International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 3, May.-June. 2013 pp-1768-1773 ISSN: 2249-6645

Color Image Encryption Based on Symmetric and Asymmetric Cryptosystems and Transcendental Numbers

C. A. Jiménez-Vázquez[1], R. Flores-Carapia[2], V. M. Silva-García[3], B. Luna-Benoso[4]
[123]*Instituto Politécnico Nacional, CIDETEC, México.*
[4]*Instituto Politécnico Nacional, ESCOM, México.*

ABSTRACT:*This work presents an algorithm to cipher color images using a hybrid cryptosystem, one which is symmetric FIPS-197 and the other an asymmetric elliptic curve being a nonsingular* $y^2 \equiv x^3 + Ax + B(mod p)$ *over* $Z_p(ECC)$*. The construction of the hybrid cryptosystem proposed, has two important aspects; the first is the generation of a random number, which we will call* γ*, of the same prime length finite field* Z_p*. The issuer figures* γ *ECC with point compression technique, in such a way that the result is a string encryption twice the length of the string representing* p *plus an extra byte called* γ^**. The second aspect is to multiply a* γ^* *by the transcendental number* π *and the resulting product is taken right of the decimal point for the length of the image in bytes. Subsequently, it performs the XOR operation of this with the image bytes generating* I^**.* I^**divides into sections of length equal to* γ^* *and each section is applied to the XOR operation with* γ^* *thus resulting in an encrypted image. The issuer encrypts* γ^* *with AES with the key* K^1 *resulting* γ^{**}*, turns the transmitter key* K^1*, encrypts with our private key by generating ECC* K^**. Consequently, the issuer sends the receiver the encrypted image and the ordered pair* (γ^{**}, K^1)*; this with their private key to perform the reverse process to obtain the original image. The security of this cryptosystem is in the size* γ^* *as this can have a size of over 225 bytes (if taken top* $\geq 10^{270}$*) and would have to prove more than* $2^{225\times 8} - 1$ *possible blocks depending on the size of* p*.*

KEYWORDS: *Encryption, images cipher, transcendental numbers, AES, elliptic curve.*

I. INTRODUCTION

The proliferation of computers and the Internet boom that has happened in recent years has made it possible for anyone to distribute any type and amount of information easily. There are many numbers of applications that make use of the latest exchange systems information across Wifi networks, fiber optic networks, satellites, etc. In the exchange of information and thanks to the popular use of mobile computers, now sharing images is a very important part in our daily lives.However, the importance of images exchange not only applies to our everyday life, such as military class databases which have images of maps with locations of secret facilities, or in the banking industry where millions of dollars are invested daily in the exchange of images containing highly sensitive information. Therefore, much research has been developedon ciphering and deciphering images in which one of the main objectives is to recover the original image from the cipher image without some data loss. To achieve this, it is necessary to ensure the confidentiality, integrity and authenticity of the transmitted image.

In literature different proposals can be found such as the development of a cryptosystem whichcan cipher images using chaotic logistic maps [1].These have an advantage over traditional algorithms such as high security, speed, etc. Another example of this type of cryptosystem is the one in which the encryption is based on DNA sequences [2]. The main characteristic of this algorithm is to reduce the cipher time of a very large image (such as FullHD). There are cryptosystems where a change has been made to the algorithms that are within the international standard as DES [3]. In this proposal the Triple-DES algorithm has been modified, based on the initial permutation that begins the algorithm's rounds [4].This permits each data ciphered generates a different dynamic permutation. There is another work in which image encryption is based on how the Rubik cube rotation generating its sequence to be sorted [5]. This article intends to use Elliptic Curve Cryptography. The ECC has been researched very much over the past 30 years and importantly has been used to solve Fermat's Last Theorem [6].

Elliptic curves were introduced by Neal Koblitz [7] and Victor S. Miller in 1985 [8] independently, and since then, this has been a vast research area in which mathematical work has been developed with this tool. One application is where the ECC has been a digital signature algorithm [9-12] which can be used to replace existing algorithms with equal or greater security. ECC also has been applied in security systems based on radio frequency [13]. Regarding the image encryption with this mathematical tool, there is a paper that makes the image encryption based on a mapping from a point on the curve for each image pixel [14, 15].Based on a point table associated with each point of the curve, each pixel is transformed into its corresponding encrypted pixel. Although this sounds feasible, the problem with this is to know the order of the field that generates the curve. A system with a similar target develops random sequences generated by the cyclic group of the elliptic curve [16]. A crypto system is proposed that generates a random number known as NONCE which transforms the message akin to a point on the elliptic curve [17]. There are many hybrid cryptosystems (such as this article) as shown in [18], which combines chaotic maps with ECC and there is another which is based on using ElGamal homomorphism for ECC [19].

Another feature of this work is the ability to cipher an image (say FullHD) in a fast enough time and achieve good encryption information thanks to the method proposed. To achieve this, we have applied the use of transcendental numbers (in this case π) [20, 21] to achieve this goal, which also created a hybrid cryptosystem which uses ECC and AES encryption to ensure the strengthening of the image.

II. PRELIMINARIES

A nonsingular elliptic curve is the solution set of the equation $y^2 \equiv x^3 + Ax + B \pmod{p}$ and must satisfy $4A^3 + 27B^2 \neq 0 \pmod{p}$. Therefore; the equation condition ensures that there are 3 different solutions. Elliptic curve points form an additive abelian group with $\mathcal{O}$ as the identifying element that satisfies the properties: commutatively, existence of identity and associativity [22].

Let Ebe an elliptic curve and $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$ two points over $E$with $P\_1, P_2 \neq \mathcal{O}$. We define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:

1. If$x_1 \neq x_2$, then$x_3 = m^2 - x_1 - x_2, y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{y_2 - y_1}{x_2 - x_1}$
2. If $x_1 = x_2$ but$y_1 \neq y_2$, then $P_1 + P_2 = \mathcal{O}$
3. If $P_1 = P_2$ and$y \neq 0$, then$x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{3x_1^2 + A}{2y_1}$
4. If $P\_1 = P\_2$ and$y_1 = 0$, then$P_1 + P_2 = \mathcal{O}$. We define $P + \mathcal{O} = P$ for all points P over$E$.

The curve's cardinality Eon F_q, corresponds to the point number that is generated in the field. It is a very important issue in safety cryptosystems since it depends on the cryptosystembeing sufficiently robust.The Hasse-Weil theorem relates the point number ofthe field size and for counting the pointgroupSchoof's algorithm can be used. For calculating a root and finding the generator for an elliptic curve E, we $Z^{\frac{p-1}{2}} \equiv 1 \bmod p$, if $p \equiv 3 \bmod 4$, it is given by $\pm Z^{\frac{p+1}{4}} \equiv 1 \bmod p$, this will help us in order to find the field generator which solves the equation $y^2 \equiv x^3 + Ax + B \pmod{p}$ [22-26].
The compression point operation can be expressed as**:**

Compression_Point::$E \backslash \mathcal{O} \rightarrow Z_p \times Z_2$

And is defined as:

Compression_Point$(P) = P = (x, y \bmod 2)$, where $P = (x, y) \in E$

Algorithm 1 shows the inverse operation (**Descompression_Point)** to recover the elliptic curve point $P = (x, y)$ of $(x, y \bmod 2)$. This algorithm computes $\sqrt{z} \bmod p$.

Algorithm 1: Function for recovering the compression point
Require:axis x, byte i
Ensure: Point P.
1: **procedure**Descompression_Point(x, i)
2: $z \leftarrow x^3 + Ax + B$
3: **if**z is not quadratic module remainder p **then**
4: **return** "(fail)"
5: **else**
6: $y \leftarrow \sqrt{z} \bmod p$
7: **if**$y \equiv i \pmod 2$ then
8: **return**(x, y)
9: **else**
10: **return**$(x, p - y)$
11: **end if**
12: **end if**
13: **end procedure**

III. PROPOSED MODEL

The proposed hybrid cryptosystem is the combination of AES symmetric system and the elliptic curve as the asymmetric encryption, but to generate a good disordering of the image, the decimal numbers of π are used.

1. This cryptosystem has two important aspects: The random number generation. In this step we proceed to generate a random number η where $1 \leq \eta \leq \#E(fp) - 1$. This number is encrypted with the point compression technique described above. The data encryption Ψ of length $2l + l$ where$l = \frac{t}{8}, t = \log_2(p)$, will be used as a private random key cryptosystem.
2. Secret number. WhereΨ will serve to multiply by π since π is a transcendental number. All decimals of this number are not periodical, the multiplication by Ψ with the other number would generate another transcendental number. This result, called$F$, will be used to clutter an image.

Definition 3.1 Ψ is the result of encrypting the random number $\eta$where $1 \leq \eta \leq \#E(fp) - 1$, the compression point scheme is used and $\phi = (\Psi)(\pi)$.

Since $\Psi$and ϕ are very large numbers, these are stored in strings of bytes depending on the size of each, i.e., these numbers are arrays of bytes which are treated as large integers.

Let's suppose that we have two entities $A$and B. Entity A sends an encrypted image to entity B, therefore:$A$and$B$ agree with each other to use an elliptic curve cryptosystem and follow the entire procedure described in [27].

- $A$and$B$ have already chosen their private keys for ECC, but A needs to choose a key for the AES asymmetric system which we will call ρ.

To encrypt an image $I_{m \times n}$ of size$m \times n$, where $m$is the rows and n the columns, A must follow these steps:

1. Read the image $I_{m\times n}$ and generate a string of bytes $buffImage$ of size $m \times n \times 3$ for color images of 24 bits of resolution.
2. Read π of a file previously generated. Ashould read $\pi$the same size of the image $I_{m\times n}$in a string of bytes. Only the numbers are taken after the decimal point, the integer number of π is not taken.
3. Generate random number Ψaccording to Definition 3.1 with its private keyσ, for the data format follows the procedure used in [27].
4. Generate random number ϕ according to Definition 3.1 using the string π in numerical representation.
5. Amust encrypt a Ψ by AES through its key ρm this generate Ψ'.
6. Aencryptsits private key ρ ECC and formatting data using [27], this will generate an encrypted key ρ'.
7. ρshould perform the operation $buffCipherImage = \phi \oplus buffImage$, the result will scramble the image the first time.
8. Amust divide $buffCipherImage$ in blocks of $2l + 1$ bytes and each block $buffBlock_i$, where $i = 0, 1, 2, \ldots, \frac{m\times n}{2l+1} - 1$ and A must perform $buffBlock_i = buffBlock_i \oplus \Psi$ by each block. With this A has encrypted all the image information.
9. Now A saves the image and proceeds to save the i-blocks, then A can send to $B\Psi'$ and ρ' which are used for obtainingthe original image.

Therefore A has already encrypted the image and sends the encrypted key ρ' by using ECC and Ψ' that was encrypted with AES.

B In turn, upon receipt of the encrypted image, should do the reverse process as follows:

1. B gets ρ' and Ψ':

a. The key ρ' which must decode ECC through its private key k, obtaining the key ρ.

b. The block Ψ' that is encrypted with AES is decrypted with the key $\rho$to obtainΨ, recalling that this block is used to operate with the image as a random number.

2. Bshould read π according to the image size.
3. Bproceeds in reverse, i.e. operates as in step 8 and then operates according to step 7. Bobtains the original image.

IV. EXPERIMENTAL RESULTS

The experiment that was carried out to test this algorithm was performed on a 2.4 Ghz core i7 with 8 Gb Ram. The way quality encryption is determined is with the proposal made in [4], usingχ^2. With this procedure and plotting the frequency histogram we can determine if the procedure performed was successful. Table 1 and figure 1 show different picture sizes over time encryption of this hybrid cryptosystem for the procedure used in [4] and the value of χ^2. For obtaining these results the curve called P-521was used [28], and also the number prime which is given there.

The security offered by this hybrid cryptosystem, lies in the generation of a random numberthat is obtained by the process of the elliptic curve encryption. This number according tothe prime number that was used to build the field Z_p is about 10^{150}, which is generated by a string byte with a length of 66 bytes having a length of 133 bytes (This size can vary accordingto the size of the prime number that generates Z_p).

Table1: Comparison between our hybrid cryptosystem and Triple DES 96.

Size	Hibrid		Triple DES 96	
	Time$(seg.)$	χ^2	Time$(seg.)$	χ^2
320×200	0.279	755.2238	1.890	750.1360
320×240	0.161	741.2381	2.609	722.5999
640×480	0.269	793.3555	9.101	810.5983
800×600	0.270	734.9383	14.860	761.9178
1024×768	0.292	761.0994	24.203	807.7024
1280×768	0.335	741.3931	28.532	715.9650
1280×1024	0.439	742.6301	35.953	715.0464
1440×900	0.411	802.7540	36.365	798.0950
1600×1024	0.436	747.6839	49.703	761.0825
1600×1200	0.591	827.8274	54.125	773.3616
1920×1080	0.469	716.1687	58.250	760.9197
4096×3112	2.146	798.2641	384.422	886.2007

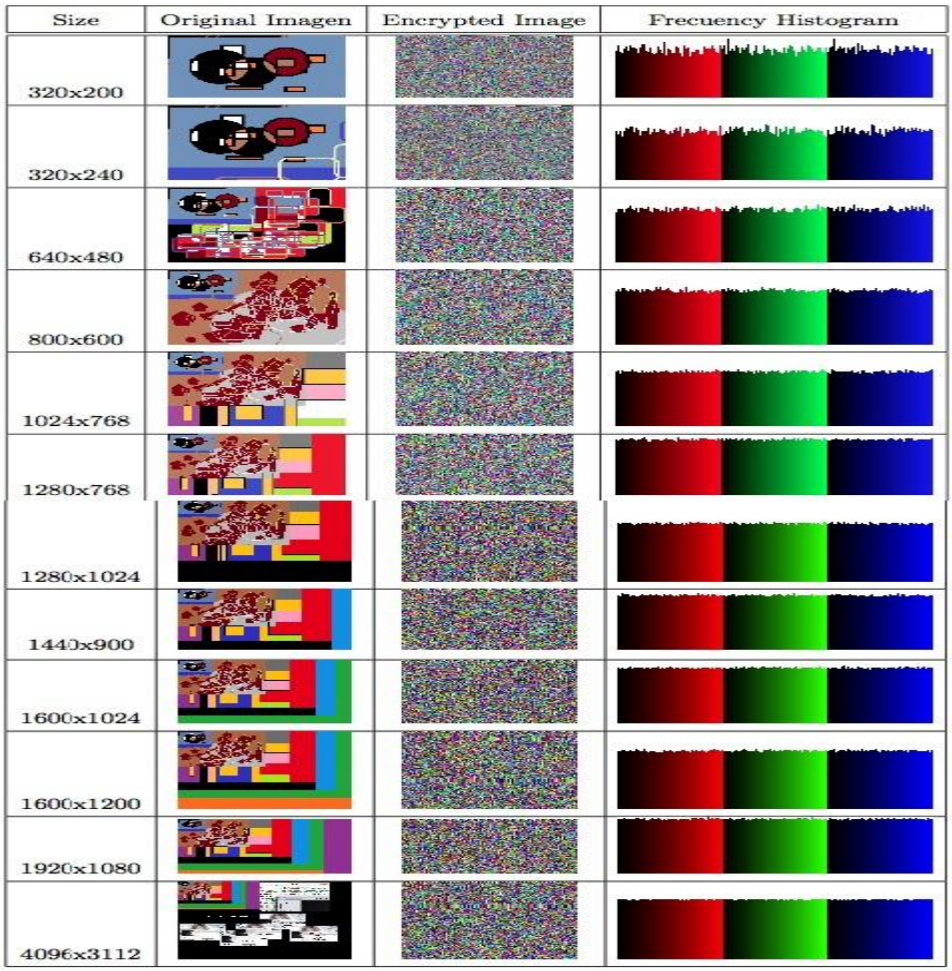

Figure 1: Original images, encrypted images and histograms for different image sizes.

For attacking this cryptosystem, we should know the random number and we should know the private key that uses ECC. ECC's strength lies in solving the discrete logarithm problem for elliptic curves [9, 22] and also the private keys of the sender and receiver being 256 bits. The random number to be sent to the receiver is encrypted using AES with a 128-bit key and this key is encrypted with ECC using the sender's private key. In order to know the random number, we should break both, ECC and AES to obtain it. Yet another way to obtain it would be to try all possibilities to generate the number and validate with multiplication times π. In this example, the number is 133 bytes so we should prove $2^{133\times 8}-1$ operations, but this computationally is very expensive.

Table 2 shows that the security of this cryptosystem increases if we use a prime number to generateZ_p.

Table 2: Security of our cryptosystem

Prime number's order	Operations
10^{150}	$2^{1064}-1$
10^{270}	$2^{2040}-1$
10^{512}	$2^{3400}-1$
10^{1024}	$2^{6808}-1$

V. CONCLUSIONS

The result obtained by χ^2 is quite close to that shown in [4]. However, the time required to obtain the encrypted image increases significantly as we increase the image size. This also presents a hybrid cryptosystem, but the time required for the encryption is significantly much smaller. Although all articles are based on the image histogram, it is sufficiently linear to determine if encryption is good enough. The images used for encryption are small compared with the image presented in this paper which shows the strength of this hybrid cryptosystem.

We must also consider safety presented by the use of random number generation which would be very hard to find because all the combinations would have to be proved.

However, the hybrid cryptosystem's time encryption can still be improved optimizing the operation $Q=kP$ as is proposed in [29, 30, 31].

VI. ACKNOWLEDGEMENT

The authors would like to thank the InstitutoPolitécnicoNacional (SecretaríaAcadémica, COFAA, SIP, Proyecto SIP-20130156, CIDETEC and ESCOM) and the CONACyT for their economic support to develop this work.

REFERENCES

[1]. Ismail Amr Ismail. A digital image encryption algorithm based a composition of two chaotic logistic maps. *International Journal of Network Security, 11(2)*, 2010, 1–10.
[2]. Xiaopeng Wei Shihua Zhou, Qiang Zhang. Image encryption algorithm based on DNA sequences for the big image. *IEEE Computer Society, editor, International Conference on Multimedia Information Networking and Security, 978-0-7695-4258-4/10*, 2010, 884–888.
[3]. Federal Information Processing Standards Publication, editor. *Data Encryption Standard (DES)* U.S. Department of Commerce/National Institute of Standards and Technology, 1999.
[4]. M. Silva-García, R. Flores-Carapia, I. López-Yáñez and C. Rentería-Márquez. Image encryption based on the modified triple-des cryptosystem. *International Mathematical Forum vol. 7, no. 59* 2012, 2929-2942.
[5]. Shaowei XIA Li Zhang, Xiaolin TIAN. *A scrambling algorithm of image encryption based on rubik's cube rotation and logistic sequence*. IEEE Computer Society, editor, nternational Conference on Multimedia and Signal Processing, 2011.
[6]. Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals Of Mathematics 142*, 1995, 443–551.
[7]. Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation, 48(177)*, 1987, 203–209.
[8]. Victor S. Miller. Use of elliptic curves in crypyography. *Lecture notes in computer sciences; 218 on Advances in cryptology—CRYPTO 85*, 1985, 417–426.
[9]. *The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standards Institute, 2005.
[10]. *Suite B Implementer's Guide to FIPS 186-3* (ECDSA), 2010.
[11]. Scott Vanstone Don Johnson, Alfred Menezes. *The elliptic curve digital signature algorithm (ecdsa)*. Certicom Office Locations 25801 Industrial Blvd. Hayward, 2001.
[12]. Amar SiadMoncef Amara. *Elliptic curve cryptography and its applications*. IEEE Computer Society, editor, 7th International Workshop on Systems, Signal Processing and their Applications (WOSSPA), 978-1-4577-0690-5/11, 2011.
[13]. Yong Ki Lee. Elliptic-curve-based security processor for rfid. *IEEE Transactions On Computers, 57(11)*, 2008, 1514–1527.
[14]. Kamlesh Gupta. *An ethical way for image encryption using ecc*. IEEE Computer Society, editor, First International Conference on Computational Intelligence, Communication Systems and Networks, 978-0-7695-3743-6/09, 2009,342–345.
[15]. Anita JadhavMeghaKolhekar. Implementation of elliptic curve cryptography on text and image. *International Journal of Enterprise Computing and Business Systems, 1(2)*, 2011.
[16]. S. Sathyanarayana. Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points. *International Journal of Network Security, 12(3)*, 2011, 137–150.
[17]. K. MuneeswaranMariaCelestin Vigila. Nonce based elliptic curve cryptosystem for text and image applications. *International Journal of Network Security, 14(4)*, 2012, 236–242.
[18]. Sanjay SilakariKamlesh Gupta. Efficient hybrid image cryptosystem using ecc and chaotic map. *International Journal of Computer Applications, 29(3)*, 2011.
[19]. XiamuNiu Li Li, Ahmed A. Abd El-Latif. *Elliptic curve elgamal based homomorphic image encryption scheme for sharing secret images*. ElSevierSignalProcessing(92), 2012, 1069–1078.
[20]. Antonio Rosales G. Números trascendentes: Desarrollo histórico. *Revista digital Matemática, Educación e Internet , 10(2)*, 2010.
[21]. Anita JadhavMeghaKolhekar. Implementation of elliptic curve cryptography on text and image. *International Journal of Enterprise Computing and Business Systems, 1(2)*, 2011.
[22]. Lawrence C.Washington. *Elliptic Curves Number Theory and Cryptography*. Discrete Mathematics and its Applications. Chapman and Hall/CRC, University of Maryland College Park, Maryland, U.S.A., 2 edition, 2008.
[23]. René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation, 44(170)*, 1985, 483–494.
[24]. Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge UniversityPress., 2 edition, 2008.
[25]. Jos'e de Jesús Angel. *Criptografía y curvas elípticas*. Master'sthesis, Universidad Autonoma Metropolitana, 1998.
[26]. William Steain. *An Explicit Approach To Elementary Number Theory (With An Emphasis On Elliptic Curves)*. Math 124. 2001.
[27]. M. Qu-S. Vanstone J. Koeller, A. Menezes. *Elliptic curve systems*. Draft 8. IEEE P1363 Standard for RSA, Diffie-Hellman and Related Public-Key Cryptography, 1996.
[28]. *Recommended Elliptic Curves for Federal Government Use*, 1999.
[29]. M. Anwar HasanBijan Ansari. High-performance architecture of elliptic curve scalar multiplication. *IEEE Transactions On Computers, 57(11)*, 2008, 1443–1453.
[30]. N. Saqib Francisco Rodríguez Henríquez. *Cryptographic Algorithms on Reconfigurable Hardware*. Springer Series on Signals and Communication Tecnology. 2006.
[31]. Ding Yong. Speeding scalar multiplication of elliptic curve over gf(2mn). *InternationalJournal of Network Security, 11(2)*, 2010, 70–77.