American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Combine and Multilevel Implementation of Cryptographic and Data Hiding Algorithms to Provide a Hybrid Data-Security Scheme

Syed Muhammad Jamil Shah[a*], Prof. Qamar ul Islam[b]

[a,b]*Department of Electrical Engineering, Institute of Space Technology (IST), Islamabad, Pakistan.*
[a]*Email: Jamilsyed90@gmail.com,* [b]*Email: qamar.islam@ist.edu.pk*

Abstract

It is generally accepted that data encryption is the key role in current and future technologies for information security. Cryptography plays an important task in accomplishing information security. Elliptic Curve Cryptography (ECC) is considered as more suitable for limited resources applications such as RFID, and for Chip based Systems such as modern day Pervasive and ubiquitous Computing Communication Systems, than other public key cryptography algorithms because of its small key size. Generally, a random generator is used to produce. ECC domain parameters. Here in this work, we have proposed "Combine and Multilevel Implementation of AES & ECC along with Steganography to provide a Hybrid Cryptographic Security technic in Data communication Systems. Which will help in development of an algorithm to secure the data of users (both Wired and Wireless/Satellite Communication) in complex manner with more security and accuracy by implementing multilevel and hybrid scheme of AES and ECC encryption algorithms along with Steganography. The design is implemented using the MATLAB R2012a simulations. The data is secured using the resulted public and private keys (generated by ECC in combination with (AES) encryption and decryption process) along with the technic of steganography for hiding this encrypted data in a fake message or Image to provide the strong cryptographic solution for highly secured data communication systems. It is tested over plain text and image with multiple data sizes. Furthermore, in order to elaborate the effectiveness of the proposed scheme, we provided a comprehensive performance analysis (evaluation) of the approach: hybrid implementation of symmetric and asymmetric key cryptographic algorithms w.r.t these parameters: time elapsed, data sizes, key sizes (variance of Key Space) and impact of steganography.

Keywords: Cryptography; Steganography; Hybrid approach of AES and ECC; Symmetric Key; Asymmetric Key; Public Key; Private Key; Hybrid Cryptographic Security.

---

* Corresponding author.

1. Introduction

In the current time, when the Internet provides essential communication between millions of people and is being increasingly used as a tool for ecommerce, security becomes a tremendously important issue to deal with Internet is often used to upload web pages and other documents from a private development machine to public webhosting servers. Transfer of files like banking transactions e-shopping, tenders etc. need special authenticated mechanism.

1.1. Cryptography

It is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from the casual reader and only the intended recipient will be able to convert it into original text. Cryptography is a technique of hiding the plain information from the web. By using cryptography we can assist this shaky information by secrete writing on our computer network. Cryptography renders the message unintelligible to outsider by various transformations. Data Cryptography is the scrambling of the content of data like text, image, audio and video to make it unreadable or unintelligible during transmission. Its main goal is to keep the data secure from unauthorized access. As communications and transmission of files over internet has increased exponentially since last few years, there is need of security in such file transfer. One of the solutions to secure communication is cryptography. It is the process of converting plain text into encrypted text and decrypt cipher text to plain text at other end. In a distrusted medium cryptography becomes essential part of secure communication.

There are two types of cryptographic algorithm to accomplish these goals [2]:

1. Symmetric cryptography,
2. Asymmetric cryptography.

The initial unencrypted data is referred as normal text. It is encrypted into cipher text with a cryptographic algorithm, which will in turn be decrypted into usable plaintext.

Symmetric-Key Cryptography: In traditional (symmetric-key) cryptography, the sender and receiver of a message know and use the same secret key. The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. Because all keys in a secret-key (symmetric-key) cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management. In symmetric cryptography single key is used for encryption and decryption e.g. Data Encryption Standard (DES) and Advanced Encryption Standards (AES).

a) Advance Encryption Standard (AES):

AES, is a well-known Symmetric Key Cryptosystem technique. Which is also referred as the Private Key Encryption Standard, which was first introduced by NIST in 2001. It is a technique or Cryptosystem where the sender and receiver share the same secret key, which is used to perform both encryption and decryption works. It converts the **Plain Text Message** into **Cipher Text Message**: which is the combination of Plain Text Message and the Secret Key on the Sender side, this is called AES Encryption. While, at the Receiver side, the Cipher text is deciphered into plain text using the same secret key, called as AES Decryption. Among all types of Symmetric Key Cryptosystems, Advanced Encryption System (AES) is the most popular and being widely used Cryptographic Scheme in various applications for maintaining security due to its better security and efficiency features. Since the introduction of Public Key Cryptosystems, still it has its own space in the information security, specifically, when the information is to be shared between two parties.

A-Symmetric-Key Cryptography: Since the Symmetric-Key Cryptography had issues to provide the Secure Key Management due to the fact that Secret Keys on both ends must be same. To solve the key management problem, A-Symmetric-Key Cryptography method was introduced. Whitfield Diffie and Martin Hellman introduced the concept of public-key cryptography in 1976[1]. Public-key cryptography refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are mathematically linked. The algorithms used for public key cryptography are based on mathematical relationships (the ones being the integer factorization and discrete logarithm problems).Although it is easy for the recipient to generate the public and private keys, to decrypt the message using the private key, and easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to derive the private key, based only on their knowledge of the public key. This is why, unlike symmetric key algorithms, a public key algorithm does not require a secure initial exchange of one (or more) secret keys between the sender and receiver. In practice, only a hash of the message is typically encrypted for signature verification purposes. Public-key cryptography is a fundamental, important, and widely used technology. It is an approach used by many cryptographic algorithms and cryptosystems. In Asymmetric algorithm different keys are used to encrypt and decrypt the data e.g. RSA and Elliptic Curve Cryptography.

b) Elliptic Curve Cryptosystem (ECC):

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz [3] as an alternative mechanism for implementing public key cryptography. Elliptic curve cryptography (ECC) can provide the same level and type of security as RSA but with much shorter keys. Elliptic curve cryptography **(**ECC**)** is an approach of public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Advantage of Elliptic curve cryptography is the public key and private keys have smaller size. The computation is fast as compared to other method and also it needs less storage space. Whereas the drawback of EC curves generation is complex, and difficult to implement a sustainable ECC algorithm. However, implementers can rely on third parties for curves, which can be validated. Since ECC (Elliptic Curve cryptography) is kind of public key cryptography like RSA. But it differ from RSA in its quicker evolving capacity and by providing attractive way to researchers of cryptography algorithm. The security level which is given by RSA can provider even with smaller keys of ECC. For example the 1024 bit security of RSA could be offered by 163 bit security strength of ECC. And it is well suited for wireless communications.

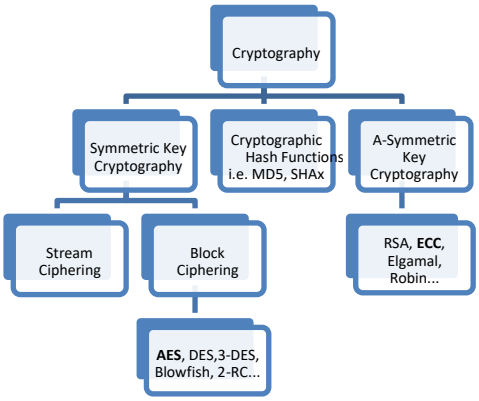

Figure 1: classification of Cryptographic schemes

Due to the fact that AES is still considered to be the most reliable and secure Private Key Data Encryption scheme; while ECC uses small key sizes as compared to other Public Key Cryptosystems, being more suitable for the limited resource applications and for Chip based Systems such as modern day Pervasive and ubiquitous Computing Communication Systems.

1.2. Steganography- Data Hiding

Steganography is the science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. The main goal of steganography is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot detect the presence of m in d'. On the other hand the goal of watermarking is to hide a message m in some audio or video (cover) data d, to obtain new data d', practically indistinguishable from d, by people, in such a way that an eavesdropper cannot remove or replace m in d'. Differences between steganography and watermarking are both subtle and essential. Shortly, one can say that watermarking is about protecting the content of messages, steganography is about concealing its very existence. Steganography methods usually do not need to provide strong security against removing or modification of the hidden message. Watermarking methods need to be very robust to attempts to remove or modify a hidden message. The proposed method (Hybrid implementation of ECC with AES) can make the steganography more and more strong by encrypting the hidden message (to be sent in fake message).

2. Proposed Work: Combine and Multilevel Implementation of AES & ECC along with Steganography

Here in this work, Firstly, I have worked to develop a hybrid Cryptographic Scheme “Combine Implementation of AES & ECC to provide a strong cryptosystem in Data communication Systems. Which will help in development of an algorithm to encrypt the data of users (both Wired and Wireless/Satellite Communication) in complex manner with more security and accuracy by implementing multilevel and hybrid scheme of AES and ECC algorithms. The resulted private keys were tested by using them for plain text message encryption and decryption to provide the strong cryptographic solution. Then Secondly, The proposed method (Hybrid implementation of ECC with AES) is used with the Steganography to encrypt the hidden message (to be sent in

fake message) can make the steganography more and more strong. The same is also implemented for the variety of user data like an image. In satellite communication where the links are long and prone to variety of intruders and hackers to steal the satellite imagery before it is being received by the ultimate but authentic Receiver of that message.

2.1. A Hybrid Scheme of AES and ECC

Here in this work, we have proposed a "Combined and Multilevel Implementation of AES & ECC to provide a Hybrid Cryptographic Security in Data communication Systems. Which will help in development of an algorithm to encrypt the data of users (both Wired and Wireless/Satellite Communication) in complex manner with more security and accuracy by implementing multilevel and hybrid scheme of AES and ECC algorithms. Hybrid Scheme means the combine implementation of AES (Symmetric Key Encryption Scheme) with the ECC (A-Symmetric Key Encryption Scheme) to provide the strong encryption and decryption standards while using the benefits of both cryptographic schemes to develop a novel Cryptographic System. Thereby, increasing overall security of the system by implementing both the Symmetric and A-Symmetric Keys Cryptographic systems in a single System Model. Since here I used ECC, to encrypt and transfer the Private keys as AES Private Keys, while AES encrypts the plain text (communication data). So, ECC Provides the efficient Key Management mechanism in the beginning of session establishment for the communication process to be starting on, hence the AES key that is encrypted by ECC and transmitted for data communication, there is no need to send private secret key before communication. Multilevel Implementation refers to the No. of Passes to generate the keys. Like here we are giving 3 passes to generate the strong and complex keys for data encryption.

The design is implemented using the MATLAB R2012a simulations. The resulted public and private keys (generated by ECC) in combination with (AES) encryption and decryption process are tested - over plain text and image (with multiple data sizes) – to provide the strong cryptographic solution for highly secured data communication systems. Furthermore, in order to elaborate the effectiveness of the proposed scheme, we provided a comprehensive performance analysis (evaluation) of the approach: hybrid implementation of symmetric and asymmetric key cryptographic algorithms w.r.t these parameters: time elapsed, block size and key size (variance of Key Space). Multilevel Implementation to generate strong keys. Multilevel Implementation refers to the No. of Passes to generate the keys. Like here we are giving 3 passes to generate the strong and complex keys for data encryption. Hybrid Scheme means the combine implementation of AES (Symmetric Key Encryption Scheme) for the Message Encryption with the ECC (A-Symmetric Key Encryption Scheme) for the Secure Key Management mechanism, which is then used along with data hiding scheme "steganography" to provide the strong encryption and decryption standards while using the benefits of both cryptographic schemes. With this hybridization of Cryptographic and Data hiding Algorithms a strong Hybrid Data-Security Scheme may be developed, which in turn enhances the effectiveness of steganography in data security.

2.2. Proposed Work Flow

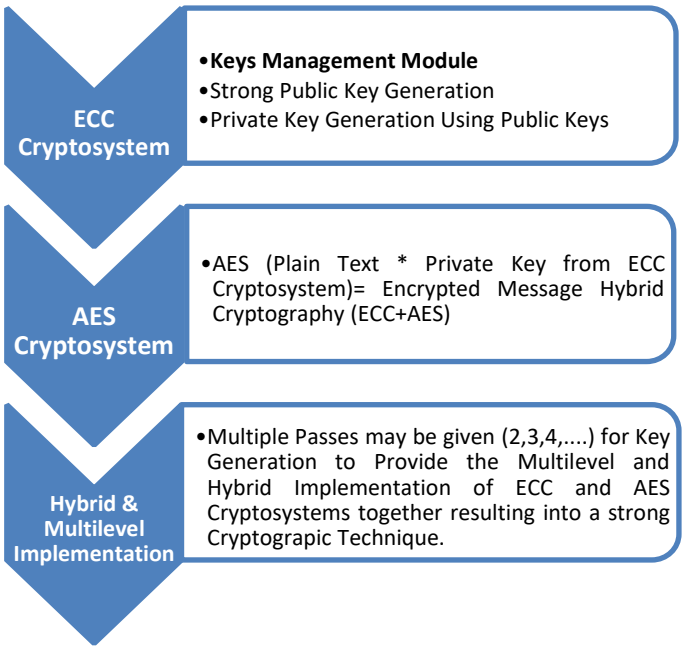

Figure 2: Proposed Work Flow Diagram

3. Proposed Work: Combine and Multilevel Implementation of AES & ECC along with Steganography

Elliptic Curves can be generated by using the following random numbers generation methods over the Galois field mathematics [2]:

a) Elliptic Curves over Real Numbers
b) Elliptic Curves over GF (p)
c) Elliptic Curves over GF (2^n)

The Elliptic curves generalized equation can be given as following:

$$y^2+b_1xy+b_2y=x^3+a_1x^2+ a_2x +a_3 \qquad (1)$$

Here in our work, we use the Galois Functions [3] for random numbers generation to produce the Public Keys and further the Private keys generation for the cryptography.

2) Elliptic Curves over GF (p)
3) Elliptic Curves over GF (2^n)

Following eq. explains the Elliptic curves over real numbers:

$$y^2+xy=x^3+ax^2+b \qquad (2)$$

A Primitive Polynomial [3,4] Is Used to Define the Finite Field because such functions define the finite fields

GF (2m).Condition of Primitive Polynomial is: An irreducible polynomial f(X) of degree m is said to be primitive if the smallest positive integer n for which f(X) divides X n + 1, is n = 2m- 1.

4) Mathematical Model using LFSR Circuit.

LFSR Circuit may be used to demonstrate the mapping of field elements in terms of basis elements, described by following Equation [3]:

$$\alpha^i = a_i(X) = a_{i,0} + a_{i,1}X + a_{i,2}X^2 + \ldots + a_{i,m-1}X^{m-1} \qquad (2)$$

3.1. Proposed Linear feedback shift register (LFSR) circuit

In my work, since the message is of the order of m=8, so following Primitive Polynomial is used [3]:

$$1 + X^2 + X^3 + X^4 + X^8 \qquad (3)$$

Pseudocode for finding points on an elliptic curve

```
ellipticCurve_points (p, a, b)                    // p is the modulus
{
   x ← 0
   while (x < p)
   {
        w ← (x^3 + ax + b) mod p                  // w is y^2
        if (w is a perfect square in Z_p) output (x, √w) (x, −√w)
        x ← x + 1
   {
}
```

To demonstrate the mapping of field elements in terms of basis elements, described by Equation (3) following linear feedback shift register (LFSR) circuit, can be used.

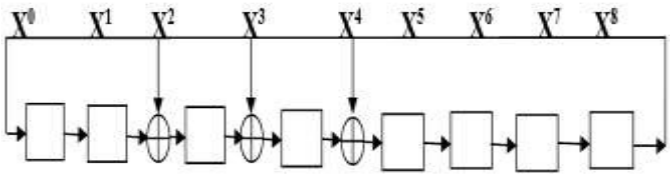

Figure 3: LFSR circuit for m=8

The circuit generates (with m = 8) the $2^m - 1$ nonzero elements of the field, and summarizes the findings into a 8x256 matrix of Mapping field elements in terms of basis elements for GF(256) with the following:

$$F(x) = 1 + X^2 + X^3 + X^4 + X^8 \qquad (4)$$

3.2. Work Flow Model

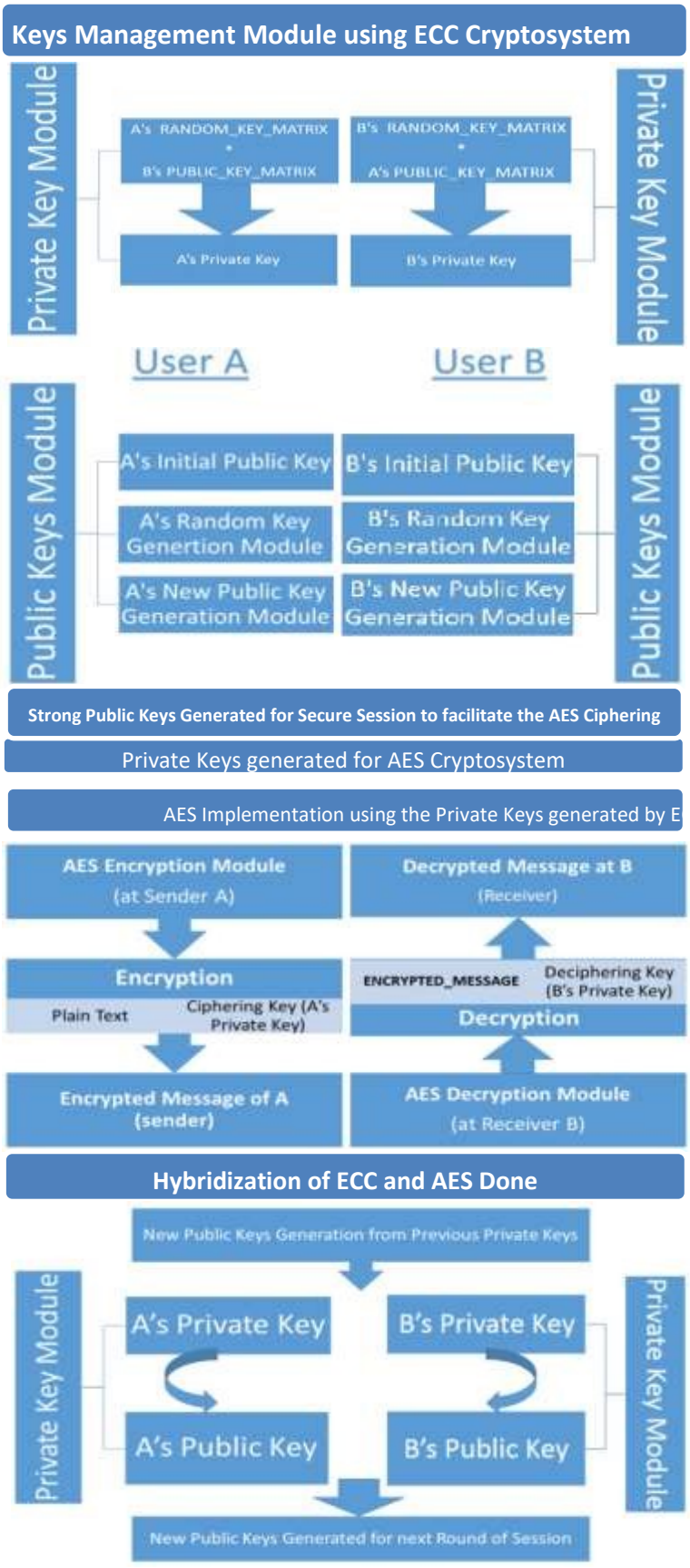

Figure 4: Work Flow diagram of Hybrid and Multilevel Crypto System Implementation Model

3.3. Results

Here in figures 5 (a, b and c), respectively for the passes 1, 2 and 3; the Random Points generated at each pass are shown, with reference to each pass: As described earlier that the generation of these (random) points will be accomplished using elliptic curve and LFSR method. Figure below is showing the result of both methods, in the left hand side of the figure we generates random points using the algorithm pseudo code given above, The random points against the equation $\mathbf{y^2 = x^3 + x + 1}$ using modulo 13 and by using the above algorithm will be as can be seen in figure below;

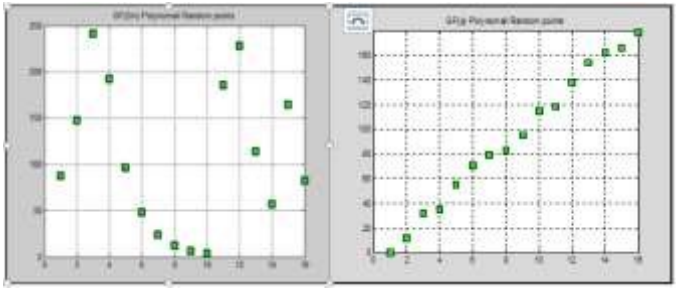

Figure 5: (a)

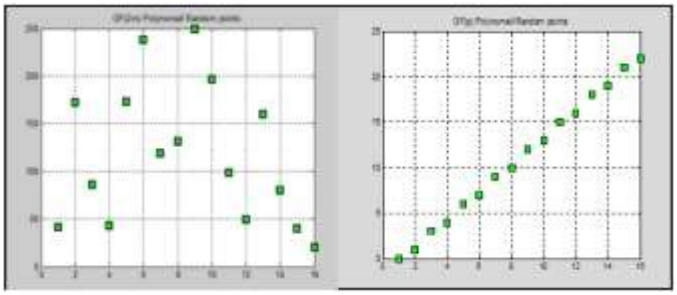

Figure 5: (b)

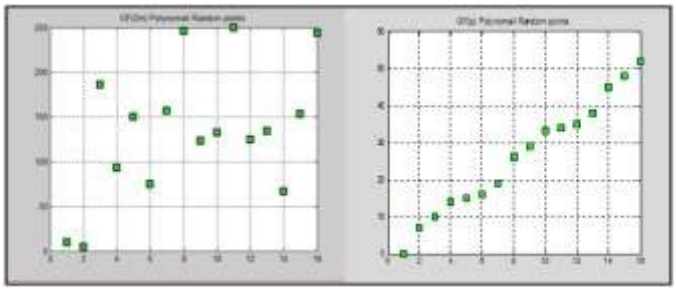

Figure 5: (c)

The random points upon the right hand side of the graph can be generated simply by LFSR by inserting initially some random values in the shift registers and then by performing cyclic shifts (to generate another random value).

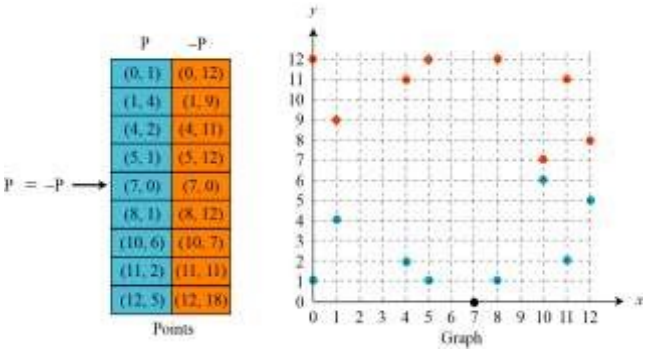

Figure 6: Random Points Generation [3]

3.4. Implementation of Proposed Hybrid Cryptosystem along with Steganography.

If the 6-bit version is displayed as an 8-bit image then the 8-bit pixels all have zeros in the lower 2 bits:

B	b	b	b	b	b	0	0

Where b=0 or 1,

This introduces the possibility of encoding other information in the low-order bits. Perhaps that other information could be a message, perhaps encrypted, or even another image.

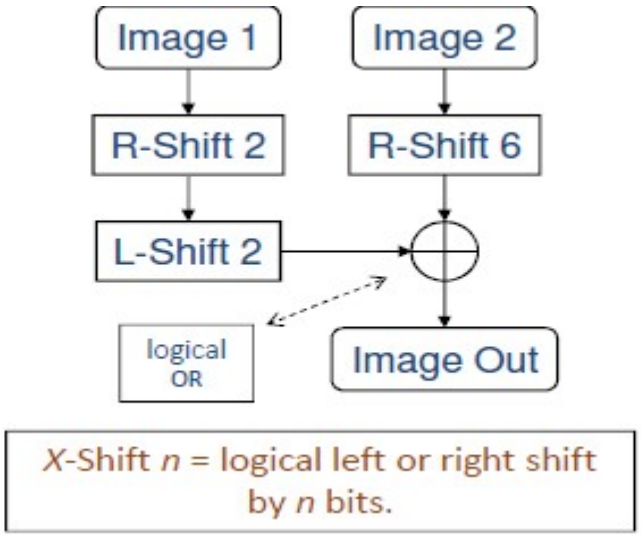

Figure 7: Steganography Algorithm

3.4.1. Results

The paractical implementation can be depicted by the following:

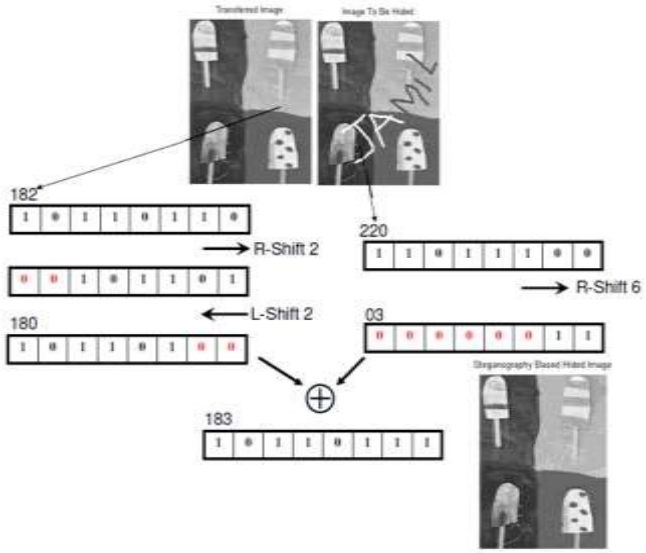

Figure 8

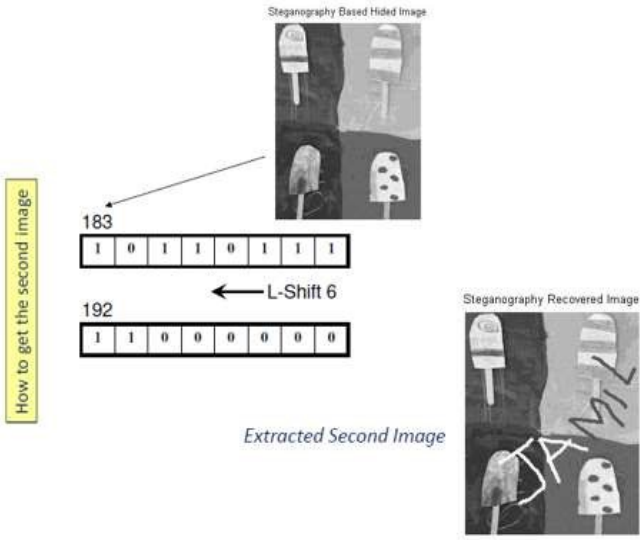

Figure 9

Since the authorized recipients can quickly retrieve the hidden information in the received image, however, the unauthenticated user can try multiple combinations to recover the hidden information. But it's not guaranteed that the hidden information can be secured through steganography alone. So we introduced the above proposed strong hybrid cryptosystem (Hybrid of ECC and AES) to secure the hidden information (steganography) with more quick format where we need to encrypt the only those contents (bits) of data which need to be hidden in the transferred (fake) image. Whereas, if we encrypt the whole 8 bit data, it will take even more time to be read by the unauthorized user.

In fig. 8, we will be replacing the image to be hidden (actual message) with its encrypted version as it can be seen in the following figure 10.

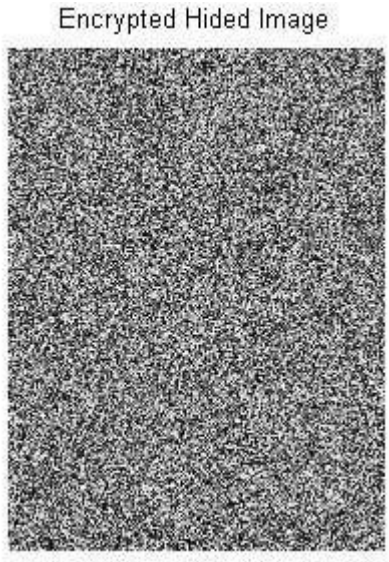

Figure 10

Here despite of trying multiple combinations, one can never be able to retrieve the actual data content, unless he doesn't have the encryption key values. In the proposed scheme even the users at the transmitting & receiving end don't know about the key contents used for the data security as they are completely relying upon the system generated keys (handshaking of Tx. and Rx.). In turn, this makes the security even stronger while using the proposed three levels cryptosystem (ECC + AES + Steganography).

4. Performance Analysis and Evaluation

In order to elaborate the effectiveness of the proposed scheme, we provided a comprehensive performance analysis (evaluation) of the approach: hybrid implementation of symmetric and asymmetric key cryptographic algorithms w.r.t these parameters: time elapsed, block size and key size (variance of Key Space). Here in table 1, a comparison on the bases of time elapsed and throughputs for the variety of data samples i.e. Text data and Image data of equal data sizes, on same key sizes is showing the performance of the proposed Hybrid scheme of AES and ECC to provide a strong cryptosystem for the limited resources appliances and to facilitate the more secure communication systems for the variety of user's data.

Table 1

Table 1Parameters	**Results**	
Passes	3	3
Data Type	Text	.jpeg Image
Data Size	16 Bytes	16 KBs
Key Size	16 Bytes	16 Bytes
Time elapsed (Avg.)	3.143360 seconds	2470.955246 seconds
Throughput	4.77196375	0.08845726044

4.1. Simulation Results for Text and Image (Data Types)

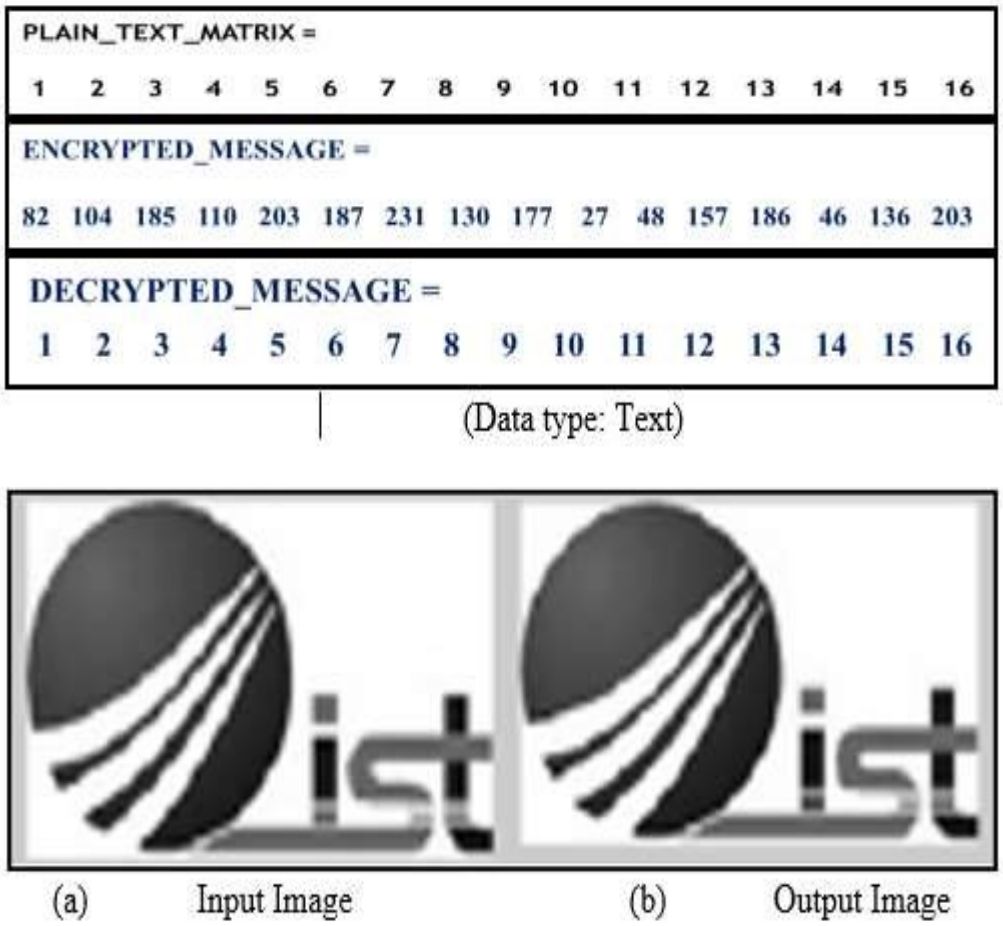

Figure 11

4.2. Comparative Analysis of AES and Hybrid ECC&AES

Table 2

Parameters	**Results**		
Cryptosystem	AES alone	Hybrid ECC & AES [GF(2^8)]	Hybrid ECC & AES [GF(2^{23}]
Data Type	Text	Text	Text
Data Size (KBs)	15	15	15
Key Size (Bytes)	16	16	16
Time elapsed (Pass1)	2.752671	2.581398	2.736882
Time elapsed (Pass2)	2.552671	2.518858	10.671419
Time elapsed (Pass3)	2.270000	2.346202	28.358687
Throughput (KB/s)	5.940325863	6.043141585	1.0774059

Table 3

Table 3Parameters	**Results**	
Cryptosystem	AES alone	Hybrid ECC AES &
Data Type	image	image
Data Size (KBs)	15	15
Key Size (Bytes)	16	16
Time elapsed (Pass1)	2477.633642	2479.368444
Time elapsed (Pass2)	2585.531310	2446.371118
Time elapsed (Pass3)	2591.633310	2487.126176
Throughput (KB/s)	0.005878666	0.006070527

As can be seen from the tables above that when we move towards longer polynomial of the Galois field the time consumption increased because of modular operation over long integers (generated by polynomial circuit) in order to make it 8-bits compatible.

A similar situation occurs when we explore random points (for key generation) over elliptic curves with large Prime numbers P. It takes too much time to converge when the algorithm start calculations for perfect square. As we move in subsequent rounds (passes) the Prime number P gets larger and larger while making key calculation lengthier.

Having these type of situations when the algorithm takes more time for key generation the security level also increases in a similar fashion.

4.3. Effectiveness of Steganography along with *the Hybrid of ECC &AES*

While encrypting an 8 bit image (ref. fig. 11(a) & (b)) it takes too much time as compared to the proposed scheme (using the steganography along with the hybrid cryptosystem of ECC &AES), since it picks only few bits of data for encryption, which makes the cryptosystem to work in a more efficient way for data security.

Furthermore, it also depicts that the information is not secured for an unauthorized user by distributing the salt and paper noise over the transferred (fake) image as hidden contents are strongly encrypted and showing the water mark of noise over the transferred image. So, with the help of the proposed “Combine and Multilevel Implementation of Cryptographic and Data hiding Algorithms” one can provide a Hybrid Data-Security Scheme with 3 levels of a security system which becomes complex to be broken.

4.4. Constraints & Limitations of the scheme

1. While generating random points for enhancing key strength if we implement this module in some hard

ware (dedicated for on-board processing of data in satellites) like FPGA we can efficiently develop a very fast algorithm but it also consumes more and more hardware resources at the end.

2. Using Elliptic Curve Cryptography we needs at least two passes of satellites to successfully exchange the keys and useful information (encrypted data) because the data transfer rate at up-link channel cannot exceeds from few kbps whereas the satellite pass exists for few minutes in which the second session cannot be initiated.
3. Steganography has the advantage in securing information but we need more dummy images in which we will be hiding the actual information. Hiding information in a single dummy data could indicated the presence of Steganography in data transmission.
4. Sometime the random point's generation could cause more time consumption which purely depends upon the algorithm used for the task. While consuming more time could cause the loss of satellite pass while key exchange scenario.

5. Conclusion and Future work

The proposed method (Hybrid implementation of ECC with AES) along with the steganography may ensure that the data is secured using the public and private keys (generated by ECC in combination with (AES) encryption and decryption process) along with the technique of data hiding (steganography) which actually provides the strong cryptographic solution for the systems which requires high security measures in the data communication. Further, the proposed scheme is tested and comprehensive performance analysis (evaluation) is done over plain text and image with multiple data sizes and formats to elaborate the effectiveness of the proposed scheme. The simulation of above algorithm was carried out in MATLAB however these scenarios need to be tested over different embedded systems in order to evaluate the performance for real time applications. Moreover, the proposed scheme can be used for Audio/Video or any other data sets in future to check the complexity and performance parameters for variety of data and applications.

References

[1] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644–654, Nov 1976.

[2] Forouzan Behrouz "Cryptography & Network Security",McGraw-Hill Forouzan Networking , 2007.

[3] Neal Koblitz "Elliptic curve cryptosystems", Mathematics of Computation /American Mathematical Society, 203-209, 1987. V.S. Miller "Use of elliptic curves in cryptography". In CRYPTO'85: Proceedings of Crypto, 417- 426, Springer, 1985.

[4] M. Alimohammadi, and A. A. Pouyan, "Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET", International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014, ISSN 2229-5518

[5] Nadeem, A., Javed, M.Y., 2005 "A Performance Comparison of Data Encryption Algorithms," IEEE, Information and Communication Technologies, ICICT, First International Conference, pp. 84- 89.

[6] D. S. Abdul, Elminaam, H. M. Abdul Kader and M. M. Hadhoud, 2009 "Performance Evaluation of Symmetric Encryption Algorithms" Communications of the IBIMA Volume 8, ISSN: 1943-7765.

[7] Practical Evaluation of Hybrid Cryptosystems Ijaz Ali Shoukat1,2, Abdullah Al-Dhelaan1, Mznah AlRodhaan1, Kamalrulnizam Abu Bakar2, Subariah Ibrahim2.

[8] H. Tange and B. Andersen, "Attacks and Countermeasures on AES and ECC," in IEEE International Symposium onWireless Personal Multimedia Communications (WPMC), pp. 1-5, Jun. 2013.