A Hybrid Approach for Image Encryption using Different Number Iterations in ECC and AES Techniques

Divija Ameta
Computer Science Department
Techno NJR, Udaipur (Raj.)

Sandeep Upadhyay
Assistant Professor, Computer Science
Department Techno NJR, Udaipur (Raj.)

ABSTRACT
Image encryption has been emerged as the important aspect in order to protect the authenticity of the data being transferred among the different sources. Protecting the multimedia data so as to keep the integrity of the data intact has become the major concern these days. There have been several algorithms made so far. But each of them has some sort of disabilities and suffers from limitations. To overcome drawback of such algorithms we had formulated the same in the paper whose main focus is on keeping the original information secure. This paper includes the hybrid approach for implementing encryption techniques over a binary image. This work basically focus on image encryption using the derived concept of AES and ECC, once applying ECC individually on a single image and then altogether with AES with different threshold value set by user to check the accuracy on pixel intensity. The work not focuses only normal encryption but also considering horizontal and vertical components along with region of interest (ROI). The work will apply the proposed algorithm over specific area within an image.

General Terms
Encryption, Hybrid Cryptography

Keywords
Image encryption, AES, ECC, ROI, Transposition

1. INTRODUCTION
Information in form of text, images, or video is the vital source of data which one needs to communicate over the network. Today with the increasing technology aspects we are at the level of increasing the threats associated with it. When we talk about the information in any form the most important thing need to be considered is its security. The any source of data needs to maintain its integrity, identity, and confidentiality. In today's world the multimedia data has become the main source of exchange between the parties. Presently all the information travels in the form of images, video, audio etc. Thus this form needs to be more secure from the threats arising due to various attacks in between the transferring of the information. There are several methods in which it can be done. When we talk about the multimedia data, watermarking, encryption, stenography etc are the basic ways through which we can secure these form of data.

2. LITERATURE SURVEY
Paper [1] explains the review on the various symmetric as well as the asymmetric algorithms used so far for the encryption as well as decryption of the data. This paper analyzes various algorithms on the different parameters and then finds the best suitable one. The paper concludes strength of each algorithm depends on the key strength, cryptography, key bits used. ECC and blowfish are considered to the best suitable for all the parameters given and stands on the top among so many. These are also prone to various attacks found in encryption. These are fast and provide better security aspects than other.

Hybrid encryption is something that author uses in this paper [2]. It uses both the public and private cryptography system. A secured encryption algorithm was proposed which ensures the data authentication, integrity, and privacy at the same time. Public key cryptography is based on the linear block cipher and the private key is based on the symmetric algorithm. Hybrid encryption is done by data transfer using various session keys which are combined with the symmetric algorithms.

This paper [3] involves both approaches for text as well as the image with the little variation in the AES code. For the textual encryption, input of 128 bit size are simulated and synthesized on processor using simple c language tool. As 128 bit size is used each of the input value is coded in the 8 bit sequence code. For the image encryption java code is used in the JDK environment for providing the encryption. CBC mode is used with the padding and AES algorithm in the first phase of the image encryption. After that MD5 and DES are used together to ensure the further security of the multimedia data.

A comparative study on various transposition and substitution techniques have been done in [4] on the basis of the parameters like key size, key attack, key type. Various substitution and permutation techniques have been applied in the paper to find the best suitable one. It has described the main aspects of the cryptography which includes confidentiality, integrity, and authentication.

Transposition is the method of changing or altering the bit values to make the encrypted text. This type of transposition can be applied to the different sort of the data. This paper [5] shows the transposition on the audio data by using the mean square value concept. The encryption is done by keeping the original sound intact.

A hybrid model is prepared in [6] which use the combination of symmetric algorithms such as Blowfish and AES. Digital signatures have also been applied in this encryption algorithm by using ECDSA (Elliptic Curve Digital signature algorithm) and for key exchange Elliptic Curve Diffie Hellman algorithm are being used. AES algorithm is being used in combination of the s-boxes and later on combined with the blowfish algorithm to provide with the hybrid cryptography. This cryptography maintains the data confidentiality and integrity. Pixels position plays a great role in the encryption purposes. These criteria have been used in the [7] by the combination of HAAR and DNA cryptography. In this technique the HAAR wavelet transform is been used to compress the image pixels. Wavelets are being used to show the data sorting by frequency. HAAR transforms performs the averaging and differencing on the image to convert the image in the low

resolution image and thus produces the detail coefficients. After this DNA algorithm is being used to encrypt the image further into the unreadable format

HAAR Wavelet is being implemented in [8]. The wavelet transform is sub band–coding system used for image as well as speech compression. HAAR transformation proves the image encryption by showing the values of MSE (Mean Square Error) and PSNR (Peak Signal Noise Ratio). Image matrix is divided into different blocks by using the Quantization process to calculate the mean pixel value of each block. This proves the Wavelet Transformation (DWT) a useful application in the compression problems.

3. PROPOSED WORK

3.1 AES Algorithm

AES is Advance Encryption standard which was adopted by the encryption standard by the US government. This is a symmetric encryption which works on the three different sizes of keys, namely 128, 192, 256 keys. Each of the key size produces the different form of the results and thus increases the strength and the complexity of the algorithm. AES mainly follows the Permutation- substitution framework. In this algorithm the plaintext is transformed number of times depending upon the rounds based on the key sizes. The following fig depicts the actual working of the AES.

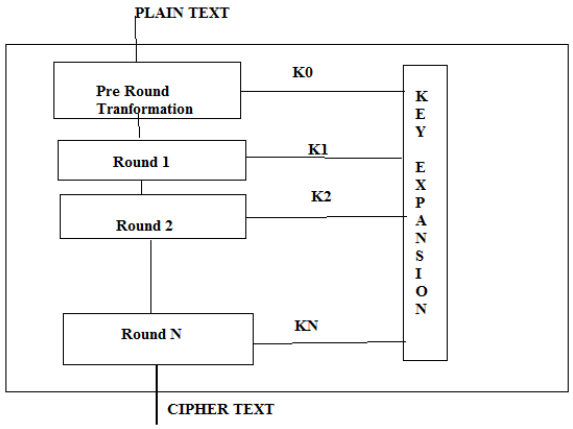

Fig1. Block diagram for AES encryption

3.2 ECC Algorithm

Elliptical Curve Cryptography is one of the emerging algorithms that have been used these days to secure the data. ECC is the asymmetric algorithm which uses the small key but still provides with the greater security as compared to other algorithms. It makes the use of the plane curve which acts as the finite fields. It uses the prime number function and a specific base point. When a maximum limit on the curve is reached encryption is done. The equation for the Elliptical curve is given as follows:

$$X^2 = YX^3 + iX + j$$

i and j are the integers.

4. IMPLEMENTATION

In the proposed work before applying the hybrid combination of the ECC and AES we had refine the image by using various other algorithms. It is a two module process. In the first module we are applying the ECC alone to look at the drawbacks it is having after refining the image. Steps for the first module of the process:-

1. Input the image and set the number of iterations.
2. Transform the image pixel by using the Haar algorithm to make it compatible with the pixel dimensions.
3. Set the specific Region of Interest (ROI) to get the specific domain for encryption.
4. Apply the ECC algorithm alone for the error calculation to get the image output.

In the second module we are applying ECC and AES together to show the accuracy on pixel intensity. The steps involve in the second module.

1. Input the RGB image
2. Transpose the image to alter the pixel values using HAAR algorithm
3. Take the previous input along with the calculation of the pixel intensity
4. Now again set the ROI to select the specific domain for the image encryption
5. Apply the hybrid combination of AES and ECC to get the more accurate encrypted image.

5. RESULTS

The results of both the modules are different and clearly show the accuracy of the algorithm.

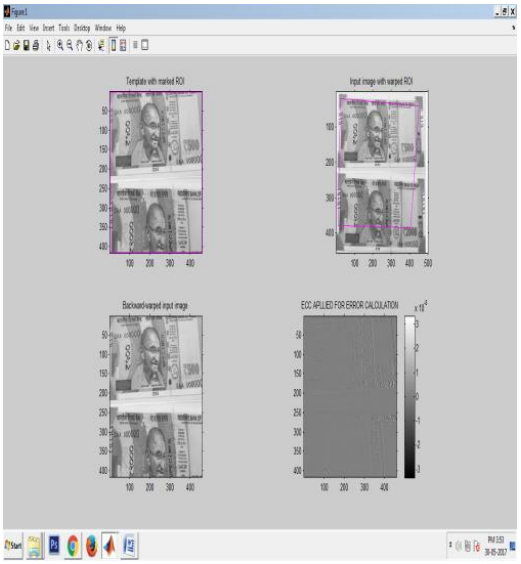

Fig2. ECC algorithm applied over ROI region

The fig shows the template marked with the ROI to select the specific area for the encryption. The other subplot in the image shows the wrapped area where the ECC is to be applied. The last plot show the ECC applied over the image which clearly has the marks for the error.

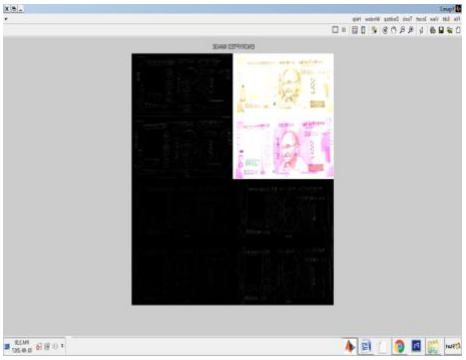

Fig 3. ECC and AES applied all together

The fig shows how appearance and visualization changes when ECC applied over encrypted image. This approach is different from the previous one because in last approach of ECC Algorithm. Original normal image was used where as in this case the resultant image is generated using encrypted image. Here we are trying to show the hybrid combination of the algorithm with more security and accuracy. The transposition of an image is performed by swapping the X and Y indices of its array representation. The transposition of image is necessary for providing the normalized effect. The HAAR transform has been used for the transposition of the image. The following histogram shows the transposed image.

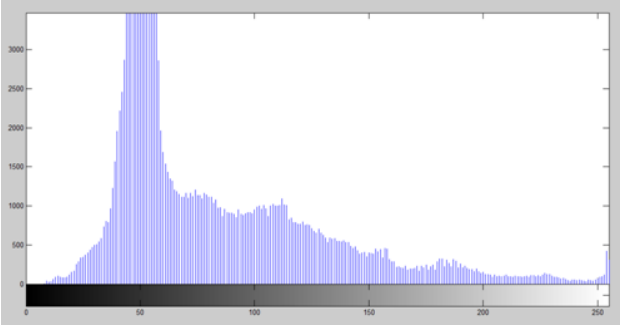

Fig4:Image histogram generated after transposition of image

6. CONCLUSION

In this paper hybrid combination of two symmetric and asymmetric algorithms is used to provide more accuracy to the encryption process. The ECC and AES are combined in such a way that differentiates them from the usual manner of encryption. The work just not concentrates typical encryption but rather consider even and vertical segments alongside district of intrigue (ROI). These days with the increasing trend of security it becomes essential to protect the data and information in a better way. This work can also be done on the various forms of data. The same encryption technique can be utilised for the video stream of data as one the future work.

7. REFERENCES

[1] Rajdeep Bhanot , Rahul Hans, " A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and Its Applications Vol. 9, No. 4 (2015), pp. 289-306.

[2] Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi, "Hybrid Encryption/Decryption Technique Using New Public Key and Symmetric Key Algorithm ", MIS Review Vol. 19, No. 2, March (2014).

[3] Kundankumar Rameshwar Saraf, Vishal Prakash Jagtap, Amit Kumar Mishra, "Text and Image Encryption Decryption UsingAdvanced Encryption Standard", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May – June 2014.

[4] Preeti Poonia, Praveen Kantha, "Comparative Study of Various Substitution and Transposition Encryption Techniques", International Journal of Computer Applications (0975 – 8887) Volume 145 – No.10, July 2016.

[5] Ahmad Jawahir, Haviluddin, "An audio encryption using transposition method", International Journal of Advances in Intelligent Informatics ISSN: 2442-6571 Vol 1, No 2, July 2015.

[6] A. P Shaikh and V. kaul, "Enhanced security algorithm using hybrid encryption and ECC", IOSR Journal of Computer Engineering (IOSRJCE),Vol. 6, Issue 3, pp. 80-85, 2014.

[7] Rohit kumar, bhanu pratap, and vaibhav singh, "image encryption using a combinantion of haar and dna algorithm", international journal of advanced trends in computer science and engineering issn 2278-3091 volume 3, no.5, september - october 2014

[8] Nidhi Sethi, Ram Krishna and Prof R.P. Arora, "Image Compression Using Haar Wavelet Transform", Computer Engineering and Intelligent Systems ISSN 2222-1719 (Paper) ISSN 2222-2863