Indian Journal of Science and Technology, Vol 9(10), DOI: 10.17485/ijst/2016/v9i10/88987, March 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

# A Hybrid Multilevel Security Scheme using DNA Computing based Color Code and Elliptic Curve Cryptography

**P. Vijayakumar[1*], S. Indupriya[1] and R. Rajashree[2]**

[1]School of Electronics Engineeirng, VIT University Chennai – 600048, Tamil Nadu, India; vijayrgcet@gmail.com, s.indupriya2014@vit.ac.in
[2]ECE, GKM College of Engineering and Technology, Chennai - 600 063, Tamil Nadu, India; rajashree.ece@gmail.com

## Abstract

**Background/Objectives:** The terrorism threat caused by terrorist who posses forged passport and identities due to insecure environment which could be more serious imminent. Traditional scheme and techniques available to protect the information from unauthorized user is not enough for the current environment. **Methods/Statistical Analysis:** So, a hybrid multilevel DNA computing based Color Code Cryptographic scheme combined with Elliptic Curve Cryptography is proposed to protect the passport data from the eavesdropper. Proposed data encryption algorithm consists of two level of security, first level of security is provided by convert the personal details (Plain Text) of the customer into Unicode and RGB color code and then map the color code with DNA nucleotide. The mapped DNA molecules converted into ASCII values for encryption process. DNA molecules help to store enormous amount of data intended to allow more number of user to access the system. Second level of security is provided by encrypt the ASCII values using Elliptic Curve Cryptography techniques which require very less key size compared with traditional schemes. Resultant Cipher Text is hidden in the personal image of the customer using LSB steganographic method. **Findings:** Compared with traditional scheme, proposed scheme provides multilevel of security with less communication and computational overhead due to its lesser key size. ECC-80 bit key size based encryption scheme provides same level of security as RSA-1024 scheme with less number of operations involved in the passport verification system. **Applications/Improvements:** Since the proposed scheme require very less key size, consumes very less power, it will be more suitable for power constrained devices such as smart card, sensors, mobile phones, PDA's, RFID tags, etc.,

**Keywords:** ASCII Values, Color Code Cryptography, DNA Cryptography, Elliptic Curve Cryptography, Steganography, Unicode

## 1. Introduction

Cryptography means hiding information's and it is the study of techniques for secure communication in the presence of third parties. Cryptography is not only about encrypting and decrypting messages; it is also about solving real world problems that require information security. It is analyzed by various aspects in security information like authentication, confidentiality, data integrity and non-repudiation. A new cryptographic scheme proposed for securing color image based on color code cryptography scheme. A color image to be protected and a compression of the colors can be used as key to encrypt and decrypt the original data. DNA Cryptography is defined as hiding the data in terms of DNA Sequence. DNA can be used to store and transmit data. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new hope for unbreakable algorithm. Strands of DNA are long polymers of millions of linked nucleotides.

*Author for correspondence

The nucleotides that make up these polymers are named after the nitrogen base that it consists of Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). Elliptic Curve Cryptography is one of the famous public key cryptographic technique was independently proposed by Miller and Koblitz in 1985. It uses elliptic curve where variables and coefficient are bounded to elements of finite field. These researchers puts enormous amount of work to offer same level of security with lesser key size compared with existing methods which are based on difficulties of solving discrete logarithm problem over integers or integer factorization. Armstrong number is used for message encryption and color code act as password for authentication process[1–4].

Improved ECC algorithm is designed to be more challenging as the repetitive characters of the text are replaced with the different cipher text in each of the iteration and outperforms the standard ECC in terms of cipher text, encryption, decryption time and security. This algorithm helps to assure end to end encryption for Online Social Network (OSN) users[5]. A secure data hiding technique for video images using random key encoding function. Secret data are embedded into the random Red Green Blue (RGB) pixel values of the cover-video images using an encryption key. The cover-video images are pre-processed to prevent overflow/underflow. Experimental results indicate that the extracted data are without any errors. The performance of the proposed scheme is proved in terms of security and (Peak Signal Noise Ratio) PSNR values[6]. A new promised steganographic algorithm[7] is proposed for Arabic text based on features of Arabic text. The main focus of the algorithm is secure and high capacity of the carrier media. The embedding capacity rate ratio of the proposed algorithm is high. In addition, the proposed algorithm can resist traditional attacking methods since it makes the changes in carrier text as minimum as possible. A bit level key agreement and secured key exchange protocol is introduced for the digital image steganographic applications. This protocol is constructed with the help of simple binary arithmetic and the XOR operation, mostly suitable for digital image steganographic algorithms[8]. A new data hiding approach using Pixel Value Difference (PVD)[9] steganography is proposed for digital image. PVD steganography, proposed by Wu and Tsai, use non-overlapping block of two pixels to find the edge areas to hide secret message by adjusting the pixel pairs. In PVD method only the edge between two pixels within a block is detected.

This paper is organized as follows: This section deals with basic introductions about Cryptography, DNA cryptography, color code cryptography and Elliptic Curve Cryptography. Section 2 provides the traditional security scheme using RSA algorithm. Section 3 gives the proposed Hybrid Multilevel Security Scheme using DNA Computing based Color Code and Elliptic Curve Cryptography. Chapter 4 shows the simulation results and security analysis. Finally conclude the paper.

## 2. Traditional Passport Anti-Forgery System using RSA Algorithm

Encryption of data for a passport anti-forgery system based on the public key signature scheme using RSA algorithm[10]. RSA algorithm gives a multilevel security for data transformation process. The complexity of the computation required for RSA algorithm is mainly based on time taken to execute RSA key generation, encryption and decryption algorithms. Security of RSA is analyzed by taking brute force, mathematical, timing and chosen cipher text attacks into consideration. Attacks on RSA can be overcome by increasing the key size 'd' but this makes the key generation process more complex and time consuming. This increases the storage requirement and also increases the simulation time of the encryption and decryption algorithms.

## 3. Proposed Hybrid Multilevel Security Scheme using DNA Computing based Color Code and Elliptic Curve Cryptography

In order to overcome the limitations in existing method, ECC algorithm is used with DNA cryptography and color code cryptography. ECC algorithm is modular addition and requires shorter key length to perform encryption and decryption operation than RSA algorithms. The passport verification is done by matching the details provided by the individual with the details enrolled in the database. This system extends the privacy to the image as well as the personal information that are shown in Figure 1. Passport details and personal image of the person is given to the system that is processed and sends to the client and server.

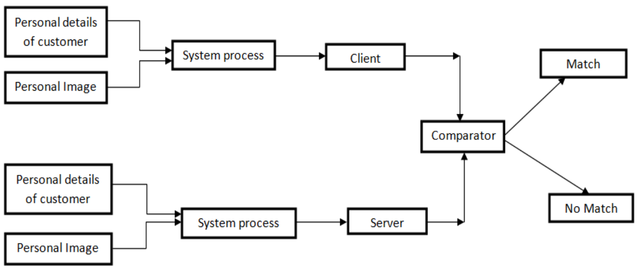


**Figure 1.** Block diagram for passport verification system.

Save all the information's from in server at that time a person show his passport for verification. Comparator check the client details of the person from data stored in the server, both of them are compared after the system shows if it is matched or not matched. This is the overall process of the passport verification system.

- The plain text is converted into cipher text the encrypted data is then hidden in an image using LSB algorithm.
- This input private image is now decomposed into two independent sheet images that are stored in two different database servers.
- The reconstructed private image is performed by overlapping the two shared images available in the database and extracted by decryption of cipher text into plain text.
- The following steps provide a high level security for passport verification system.

Plaintext Pm includes all the passport details (Customer name, Passport No, Issue date, Issue place) are converted into UNICODE that is mapped with RGB color for every letter. RGB color is converted into binary codes then the codes mapped with DNA Nucleotide. Write the ASCII values for DNA sequence and those values are converted into plain text points using Koblitz method. Plain text points are again converted into Cipher text points using a Private key, Cipher text points is send to the embedding algorithm. At the same time Personal Image (PI) is also sent to the embedding algorithm; both points and image are combined to form the Stego Image (SI). Finally the Stego Image is send to the server as shown in Figure 2. The following steps are followed to obtain cipher text.

**Step 1:** Take Personal Information (PI) as plain text**.**
Example: Personal details

- Customer Name: Priya Selvam.
- Passport No: 325461.

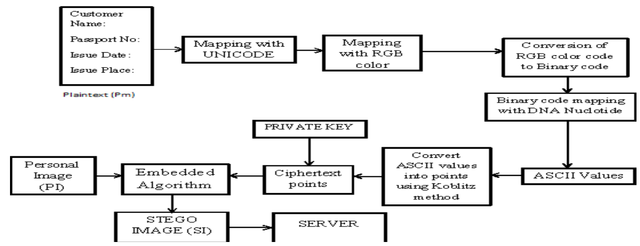


**Figure 2.** Block diagram of encryption process.

- Issue date: 09/10/2015.
- Issue Place: Chennai.
    - First letter of plain text is 'P'

**Step 2:** Convert plaintext into UNICODE by using Table 1.
Example : P = U + 0050.

**Step 3:** UNICODE is converted into RGB color code using Table 2 and write the hexadecimal value of the color model**.**
Example: U + 0050 = Blue = 0000FF.

**Step 4:** Convert the hexadecimal value into binary codes**.**
Example: 0000FF = 0000 0000 0000 0000 1111 1111.

**Step 5:** Binary code is then taken as DNA sequence using DNA cryptography as shown in Table 3.
Example: 0000 0000 0000 0000 1111 1111 = AA AAAAAA TT TT.

**Step 6:** Convert DNA sequence into ASCII values.
Example: AA AAAAAATTTT = 65 65 65 65 65 65 65 84 84 84 84.

**Step 7:** Using Koblitz method, the ASCII values are converted into plaintext points.
Example: A = 65 → m = 65.

Step to be followed to convert ASCII value into ECC points is shown below:

- x = mk + 1
- Assume K = 20, P = 751, (a,b) = (-1, 188)
- X = 65 $^*$ 20 + 1= 1301
- 1301 mod p → 1301 mod 751
- X = 550, Y = 38.4
- Y~= 38
- 1474 mod 751 = 723
- Y2 mod 751 = ( x2 + ax + b) mod 751
  = [(550)2 + (-1)(65) + 188) mod 751
  = ( 302500 + (-65) + 188) mod 751
  = 302623 mod 751 = 721

Plain text points of (x, y) = (550, 38)

**Table 1.** Plain text into UNICODE

| Alphabets and numbers | UNICODE values |
|---|---|
| A | U+0041 |
| B | U+0042 |
| C | U+0043 |
| D | U+0044 |
| E | U+0045 |
| F | U+0046 |
| G | U+0047 |
| H | U+0048 |
| I | U+0049 |
| J | U+004A |
| K | U+004B |
| L | U+004C |
| M | U+004D |
| N | U+004E |
| O | U+004F |
| P | U+0050 |
| Q | U+0051 |
| R | U+0052 |
| S | U+0053 |
| T | U+0054 |
| U | U+0055 |
| V | U+0056 |
| W | U+0057 |
| X | U+0058 |
| Y | U+0059 |
| Z | U+005A |
| 0 | U+0030 |
| 1 | U+0031 |
| 2 | U+0032 |
| 3 | U+0033 |
| 4 | U+0034 |
| 5 | U+0035 |
| 6 | U+0036 |
| 7 | U+0037 |
| 8 | U+0038 |
| 9 | U+0039 |

Now the ASCII values are converted into Plain text points by using ECC based Koblitz method with the help of private key.

**Step 8:** Plain text points are converted into Cipher text points with the help of Private Key.

**Table 2.** Color code into Hexadecimal values

| Color | HTML / CSS Name | Hex Code #RRGGBB | Decimal Code (R,G,B) |
|---|---|---|---|
| | Black | #000000 | (0,0,0) |
| | White | #FFFFFF | (255,255,255) |
| | Red | #FF0000 | (255,0,0) |
| | Lime | #00FF00 | (0,255,0) |
| | Blue | #0000FF | (0,0,255) |
| | Yellow | #FFFF00 | (255,255,0) |
| | Cyan / Aqua | #00FFFF | (0,255,255) |
| | Magenta / Fuchsia | #FF00FF | (255,0,255) |
| | Silver | #C0C0C0 | (192,192,192) |
| | Gray | #808080 | (128,128,128) |
| | Maroon | #800000 | (128,0,0) |
| | Olive | #808000 | (128,128,0) |
| | Green | #008000 | (0,128,0) |
| | Purple | #800080 | (128,0,128) |
| | Teal | #008080 | (0,128,128) |
| | Navy | #000080 | (0,0,128) |

**Table 3.** Binary mapping with DNA sequence

| Binary Value | DNA Digital Coding |
|---|---|
| 00 | A |
| 01 | C |
| 10 | G |
| 11 | T |

Example:

- Plain text Value of (x, y) is (550, 38)
- Cipher text formula**:**
  - Cm = { K.G, Pm + k . PB }
- Private key K = 3
  - Public key Q = K . G = 3 * (550, 38)
- Formula for multiplication is
  - Key * (x, y) = (x1, y1) + (x2, y2) + (x3, y3)
- Repeated Addition
  - Eg: (x1, y1) (x2, y2)
  - x1 = Xp; x2 = Xq; y1 = Yq; y2 = Yq
  - Xr = λ2 + λ + a
  - Yr = x2 + (λ + xr)
  - λ = xp + (yp/xp)
- The value of (x1. y1) and (x2, y2) = (303051, 60699)

- Then the value of (303051,60699) and (x3, y3) = (918399, 918411)
  - Assume p = 23, a, b = 1, x = 5
  - $Y^2$ mod p = ($x^2$ + ax + b) mod p
  - $Y^2$ mod 23 = ($5^3$ + 5 + 1) mod 23=(125 + 5 + 1) mod 2
    = 131 mod 23= 16
  - Let us take y = 4 then(4) $^2$ mod 23 = 16
- 16 mod 23 = 16
- G = (5, 4)
  - Cm = {K .G, Pm + k. PB }
    = {(2071, 3965), (550, 38) + 3 * (nB * G)
    = {(2071, 3965), (550, 38) + 3 * (1 * (5, 4))}
    = {(2071, 3965), (550, 38) + 3 * (5, 4)}
    = {(2071, 3965), (550, 38) + (2071, 3965)
  - Cm = {(2071, 3965), (303051, 606101)}

**Step 9:** LSB Steganography.

Cipher text point and image is combined to get Stego image by embedding them with the help of LSB algorithm and that Stego image is sent to the server as shown in Figure 3. The following steps are followed to hide the cipher text point into the personal image.

- Cipher text Cm = {(2071, 3965), (303051, 606101)}
  - Convert the cipher text values into binary form.
    2071 = 0010 0000 0111 0001
    3965 = 0011 1001 0110 0101
    303051 = 0011 0000 0011 0000 0101 0001
    606101 = 0110 0000 0110 0001 0000 0001
- Take 16 * 16 matrix from Personal Image.
  [2 1 4 6 8 5 3 1    2 1 4 6 8 5 3 1
  5 8 2 4 6 1 5 2    5 8 2 4 6 1 5 2
  3 2 1 8 1 2 7 9    3 2 1 8 1 2 7 9
  0 9 5 4 8 9 6 7    0 9 5 4 8 9 6 7
  4 7 9 7 5 6 4 3    4 7 9 7 5 6 4 3
  7 5 2 1 9 8 7 5    7 5 2 1 9 8 7 5
  2 6 5 9 6 3 8 4    2 6 5 9 6 3 8 4
  1 4 0 5 9 6 5 9    1 4 0 5 9 6 5 9]
- Convert the matrix into binary form.
  [0010 0001 0100 0110 1000 0100 0011 0001 0010 0001 0100 0110 1000 0100 001 10001
  0100 1000 0010 0100 0110 0001 0101 0010 0100 1000 0010 0100 0110 0001 0101 0010
  0011 0010 0001 1000 0001 0010 0111 1001 0011 0010 0001 1000 0001 0010 0111 1001
  0000 1001 0101 0100 1000 1001 0110 0111 0000 1001 0101 0100 1000 1001 0110 0111
  0100 0111 1001 0111 0101 0110 0100 0011 0100 0111 1001 0111 0101 0110 0100 0011
  0111 0101 0010 0001 1001 1000 0111 0101 0111 0101 0010 0001 1001 1000 0111 0101
  0010 0110 0101 1001 0110 0011 1000 0100 0010 0110 0101 1001 0110 0011 1000 0100
  0001 0100 0000 0101 1001 0110 0101 1000 0001 0100 0000 0101 1001 0110 0101 1000]
- Enter the cipher text value in LSB of the matrix.
- Cipher text values are:
  2071 = 0010 0000 0111 0001
  3965 = 0011 1001 0110 0101
  303051 = 0011 0000 0011 0000 0101 0001
  606101 = 0110 0000 0110 0001 0000 0001
- Encrypted matrix for P:
  [1011 0000 1100 0111 1000 0100 0010 0001 1011 0000 1100 0111 1000 0100 0010 0001
  0101 1000 0010 0100 0110 0000 0101 0011 0101 1000 0010 0100 0110 0000 0101 0011
  1011 0010 0000 1001 0001 0010 0110 1001 1011 0010 0000 1001 0001 0010 0110 1001
  0001 1000 0100 0101 1000 1000 0110 0111 0001 1000 0100 0101 1000 1000 0110 0111
  0101 0110 1000 0110 0100 0111 0100 0010 0101 0110 1000 0110 0100 0111 0100 0010
  0110 0100 0010 0001 1000 1000 0110 0101 0110 0100 0010 0001 1000 1000 0110 0101
  0010 0110 0101 1001 0110 0011 1000 0100 0010 0110 0101 1001 0110 0011 1000 0100
  0001 0100 0000 0101 1001 0110 0101 1000 0001 0100 0000 0101 1001 0110 0101 1000]

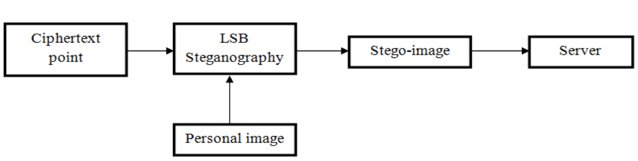


**Figure 3.** Block diagram of LSB steganography.

## 4. Passport Verification System

Separate the Stego image into cipher text and personal image by using Extraction algorithm. Personal Image is directly sent to the passport verification system and the cipher text is converted points into plain text points using private key, these points are converted into plain text using Koblitz method. After that reverse process of encryption is done to decrypt all the data, get back the Personal Information and send it into the passport verification system. The system checks the details and image already stored in the server, weather it is matched or not as shown in Figure 4. The following steps are followed to decrypts the data from the Stego image.

**Step 1:** Stego-Image (SI)

- Take Stego-Image matrix.
  [1011 0000 1100 0111 1000 0100 0010 0001 1011 0000 1100 0111 1000 0100 0010 0001
  0101 1000 0010 0100 0110 0000 0101 0011 0101 1000 0010 0100 0110 0000 0101 0011
  1011 0010 0000 1001 0001 0010 0110 1001 1011 0010 0000 1001 0001 0010 0110 1001
  0001 1000 0100 0101 1000 1000 0110 0111 0001 1000 0100 0101 1000 1000 0110 0111
  0101 0110 1000 0110 0100 0111 0100 0010 0101 0110 1000 0110 0100 0111 0100 0010
  0110 0100 0010 0001 1000 1000 0110 0101 0110 0100 0010 0001 1000 1000 0110 0101
  0010 0110 0101 1001 0110 0011 1000 0100 0010 0110 0101 1001 0110 0011 1000 0100
  0001 0100 0000 0101 1001 0110 0101 1000 0001 0100 0000 0101 1001 0110 0101 1000
  1011 0000 1100 0111 1000 0100 0010 0001 1011 0000 1100 0111 1000 0100 0010 0001
  0101 1000 0010 0100 0110 0000 0101 0011 0101 1000 0010 0100 0110 0000 0101 0011
  1011 0010 0000 1001 0001 0010 0110 1001 1011 0010 0000 1001 0001 0010 0110 1001
  0001 1000 0100 0101 1000 1000 0110 0111 0001 1000 0100 0101 1000 1000 0110 0111
  0101 0110 1000 0110 0100 0111 0100 0010 0101 0110 1000 0110 0100 0111 0100 0010
  0110 0100 0010 0001 1000 1000 0110 0101 0110 0100 0010 0001 1000 1000 0110 0101
  0010 0110 0101 1001 0110 0011 1000 0100 0010 0110 0101 1001 0110 0011 1000 0100
  0001 0100 0000 0101 1001 0110 0101 1000 0001 0100 0000 0101 1001 0110 0101 1000]

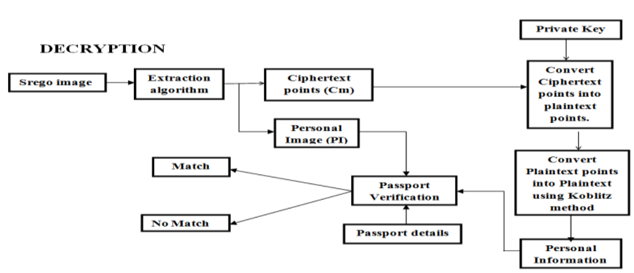


**Figure 4.** Passport Verification System.

**Step 2:** Extraction Algorithm

- Separate the SI (Stego-Image) into Cipher text (Cm) and Personal Image (PI)
- Cipher text values.
  2071 = 0010 0000 0111 0001
  3965 = 0011 1001 0110 0101
  303051 = 0011 0000 0011 0000 0101 0001
  606101 = 0110 0000 0110 0001 0000 0001
- Personal Image (PI)
  [0010 0001 0100 0110 1000 0100 0011 0001 0010 0001 0100 0110 1000 0100 0011 0001 0100 1000 0010 0100 0110 0001 0101 0010 0100 1000 0010 0100 0110 0001 0101 0010 0011 0010 0001 1000 0001 0010 0111 1001 0011 0010 0001 1000 0001 0010 0111 1001 0000 1001 0101 0100 1000 1001 0110 0111 0000 1001 0101 0100 1000 1001 0110 0111 0100 0111 1001 0111 0101 0110 0100 0011 0100 0111 1001 0111 0101 0110 0100 0011 0111 0101 0010 0001 1001 1000 0111 0101 0111 0101 0010 0001 1001 1000 0111 0101 0010 0110 0101 1001 0110 0011 1000 0100 0010 0110 0101 1001 0110 0011 1000 0100 0001 0100 0000 0101 1001 0110 0101 1000 0001 0100 0000 0101 1001 0110 0101 1000 0010 0001 0100 0110 1000 0100 0011 0001 0010 0001 0100 0110 1000 0100 0011 0001 0100 1000 0010 0100 0110 0001 0101 0010 0100 1000 0010 0100 0110 0001 0101 0010 0011 0010 0001 1000 0001 0010 0111 1001 0011 0010 0001 1000 0001 0010 0111 1001 0000 1001 0101 0100 1000 1001 0110 0111 0000 1001 0101 0100 1000 1001 0110 0111 0100 0111 1001 0111 0101 0110 0100 0011 0100 0111 1001 0111 0101 0110 0100 0011 0111 0101 0010 0001 1001 1000 0111 0101 0111 0101 0010 0001 1001 1000 0111 0101 0010 0110 0101 1001 0110 0011 1000 0100 0010 0110 0101 1001 0110 0011 1000 0100 0001 0100 0000 0101 1001 0110 0101 1000 0001 0100 0000 0101 1001 0110 0101 1000]

**Step 3:** Convert Cipher text (Cm) into Plain text using private key.

- Decryption formula:
  - o $Pm + k.Pb - nB\ (k.G) = Pm + k\ (nB.G) - nB\ (k.G) = Pm$
- Cipher text point (Cm) is:
  - o $Cm = \{(2071, 3965), (303051, 606101)\}$
- Determine the plain text value from decryption formula:

  - Pm + k. PB – nB (k. G) = Pm + k (nB. G) – nB (k. G) = Pm
  - {(550, 38) + 2(5, 4) – 1(2(5, 4)) = (550, 38) + 2(1(5, 4))} = Pm
  - (550, 38) + (43, 74) – (43, 74) = (550, 38) + (43, 74) – (43, 74) = Pm
- Pm (x y)= (550, 38)
- Calculate the plain text point.
- Each point (x, y) should choose m integer value less than (x-1)/k to decode the point (x,y) as the symbol m.
- Let, X = 550 y = 38 K = 20.
- (x-1) / K= (550-1) / 20.
- P is the plaintext and value of plaintext m = 65.

**Step 4:** Convert plain text into DNA sequence.

- Example: M = 65
  - We have to repeat this step for all the values.
- 65 65 65 65 65 65 65 65 84 84 84 84 = A AAAAAAATTTT

**Step 5:** Convert DNA sequence into binary value.

Example : AAAAAAAATTTT = 0000 0000 0000 0000 1111 1111

**Step 6:** Convert binary value into hexadecimal value.

Example: 0000 0000 0000 0000 1111 1111 = 0000FF

**Step 7:** Hexadecimal value is convert into RGB color code.

Example : 0000FF = Blue

**Step 8:** UNICODE for RGB color.

- ExampleBlue = U + 0050

**Step 9:** Convert UNICODE into Plain text value**.**

- Example U + 0050 = P

## 5. Conclusion

The proposed algorithm provides higher level of security with less communiation and computational complexity compared with tradition security sysem. The proposed ECC based security scheme provides high security with 160 bit key length. The advantage of DNA cryptography is employed in proposed scheme to obtain the improved level of secutiy. The strength of the securiy is improved by means of Elliptic Curve Discrete Logartihm Problem where retrival of key is very difficult in both ECC encryption and decyption algorithm. Color code cryptography is introduced to increase the level of security and DNA sequences are helped to store the enormous amount of data.

## 6. References


1. Diffie W, Hellman ME. New directions in cryptography. IEEE International Symposium on Information Theory in Ronneby, Sweden. 1976 Nov; 22(6):29–40.
2. Patil D, Vishaka N, Akshaya S, Aparna B. Cryptography based on color substitution. International Journal of Computer Appications. 2014 Apr; 91(16):29–32.
3. Deepa SP, Kannimuthu S, Keerthika V. Security using Colors Code matrix and Armstrong numbers. National Conference on Innovations in Emerging Technology; 2011. p. 157–60.
4. Zhang Y, Xiao D, Wen W, Wong KW. On the security of symmetric ciphers based on DNA coding. Information Sciences. 2014 Dec; 289:254–61.
5. Rajam STR, Kumar SBR. Enhanced Elliptic Curve Cryptography. Indian Journal of Science and Technology. 2015 Oct; 8(26):1–6.
6. Ramalingam M, Isa NAM. A steganography approach over video images to improve security. Indian Journal of Science and Technology, 2015 Jan; 8(1):79–86.
7. Mohamed AA. An improved algorithm for information hiding based on features of Arabic text: A Unicode approach. Egyptian Informatics Journal. 2014 Jul; 15(2):79–87.
8. Jambhekar ND, Dhawale CA. Bit level key agreement and exchange protocol for digital image steganography. Indian Journal of Science and Technology. 2015 Jul; 8(15):1–7.
9. Halder T, Karforma S, Mandal R. A novel data hiding approach by pixel-value-difference steganography and optimal adjustment to secure E-Governance documents. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–7.
10. Shi L, Su S, Xiang Z. Design of a passport anti-forgery system based on digital signature schemes. Springer-Berlin: Heidelberg: Intelligent and Security Informatics. 2009; 5477:101–11.