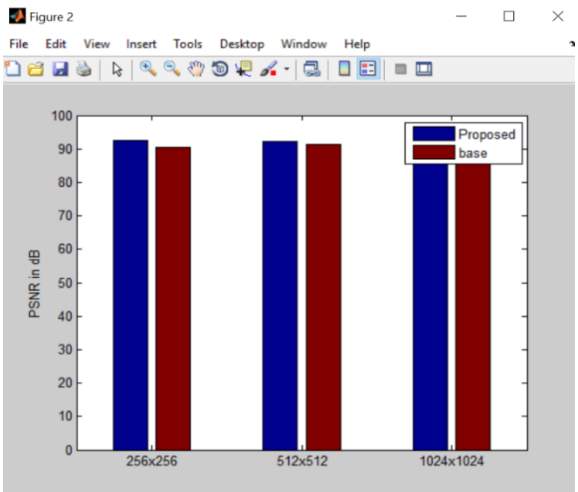


Fig 4.7: Comparison of Peak Signal to Noise Ratio

To compare the relative performance of ECC and DNA-ECC, it is discovered that genus of hybrid DNA-ECC is much faster in comparison with ECC. Hybrid computing method of DNA-ECC proved to be better than ECC in restricted environment because of its short operant size.

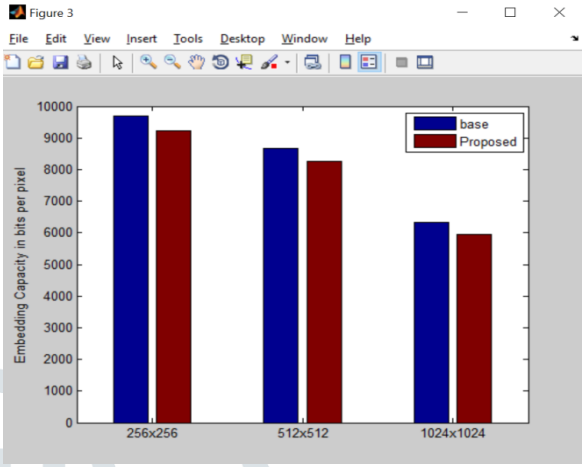


Fig 4.8: Embedding Capacity

Furthermore it has been proven before that to attain cryptology safety corresponding to the security providing through elliptic curve completed a area size log q, it is important to opt for a hyperelliptic curve over a field smaller than log q.

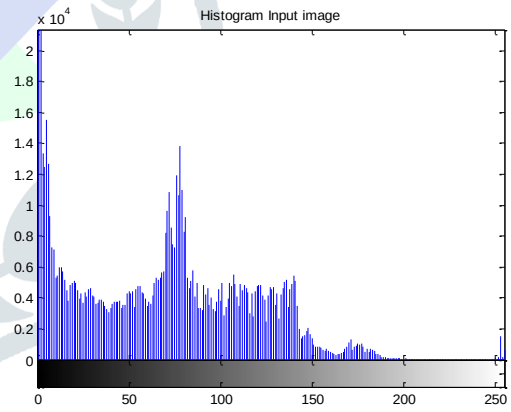


Fig 4.9: Histogram input image of sender part

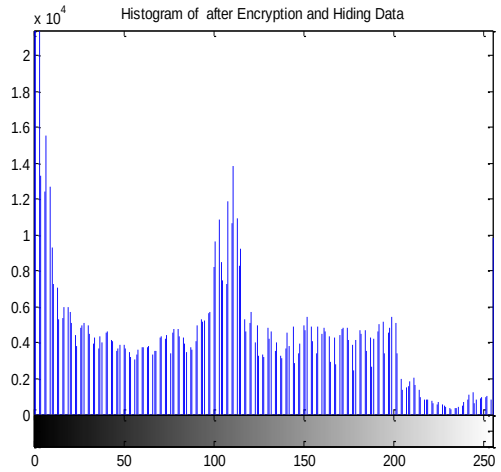


Fig 4.10: Histogram of after encryption and hiding data gram of receiver side

V. CONCLUSION

Elliptic and hyper elliptic curves are public key cryptographic protocols created on discrete logarithm problem. In this work we have conducted a study on DNA-ECCSH based primitives in the field of cryptography as with steganography with security and block based image matrix phase cryptographic primitives which have been designed based on elliptic curve. Using our proposed approach it is proved to be easy and secure way to transfer information over simple mail transfer protocol. The HECCSH data is encrypted using HECC and is embedded in the image using DNA Steganography to send through e-mail system over secure socket layer (SSL). It is proved to be dependable and safe method. At the receiver side, the application forms the obtainability of information and validates it. HECCSH recovers data after the stego image and decrypts it with minimizing overall processing time and computational complexity.

REFERENCE

[1] Amritpal Singh, "An Improved LSB based Image Steganography Technique for RGB Images", Electrical,Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on. IEEE, 2015.,pp 1-4

[2] Mehdi Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Vol. 54, May, 2013, pp 113-124

[3] T. Morkel, "AN OVERVIEW OF IMAGE STEGANOGRAPHY", ISSA. 2005, pp 1-11

[4] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, 0Computer Science and Network Technology (ICCSNT), International Conference,pp. 1017-1020.IEEE. 0 10000 20000 30000 40000 50000 Gray True color LSB Proposed Applied Computational Science ISBN: 978-960-474-368-1 133, Vol.2, No.2.11, 2011

[5] Bharti,P.,andSoni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography,InternationalJournalof Computer Applications,Vol.58,No.18,pp1-5,2012.

[6] Catherine Taylor Clelland. Hiding Messages in DNA Microdots. Nature, 399:533–534, June 1999.

[7] Xing Wang and Qiang Zhang, "DNA computing-based cryptography", in the IEEE proceeding of BIC-TA '09. Fourth International Conference on Bio-Inspired Computing, Page(s): 1 - 3 , Oct. 2009

[8] Guozhen Xiao, Mingxin Lu, Lei Qin and XuejiaLai , "New field of cryptography: DNA cryptography", in the Journal on Chinese Science Bulletin , vol.51, Issue 12 , pp.1413-1420, June 2006.

[9] Guangzhao Cui, Cuiling Li, Haobin Li and Xiaoguang Li, "DNA Computing and Its Application to Information Security Field", in the IEEE proceedings of Fifth International Conference on Natural Computation, pp.148-152, June 2007.

[10] R.Poornima, "AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY", (IJCSES) Vol.4, No.1,February 2013, pp 23-31

[11] Anil Kumar, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", IJARCSSE, Volume 3, Issue 7, July 2013, pp 363-372

[12] ShavetaMahajan, "A Review of Methods and Approach for Secure Stegnography", IJARCSSE, Volume 2, Issue 10, October 2012, pp 67-70

[13] JasleenKour, "Steganography Techniques –A Review Paper", International Journal of Emerging Research inn Management &Technology, Volume-3, Issue-5, May 2014, pp 132-135

[14] Andre Leier. Cryptography with DNA Binary Strands. BioSystems, 57:13–22, April 2000.

[15] Jie Chen. A dna-based, biomolecular cryptography design. In Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on, volume 3, pages III–822–III–825 vol.3, May 2003

[16] Pak Chung Wong. Organic Data Memory using DNA Approach. In Communications of the ACM, volume 46, pages 95–98, January 2000.

[17] M. Borda and O. Tornea. Dna secret writing techniques. In Communications (COMM), 2010 8th International Conference on,, pages 451–456, June 2010.

[18] Qiang Zhang. Image encryption using dna addition combining with chaotic maps. Elsevier, Mathematical and Computer Modelling, 52(1112):2028 – 2035, 2010. The BIC-TA 2009 Special IssueInternational Conference on Bio-Inspired Computing: Theory and Applications.

[19] D. Kumar and S. Singh. Secret data writing using dna sequences. In Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on,, pages 402–405, April 2011.

[20] Khalifa and A. Atito. High-capacity dna-based steganography. In Informatics and Systems (INFOS), 2012 8th International Conference on,, pages BIO–76– BIO– 80, May 2012.

[21]M. Shyamasree and S. Anees. Highly secure dna-based audio steganography. In Recent Trends in Information Technology (ICRTIT), 2013 International Conference on,, pages 519–524, July 2013.