Image Encryption using Multiple Advanced Block Cipher Techniques

Pooja Prashar
Amity School of Engineering & Technology
Sector 125, Noida
Uttar Pradesh, India

Shivanku Mahna
San Jose State University
1 Washington Sq
San Jose, CA, 95192

ABSTRACT
The technology dependent world we live in is producing information in abundance at an unparallel rate, so much so that it is extremely hard for us to keep the information secured and risk free anymore. With every passing day, the means and methods of breaking in being used by hackers are advancing and hence, there is an urgent need to upgrade the security systems currently in place and protect our data. In order to avoid the threats and risks of vital data to a certain point, several encryption algorithms have been used or have evolved over the recent time. Through this paper, we are proposing a digital image encryption technique, which can increase the security of a digital image by many folds with the help of using a combination of DES algorithm and elliptic curve cryptosystem. As a result of this, we made the data to be more secure and were able to retain the confidentiality and privacy much better as compared to using only a vanilla flavor of DES algorithm. Also the fact that the key being used in DES algorithm is being generated using a chaotic key generator, which is being guided with the help of Henon map, makes a big difference in the performance side of the things of the algorithm.

General Terms
Authentication, Cryptography, DES, ECC, Chaos, Henon Heat Map.

Keywords
DES, ECG.

1. INTRODUCTION
The world we live in is advancing every second and with it is advancing the technology we use or are surrounded by. From the car we drive to the laptop we use, everything is developing at such a fast pace that is almost impossible for anyone to keep up with the changes happening around them. And one of such sectors is the data security sector. With so much of advancement happening in every sector, the data is being consumed and produced at very alarming rate. We live in an era, where it is extremely useful and necessary to constitute information about every premise of our lives and while doing so, we are producing data. It is extremely important to make sure the valuable information is being secured from the threats and risks which one faces. Hence the large chunks of data being produced by our daily activities, not only need to be stored in an efficient manner, but also need to be guarded against the evil minds, who might want to hack into our data and use it for illicit activities. Therefore therein lies an extreme need to have top notch data security algorithms so that our precious data is safe against the data breaching efforts of hacker. This problem of information security is not just applicable to individuals but also to large organizations like ones dealing in banking sector, where even a minor information leak can cause loss of billions of dollars. Hence it cannot only be described as a property, but also or an asset which is extremely pivotal to an organization and all the possible steps need to be taken by an organization in trying to outsmart the hackers. The increment in the data in any field is directly proportional to the threats involved. So, in order to be secured, it is mandatory that information should be protected from unconstitutional access or change and should be accessible only to people having approved access. Important and sensitive information such as account numbers, images related to medical sciences, national budget and other corporate related data, should receive the best possible and most robust protection from the threats present. And one of the ways of protecting the data has been using cryptography algorithms like AES, DES, IDEA. There have been a lot of algorithms over the time which has been quite successful in guarding our data against the threats like AES, DES, IDEA etc. But as the technology has developed, so has the brute force methods of the hackers, who use extremely sophisticated and advanced methods of attacks, which exploit the loopholes in the current cryptographic algorithms and help them in accessing or confidential data, compromising our data integrity and privacy. Thus, we need to take some preventive measures and think of ways in which we can make our current set of algorithms even more secure. And one of those is suggested by us in this paper in the sections to follow. We have tried making a digital image more secure and cryptic, by using DES algorithm and planting the resultant set in the form of a elliptic curve. The outstanding point in the application of the algorithm lies in the fact that the key being used for the application of DES is being determined by a chaotic key generator, which is itself working on the basis of Henon map, thus making this a very advanced version of DES algorithm and making it super secure. The implementation of the algorithm is shown in the sections below [1].

2. ALGORITHMS BEING USED
We have used a combination of DES and ECC algorithm, along with keys being generated with the help of Henon map.

2.1 DES
DES is symmetric data encryption algorithm, which is used for encrypting and decrypting data using multiple rounds of permutation and substitution on a data set, so that the resultant data after a total of 16 rounds, is unrecognizable and has no patterns or common trail in it, which can help in recovering or deciphering the data in any way. DES divided the whole data set into blocks of 64 bit data and uses a key, which is of 56 bit for transforming the regular data into cipher text. The key, using which the data was encrypted, is the same and the only key using which it can be decrypted. No other key can help in decrypting the data in any way [3].

The algorithm functions in the following way:-

- It divides the data into 64 bit data block by applying an initial permutation on the data and makes a key 48 bit long by applying a similar initial permutation on it.
- Every 64 bit data block is then divided into a 32 bit left half block and a 32 bit right half block.
- Function 'f' is calculated, in which the 32 bit right block of the data is converted into a 48 bit data using expansion box.
- This 48 bit data is XOR with the 48-bit key which was selected and the resultant is passed through 8 S-Box manipulations. Each S-Box translates the 6 bt input into 4 bit output.
- Then the output is XOR with the initial left half L0 to obtain the new right half R1. The original right half, R0, becomes the new left half L1.
- The above steps are repeated 16 times and after the 16th iteration, the right (R16) and left (L16) halves are concatenated and an inverse permutation is applied on the resultant set to complete the encryption process [3].

2.2 Elliptic Curve Cryptosystem (ECC)

Elliptic Curve Cryptography is a robust alterative to the popular public key cryptography algorithms like RSA. It was discovered by IBM in 1985. Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Unlike other popular algorithms, ECC is based on discrete algorithms which consist of cubic equation of two variables, that is much more difficult to challenge or break at equivalent key lengths [4].

The standard equation of an elliptic curve to calculate the length of a curve in terms of circumference of the eclipse is:

$$q^2 + b_1pq + b_2q = p^3 + a_1p^2 + a_2p + a_3 \quad (1)$$

Elliptical curves consisting of real numbers can be represented using a special class of elliptic equations of the form:

$$q^2 = p^3 + ap + b \quad (2)$$

Where, a and b can be either rational numbers, complex numbers or integers which are divisible by mod n. The above equation always represents a singular elliptic curve except in the case where $4a^3 + 27b^2 \neq 0$, where it represents a non-singular version of the elliptic curve. A singular curve doesn't necessarily have three distinct roots for the equation $x^3 + ax + b = 0$ whereas a nonsingular elliptic curves always has three distinct roots. Variable 'q' has a degree of 2 while 'p' has a degree of 3. It means that a horizontal line can intersects the curve in three points if all the roots are real. However, a vertical line can intersects the curve at most in two points. Using these concepts as the basis of our DES algorithm manipulation, we have proposed an even secure and safe method of cryptography that can be applied on the digital image's protection [4].

2.3 Henon Map

In 1976, Michael Henon projected the Henon Map. Henon Map can be described as the simplified two-dimensional demonstrating chaotic behavior. Henon Map can also be signified with the help of an attractor and is also described as Lorenz equation of Poincare section. Cipher Key is generated by Henon Map which exhibits random sequence. This generation is responsible for encrypting the image that is shuffled or simple in manner [2]. The chaotic behavior is dependent on certain components which can be described as parameters of initial system and conditions. The equation of Henon Map generally maps X_b, Y_b to a new point X_{b+1}, Y_{b+1} is signified below:

$$X_{b+1} = Y_b + 1 - uX_b^2 \quad (3)$$
$$Y_{b+1} = vX_b$$

X_0, Y_0 which is the initial value is replaced by X_1, Y_1 in the next recapitulation of the generation of arrangement in Henon Map. In order to confluence the arrangement, Henon attractor is used. The control parameters in the above equation are showcased as u and v. For the value of control parameters such as u=1.4 and v=0.3, the Henon map is responsible for the random arrangement with the chaotic behavior [2].

3. PROPOSED ALGORITHM FOR ENCRYPTION

Consider, N to be the original image of the particular size x*y.

3.1 Round Key Generation Algorithm

Henon Map is used to generate the 56 bit round key in order to create the random arrangement of key bits by captivating the help of initial parameters used in the equation (3). In DES, the encryption and decryption of the image is completed with the help pf same initial parameters. Generation of Round key has chaotic nature and is delivered to the encryption technique known as DES. In Henon Map equation, the minor alteration is completed by the addition of X and Y components to another range called Z in accordance to the equation (4). After the completion of addition of the components X and Y, the result generated is stored in Z [7].

$$Z = X + Y \quad (4)$$

The key so generated becomes the key which will be used for applying DES algorithm for the digital image encryption [7].

3.2 DES Encrption

The original image 'N' is divided into 64 bit blocks, which are calculated using initial permutation in DES algorithm and hence it acts like the initial input in the algorithm. Post this, the 64 bit block is divided into two equal halves, left side and right side, each containing 32 bits. Post this, the encryption process as explained in the section 2.1 of this paper is applied and after 16 rounds of processing, a final value is obtained, on which a final inverse permutation is applied and it is joined to get back a 64 bit block[6]. A similar kind of thing is done for each and every block obtained by the image and this is the way in which the digital image is encrypted using DES algorithm[6].

3.3 Elliptic Curve

When the concluding sequences of Encryption Algorithm DES are mapped to each and every points of elliptic curve, the resultant is ciphered image 'N'[5]. Ciphered image 'N' is virtually divided into blocks of 8-bit, in which the 8-bit is mapped to the distinctive point present in the elliptic curve. Elliptic curve generates points which are mapped with one to one plaintext in the algorithm. In the final encrypted image 'N', the 16-bit (8-bit for x-coordinate and 8-bit for y-coordinate) stores the equivalent points produced by the plaintext value. The final encrypted image 'N' of size 2x*y is the output generated by the image 'N' of size x*y [5].

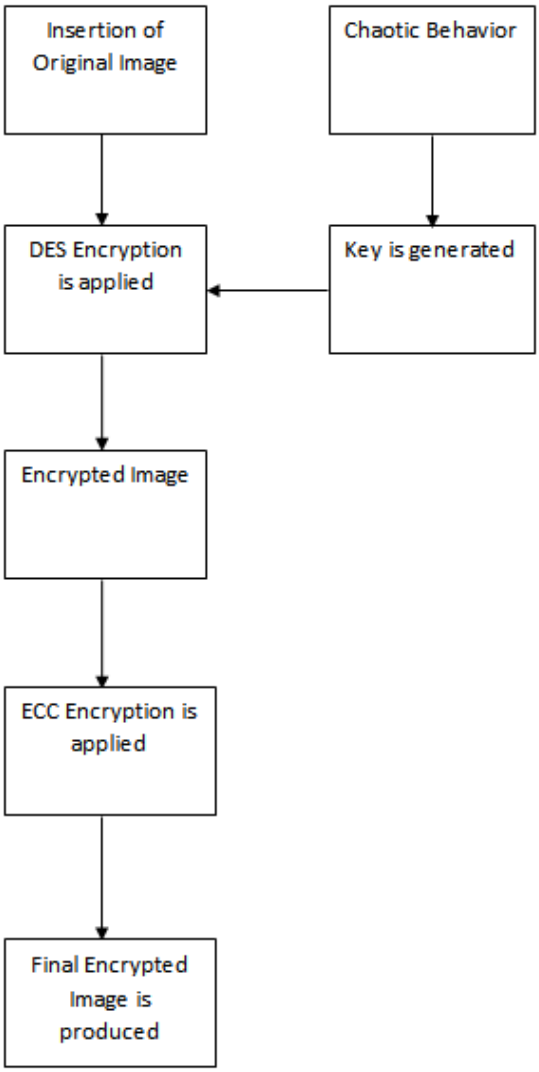

Fig 3. Encryption using DES and ECC as shown above

4. PROPOSED ALGORITHM FOR DECRYPTION

The elliptical curve had points which are recovered from the final encrypted image 'N' which has a size of 2x*y. From the equivalent recovered points, the plaintext is generated and when it is stored, it will generate an image 'P', which has the size of x*y. With the help of the same round key used in the encryption process, the resulting ciphered image is then applied to reverse DES. In DES, the input is each block of 64-bit of the ciphered image. The final output will be 64-bit plaintext on completing the 16 rounds pf processing. For the rest of the ciphered blocks remaining, the similar process should be repeated. After storing all the decrypted plaintexts which has the size of x*y, the original image is recovered [6].

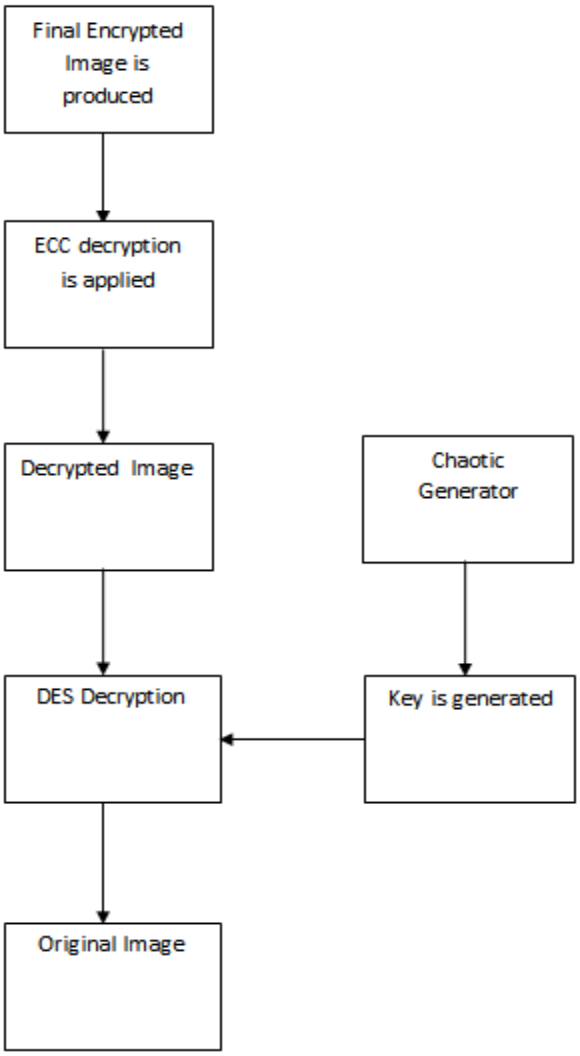

Fig 4. Decryption using ECC and DES shown above

5. RESULTS

When the famous digital image "Lena" of size 64*64 is processed under the suggested algorithm, the results obtained are as shown below in figure 4(a), 4(b), 4(c) and 4(d). is used to generate the round key of size 56-bit. The 56 bit key so generated using Henon map, was produced by using the initial values of parameters as X = 0.62, Y = 0.42, u = 2.2, and v = 0.6 using equation (3). The key so obtained as a result, shows chaotic behavior under the above parameters. MATLAB 2012a version is used for simulation. The results so obtained are that the image was encrypted in such a way that it is having supremely enhanced levels of encryption in it, which can only be undo or undone if the person gets to know the random key generated using Henon map, which is almost impossible, making the proposed solution and the algorithm very secure and efficient to use. The screenshots of the results are as shown in the figures below.

Fig 5.1 Original Image of Lena

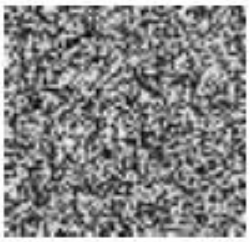

Fig 5.2 DES Encrypted Image

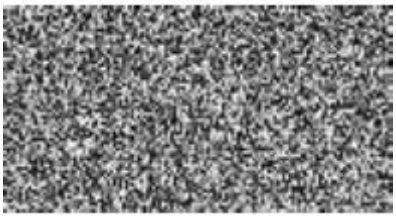

Fig 5.3 Final Encrypted Image after ECC

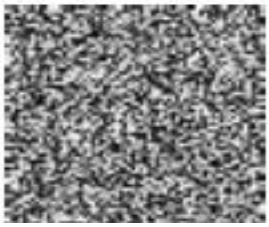

Fig 5.4 Decrypted Image post after ECC decryption

Fig 5.5 Final Decrypted Image of Lena after Decryption of DES algorithm.

6. CONCLUSION

DES is a very efficient and powerful cryptographic tool, which is very difficult to break in. However, like every other algorithm in this world, even DES has some loop holes, which if exploited, can leave our data confidentiality, integrity and its availability at the risk of being exploited by a person with malicious intentions. Hence, in an effort to make the current version of DES even more secure, a combination of DES with ECC was proposed and applied using the sample picture of Lena. As a result, the results obtained were more secure and robust as compared to the results so obtained using the vanilla version of DES. This was made possible because of use of Henon map created chaotic key in DES and because of plotting of final points so obtained in the form of an elliptic curve, the encrypted image is impossible to render back without knowing the chaotic random key. Therefore the above suggested solution makes the digital image encryption process even more secure while enhancing the complexity of algorithm and the encrypted image. The future scope of the project can be the fact that even 3D chaotic maps could have been used and implemented which might in return render results which are little more secure. But the time it takes to do the whole process still needs to be studied in detail.

7. REFERENCES

[1] Mark Stamp and Richard M. Low, "Applied Cryptanalysis: Breaking Ciphers in the Real World", Wiley-IEEE Press, 2007.

[2] Ramesh Kumar Yadava, Dr. B. K.Singh, S. K. Sinha and K. K. Pandey, "A New Approach of Colour Image Encryption Based on Henon like Chaotic Map", *Journal of Information Engineering and Applications*, vol. 3, no. 6, , pp. 14-20, 2013.

[3] Seung-Jo Han, Heang-Soo Oh and Jongan Park, "The improved data encryption standard (DES) algorithm", 1996 IEEE 4th International Symposium on Spread Spectrum Techniques and Applications Proceedings.

[4] Moncef Amara and Amar Siad, "Elliptic Curve Cryptography and its applications", International Workshop on Systems, Signal Processing and their Applications, WOSSPA, IEEE Xplore, 2011.

[5] Xianjin Fang and Yanting Wu, "Investigation into the elliptic curve cryptography", 2017, 3rd International Conference on Information Management (ICIM).

[6] Mohamed A. Seif Eldeen,Abdellatif A. Elkouny and Salwa Elramly, "DES algorithm security fortification using Elliptic Curve Cryptography",2015, Tenth International Conference on Computer Engineering & Systems (ICCES).

[7] Žarko S. Stanisavljević, "Data encryption standard visual representation", 2015, 23rd Telecommunications Forum Telfor (TELFOR).