INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 9, Issue 2 - V9I2-1136)
Available online at: https://www.ijariit.com

Data encryption on image cryptography and steganography

Ibraheem Ojelade
iojelade@my.apsu.edu
Austin Peay State University, Clarksville, USA

Ibrahim Abdulkareem
iabdulkareem94@gmail.com
Austin Peay State University, Clarksville, USA

ABSTRACT

These days, information is transmitted via the internet. Consequently, information security has emerged as a crucial concern. The well-known method of network data security is cryptography. In digital media, steganography is the method used to conceal the message. Comparatively speaking, the security of elliptical curve cryptography outweighs that of the ones currently in use. In this paper, a hybrid model that combines steganography and ECC with public keys is presented. can offer higher levels of higher security than steganographic or one ECC method alone. This initiative's primary goal is to conceal sensitive data from internet users, the military, and various corporate sectors that commonly use public networks for interaction

Keywords: *ECC, RGB, LSB, CNOT Gate, PSNR, Steganography, and Cryptography*

1. INTRODUCTION

More people are recognizing the significance of network security. data is being transmitted over the Internet. In order to safeguard against unwanted access, confidentiality and data integrity are necessary. As a result, the field of information concealment has rapidly expanded. Through the use of encryption, the data that needs to be sent can be made secret so that only the intended recipient will understand it. Cypher text refers to the unencrypted data, and plaintext to the original data. The data is hidden with a key [1]. Depending on how many keys are utilized and how they are used, there are many types.
Two different types of cryptography methods exist:

- Cryptography with symmetric keys
- Cryptography with Asymmetric key

As a matter of fact, symmetric key cryptography is a method in which the same cryptographic Both encryption and decoding rely on keys. The key can be utilized by the receiver to retrieve the original data. High data speeds are offered by symmetric key cryptography, which may also be coupled to create stronger cyphers. It can also be used as a building block for other cryptographic processes. Here, the most important aspect is that the safety of the key determines the safety of the data. As a result, caution should be used when the sender and recipient exchange keys [2].

Key transportation is a challenge for symmetric cryptosystems. Before the actual communication is transmitted, the receiving system must be provided with the secret key. Every electronic communication method is unsafe because it is difficult to ensure that communication lines won't be tapped. Therefore, face-to-face key exchange is the only secure option. A symmetric cryptosystem is unable to offer irrevocable digital signatures [3].

The employment of two keys is known as asymmetric key cryptography. Both the plaintext and the cypher text are locked or encrypted using different keys. There is no key that can perform both tasks. These keys each have one that has been publicly available or made public, but the other is kept a secret. This method's data rate throughputs are noticeably lower than those of symmetric key technique [2].

The practice and science of concealing information so that it cannot be viewed is known as steganography. A concealed piece of information is encoded to conceal its existence. even exists. Steganography can be utilized to conduct covert transactions when combined with current communication techniques.

Elliptical curve cryptography (ECC) and steganography are combined in the suggested hybrid paradigm. Key size for ECC is considerably smaller than for RSA, according to a prior study [11]. Table 1 lists the differences between the ECC and RSA algorithms. Steganography allows us to encrypt a cover image with several messages. Section 3 provides a description of the suggested model, and Section 4 provides the experimental findings.

Table 1 : We compare RSA and ECC

ECC key	RSA key
203 bits	612 bits
215 bits	868 bits
236 bits	1024 bits
266 bits	2048 bits
217 bits	3072 bits
389 bits	7680 bits

2. RELATED WORK

2.1 USING ELLIPTICAL CURVES FOR ENCRYPTION

Public key cryptography using elliptic curves (ECC) is a method that uses elliptic curves over finite fields as its foundation algebraic structure [13].

2.1.1 There are several elliptic curves operations

F should represent the Equation B2's Ellipse over the limited field Q.

= a3+xa+y and satisfy 4x3+27y2≠0 (mod q).

The operations are scalar multiplication, doubling points and adding points.

2.1.1.1 Addition of Points:

let A(a1,b1) point is the center of an infinite field F(q)

$$A(a_1,b_1)+\infty = \infty + A(a_1,b_1) = A(a_1,b_1) \quad (1)$$

let A(a1,b1) and B(a2,b2) two points, with the outcome point is R(a3,b3) for all points in E(P) $A(a_1,b_1)+B(a_2,y_2)=R(a_3,b_3)$

Where $x^3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$, and $y^3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$ (2)

2.1.1.2 Point Doubling

let $A(a_1,b_1)$ be the point in E(P) then $2A=R(x_3,y_3)$

Where $a^3 = \left(\frac{3x_1^2 + a}{2y_1}\right) - 2x_1$ and $b^3 = \left(\frac{3x_1^2 + a}{2y_1}\right) - (x_1 - x_3) - y_1$ (3)

2.1.1.3 Deduction Point

Assuming two points A(a1,y1) and B(a2,y2), the resulting point is R(x3,y3) for all points in E. (P)

$R(a_3,b_3) = X(a_1,b_1) - Y(a_2,b_2) = A(a_1,b_1) + \{- B(a_2,b_2)\}$

$= X(a_1,b_1) + Y(a_2, -b_2)$ For any point

$X(a_1,b_1) = X(a_1, -b_1)$

2.1.1.4 Point Increase

Any location along the elliptic curve, let it be X. (F). The process of multiplying point X is then referred to as iterative addition. A+ X+ k times X+ X+ equals kX.

k is an integer in the field P.

2.1.2 Applying an Elliptic Curve to F (Q) or F, the Elgamalcryptosystem [4] ()

Public and private keys creation

Rob chooses F (x, y) *applying an elliptic curve to* F (Q) or F (2^n).
Rob selects a curve point,
e_1 $x(_1, y_1)$.
Rob chooses an integer d.
Rob calculate $e_2(x_2, y_2)$ =E × e_1 $x(_1, y_1)$.
Be aware that in this case, multiplication refers to multiple point additions.
Rob announces E (a, b), $e_1(x_1, y_1)$, and e_2 $x(_2, y_2)$ as his public key;
D is kept by Rob as his own key.

Encryption

Arun chose Q as her plaintext, a point on the curve.
She then determines two locations on the text that serve as cypher messages:
C_1= r ×e_1
C_2= P + r ×e_2

Decryption

Rob uses the formula below to calculate Q after getting it.
- Q = C_2- (d× C_1)

2.2 STEGANOGRAPHY

Least Significant Bit (LSB) Injection is the simplest technique for obfuscating data in an image [5][14]. The quantity a minimal and invisible to the human eye number of changes in a 24-bit true color image. Consider, for illustration Because the RGB encoding for the three neighboring pixels in our image takes up nine bytes:

10110001	11000001	00111001
10010110	00001111	11000101
10011001	00001111	11000100

Let's say we want to conceal the next nine bits of data: 101111001. The following results are obtained if we place these 11 bits on top of the LSB of the previous 11 bytes (where the bolded portions have been altered) pixels:

11101011	11011011	00100101
11100110	11100110	00111011
10011001	00010011	11001011

A very general description of the components of the steganographic procedure is given by the formula below: Stego-image is the combination of a cover picture and text, a picture, etc.

2.2.1 CNOT Gate

[7][12] The Controlled Not Gate is another name for the CNOT gate. It fits the category of a quantum computer. For building a quantum computer, it is necessary. The first qbit in the The control bit in a CNOT gate is followed by the target bit in a second bit [7].

Figure 1: CNOT gate

Where A and B are the control and (+) denotes EXOR and target qbits, respectively. The EX-OR gate and the CNOT gate are entirely dissimilar. The CNOT gate is reversible after the EX-OR gate, which is an irreversible gate [7].

2.2.2 Transforming using Wavelet

Compressions of the wavelet lossy and without loss available [12]. When data is compressed without any loss, the original data can be recovered, whereas only some data can be recovered. in lossy compression. Lower memory requirements and data compression transmitted more simply by using wavelet modification to store data in a smaller amount of space [8]. Wavelet compression procedures: Activate wavelet decomposition on the loaded image, then compress with a defined threshold.

2.2.3 Random Number Generators

The fake random number generator is called Blum Blum Shub [12]. Random numbers are produced using this. According to the formula below [9],

$$X_{i+1} = (X_i)^2 \ mod \ n \quad (4)$$

Where, X_i is the seed, and n be the range.
In cryptography, to generate random numbers, a pseudo-random bit generator is utilized. The resources used by They are the pseudo-random bit generators seed, two huge prime numbers, and the range. Below are some mathematical formulas.,

$$X_{i+1} = (PX_i + Q)^2 \ mod \ n \quad (5)$$

The seed is If there are two important prime numbers, P and Q. the variety.

2.2.4 Cryptography algorithm

Wavelet transforms are used to compress the hidden information, which may be presented in text, an image, or another media [10]. the shortened text is first transformed into the relevant ASCII value, which is then transformed into the equivalent 8-bit binary value. The Control NOT gate is used to encode an 8-bit binary value. These bits are now prepared for LSB insertion into an image. The cover image can now contain the encrypted content. The image is changed into its desired format prior to incorporating the message. matching pixel values. These values are set up as a r r and c stand for the corresponding columns and rows in the c matrix. On the cover image in order to protect the confidentiality of the information, many undetermined locations. Using a random number generator, the random positions are identified. In this method, random integers function as a key. To generate the random rows and columns, the Both the Pseudo Random Generator and the Blum/Blum/Shub generator are used. The generator uses the key to produce random numbers (seed). Randomness varies from generator to generator. Unpredictability is produced in the sequence by padding the bits. The LSB insertion technique is now used to embed the secret message in the relevant bits. once random spots in the image (pixel values) have been chosen. 2.2.5

Decryption Process

The procedure by which encryption is revoked is known as decryption[10]. The received stego image will be converted by the receiver into its equivalent pixels (matrix form). To pinpoint the whereabouts of bits have been inserted, the receiver will generate a random number with the aid of the Key (seed) using random generators. Applying the reverse LSB insertion technique after obtaining the pixel coordinates will produce the encoded bits. Retrieving the compressed text requires applying Control NOT gates to the encoded bits. It is possible to recover the original secret information by using the wavelet transformation technique (decompression).

3. SUGGESTIVE MODEL

The elliptic curve parameters in the suggested model are a field of numbers modulo p with the notation (p, E, P, n), When prime number p is Fp. The expression y2=x3+ax+b, If and are real numbers over and (a,b) satisfy Fp. 4a3+27b20, defines E as the elliptic curve over Fp (mod p). The curve includes the infinitely distant point. E(Fpabelian)'s subgroup produced By p, P=P, P, 2P, 3P,... (n-1)P.

3.1 Producing keys

Contribution

input parameters for the elliptic curve domain (p, E, P, n,)

Production

Public key Q and private key d.
Choose $d \in_R [1,n-1]$
Select $e_1\ x(\ _1, y_1)$.
Compute $e_2(x_2, y_2)$ =d × $e_1(x_1, y_1)$
Q = $\{e_1, e_2, E\}$
Revert back (Q, d)

3.2 Incorporating LSB and encrypting

Contribution:

Plaintext m, public key Q, message image I, cover image C, and (p, E, P, n) are the parameters for the elliptic curve domain.
Stego-image Key CI and Stego Show the letter Point "m" in the letter "E." ( ).
Chose $K \in_R [1, n-1]$.
Evaluate C_1=k× $e_1(x_1, y_1)$
Evaluate C_2= M +k× $e_2(x_2, y_2)$
RGB cover photo = C
Utilizing LSB Steganography, conceal (C1, C2) in I.
Using steganography, conceal I in C.
Revert back (CI)

3.3 Decryption

Parameters for the Elliptic Curve Domain (p, E, P, n), the Private Key d, the Steno-Image CI, and the Steno Key.
Production: (message m, image I)
Excerpt I from CI Extract C_1, C_2 from I
Evaluate M = C_2 -d× C_1 and compute m from M
Revert back (m, I)

3.4 Background Research

Think about the elliptical curve y2 = x3 + 4x + 20 over a finite field.
F_{29}

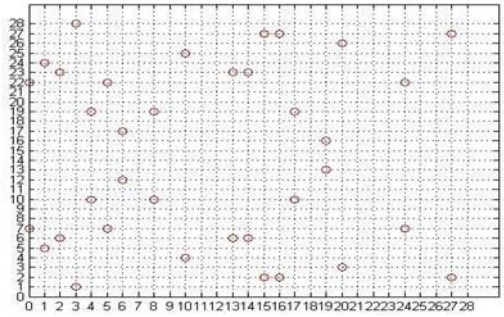

Figure 2: Curve's points y2 = x3 +4x+20 mod 29

Table 2: Different locations on an elliptical curve hide different characters.

∞	1,7	4,17	23,6	12,27	6,35	14,19
g	f	e	d	c	b	a
23,62	6,30	16,23	16,23	10,35	18,13	38,27
h	i	k	j	l	m	n
5,26	3,6	0,36	27,6	2,63	2,36	23,27
o	p	q	r	s	t	u
0,3	3,68	5,7	6,2	13,16	13,4	33,6
v	w	x	y	z	0	1
13,6	8,39	23,7	16,10	6,17	13,2	63,26
2	3	4	5	6	3	8

3.4.1 Creation of keys

y2 = x3 + 4x + 20 over a finite field for the elliptic curve F29.
Rob choose E (a, b) across an elliptic curve F_p a =4, b=20,p=29
Rob choose a point on the curve, $e1(x1,y1)$. let(1,5)
Rob chooses an integer d. Let d = 3
Rob compute $e_2(x_2,y_2)$ =d × $e_1(x_1,y_1)$. (Keep in mind that multiplication here refers to numerous point additions. $e_2(x_2,y_2)$=(20,3))
Rob proclaim E (a, b), $e_1(x_1,y_1)$, and $e_2(x_2,y_2)$, p as his public key; E(4,20),e_1(1,5),e_2(20,3)
Rob keeps d as his private key.

3.4.2 Encryption

Contribution :(cover image C, image I, message 'm')
Production : (steno object CI)
Arun selects P, a point on the curve, as her plaintext, P.
EXAMPLE Message=hello
P1=(24,22),P2=(15,27),P3=(10,25),P4=(10,25),
P5=(5,22)

She then computes a pair of points on the text as cipher texts:
D1= r ×$e1$
D2= P + r ×$e2$

Table 3: the method of encrypting the example above

points	r	D_1= r ×e_1	D_2= P + r ×e_2	(D_1D_2)
h=P1(23,22)	6	(6, 39)	(13, 23)	(c, k)
e=P2(12,27)	6	(16, 39)	(3, 28)	(g, w)
l=P3(13,25)	6	(6, 62)	(13, 4)	(f, 0)
l=P4(16,35)	65	(3,6)	(2,6)	(p ,t)
o=P5 (5,62)	6	(26, 3)	(3, 7)	(d, x)

Distinct all D1, D2 and make array of
D1* ∈{D11, D12, D13…….}
D2* ∈{D21, D22, D23……} correspondingly.
Surrounded D1* and D2* into the image I
Select one cover image D
DI = Surrounded I into D

3.4.3 Decryption

Contribution: stego-object, stego key
Production: message 'm'
Using the same stego key that was used to create the stego object, the encrypted text and picture are extracted from the stego object. Utilizing a private key that is encrypted, we may decipher the cypher text to obtain the text message. $M = D_2 - d \times D_1$

Think of the previous instance

Table 4: The method used to decrypt the example

(D_1,D_2)	$D_2 - d \times D_1$	P	M
(c, k)	(16, 36) – 3 × (4, 69)	(26, 22)	h
(g, w)	(3, 68) – 3 × (13, 19)	(13, 27)	e
(f, 0)	(13, 4) – 6 × (6, 62)	(13, 25)	l
(p ,t)	(6,6) – 3 × (3,6)	(16,35)	l
(d, x)	(5, 6) – 3 × (23, 3)	(5, 62)	o

Production message m = (hello)

4. EXPERIMENTAL RESULT

The message was processed using the aforementioned hybrid a strategy, as seen in figure (3). Figure indicates the cover image used for this procedure (4). Figure illustrates the full method's procedure in its total (5).

Figure 3: Patient info and brain MRI scan

Figure 4: Cover image (animal.jpg)

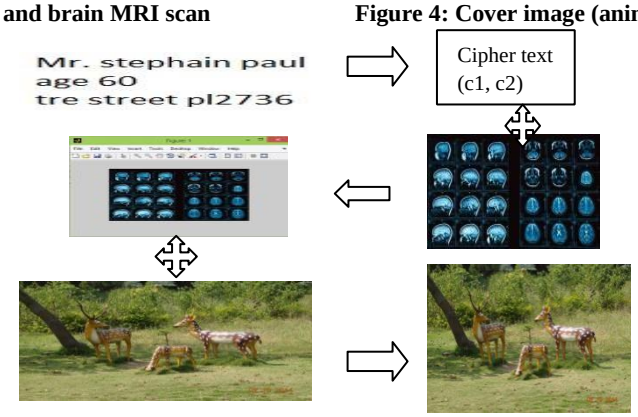

Figure 5: overall model development procedure

The primary photo, which will include the concealed information contained, is the cover image. The final image is a stego image, a similar from the cover photo's image style. Highest Signal-to-Noise Ratio (PSNR) is used to assess the stego image's quality. Statistically speaking, PSNR is utilized for Quality evaluation of digital photographs or movies [6]. The simplest definition of PSNR is using the mean squared error (MSE), which is defined as follows for two monochromatic images I and K, where I represents the original image and K signifies a noisy estimate of it:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - k(i,j)]^2 \quad (6)$$

The PSNR is defined as:

$$PSNR = 10\log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20\ \log_{10}\left(\frac{MAX_1}{\sqrt{MSE}}\right) \quad (7)$$

Better image quality or reduced distortion is indicated by a higher PSNR. The likelihood of a visual attack by the human eye decreases as PSNR increases.
Table 3 displays the PSNR value after various input data and picture sizes are embedded.

Table 5: PSNR

Shelter image size(pixel)	input		PSNR
	Text(bytes)	Image(pixel)	
600x400	64	394x284	76.3741
600x400	148	394x284	76.3747
600x400	148	356x356	75.5312
600x400	828	356x356	65.5314
600x400	2339	356x356	75.5310

5. CONCLUSION

Steganography and cryptography are both used in the proposed model that was previously presented. The method's objective is to make it challenging for the intruder to ascertain whether information is present. Information is secured more by the dual security. By using a public network and this approach, anyone can communicate numerous pieces of information to the recipient with ease. Defense, government portals for business, finance, communication, and other topics interchange is more important can all benefit greatly from this concept. Because audio and video have a greater capacity for data concealment than images, these formats will likely be used in steganography and cryptography in the future.

6. REFERENCES

[1] M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, and M.Z.I.Shamsuddin, Information Hiding using Steganography, National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 2003 IEEE.

[2] S Ushll , G A SathishKumal, K Boopathybagan,A Secure Triple Level Encryption Method Using Cryptography and Steganography, 20 II International Conference on Computer Science and Network Technology, 978-14577-1587-7/111$26.00 ©20111EEE, December 24-26, 2011

[3] X. Zhang and S. Wang, Steganography using multiplebasenotational system and human vision sensitivity, IEEE Signal Process. Lett., vol.12, no. I, pp. 67-70, Jan. 2005.

[4] BehrouzA.Forouan, Debdeep Mukhopadhyay, 2nd edition Cryptography and network security, McGraw Hill Education, pp.295-296

[5] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, A New Approach for LSB Based Image

[6] M. Hossain, S.A. Haque, F. Sharmin, Variable RateSteganography in Gray Scale Digital Images Using Neighborhood Pixel Information, Proceedings of 200912th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.

[7] Controlled NOT gate, From Wikipedia, http://en , wikipedia . org/wiki/Controlled_NOT _gate .

[8] Ivan W. Selesniek "Wavelet Transforms A Quick Study", PhysiesToday magazine, üetober, 2007.

[9] "Blum Blum Shub", From Wikipedia, http://en.wikipe dia.org/wiki/Bluffi_Bluffi_Shub

[10] R Praveen Kumar, V Hemanth, MShareef, Securing Information Using Sterganoraphy, 2013 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2013]

[11] Ipsita sahoo, SEMINAR REPORT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS http://www.facweb.iitkgp.ernet.in/~isg/ICTSEMINAR/R EPORT-Ipsita.pdf

[12] M Venkteswara Reddy, M Lakshman Naik, Securing Information Using Steganography, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064

[13] Darrel Hankerson, Alfred Menezes, Scott Vanstone, Guide to elliptic curve cryptography, springer

[14] Ahaiwe J. Document Security within Institutions Using Image Steganography Technique.

